High-Rise Security and Fire Life Safety

Office Buildings
Hotel Buildings
Residential and Apartment Buildings
Mixed-Use Buildings
This page intentionally left blank
High-Rise Security and Fire Life Safety
Third Edition

Geoff Craighead, CPP, BSCP
Board Certified in Security Management
ASIS International
Building Security Certified Professional
Building Security Council
Certified in High-Rise Life Safety Services
Los Angeles Fire Department
Dedication

To those people who lost their lives due to the September 11, 2001, New York World Trade Center terrorist attack:

Douglas G. Karpiloff, CPP, Port Authority of New York and New Jersey, security and life safety director for the New York World Trade Center, who at the time was transitioning his responsibilities to John P. O’Neill, Silverstein Properties, who was in his second day as head of the New York World Trade Center’s security operation; James Corrigan, security and life safety director for 7 World Trade Center, Silverstein Properties; Robert H. Lynch, Jr., manager 5 World Trade Center, Port Authority of New York and New Jersey; Charles Magee, chief engineer, Silverstein Properties; John M. Griffin, director of operations, Silverstein Properties; Howard B. Kirschbaum, security manager for Marsh U.S.A. Inc.; Ronald G. Hoerner, resident manager of Summit Security Services, Inc.’s, World Trade Center contract security operation; Richard Rescorla, CPP, first vice president of security for Morgan Stanley Dean Witter; Larry Bowman, Denny Conley, Francisco Cruz, Samuel Fields, Daniel Lugo, Robert Martinez, Jorge Morron, Esmerlin Salcedo, and Ervin Gaillard, security officers for Summit Security Services; Andrew Bailey, Mannie Clark, Lamar Hulse, and Stanley McCaskill, security officers for Advantage Security; and Francisco E. Bourdier, security officer for Allied Security, who was killed at a nearby building when one of the towers collapsed.

A total of 343 New York City firefighters, 37 Port Authority police officers (including Robert D. Cirri, police lieutenant; Anthony P. Infante, Jr., police inspector; Robert M. Kaulfers, police sergeant; Kathy Mazza, police captain; Ferdinand V. Morrone, director of public safety/superintendent of police; and James A. Romiot, police chief), an additional 35 Port Authority of New York and New Jersey civilians, and 23 New York City police officers.

And my wife, Sarah, my sweetheart and beloved helpmate, and Pip and Searcy, our treasured children, who put up with me working nights, weekends, and holidays.

And, the Lord, who sustains me every day. It is doubtful whether this book could have been written without the guiding hand of God.

The names of those persons, except for Francisco E. Bourdier, who perished on September 11, 2001, at the New York World Trade Center were obtained from ASISDynamics (ASIS International, Alexandria, VA, November/December 2001) and BOMA.org Staff (BOMA International, Washington, DC, May 2002).
## Contents

Author’s Biography ........................................... xxix  
Acknowledgments ........................................... xxxi  
Preface .......................................................... xxxvii  
Foreword to the Third Edition ......................... xxxix  
Foreword to the Second Edition .................... xli  
Foreword to the First Edition ......................... xliii

### 1. High-Rise Building Definition, Development, and Use  
1. What Is a High-Rise Building? .......................... 1  
2. Development of High-Rise Buildings ................. 2  
3. High-Rises Arise ........................................... 8  
4. The “World’s Tallest” Race .............................. 12  
5. Why Tall Buildings? .................................... 15  
6. Three Generations of High-Rise Buildings ........ 16  
   First Generation ......................................... 16  
   Second Generation ..................................... 17  
   Third Generation ....................................... 18  
      Steel-Framed Core Construction .................. 18  
      Steel-Framed Tube Construction ................. 19  
      Reinforced Concrete Construction ............. 20  
      Steel-Framed Reinforced Concrete Construction 21  
7. Types of High-Rise Buildings ......................... 21  
8. Summary .................................................. 22  
9. Key Terms ................................................ 22  
10. Additional Reading .................................... 26  
11. Additional Resources ................................. 26

  What Is Security? 27
  What Is Fire Life Safety? 28
Security of High-Rise Buildings versus Low-Rise Buildings 28
Fire Life Safety of High-Rise Buildings versus Low-Rise Buildings 29
Security of Modern Steel-Framed High-Rise Office Buildings 31
Impact of New York World Trade Center Terrorist Attacks on Building Security 33
  New York World Trade Center Profile 33
  February 26, 1993, Bombing 36
  September 11, 2001, Disaster 38
Fire Life Safety of Modern Steel-Framed High-Rise Office Buildings 40
Are Modern Steel-Framed High-Rises Less Fire Resistive Than Previous Generation Buildings? 44
New York World Trade Center of Investigation 46
  World Trade Center Building (WTC 7) 46
  Principal Findings of the Investigation 46
  Recommendations 48
Fire Risk in High-Rise Buildings 50
Other Fire Life Safety Features 51
Emergency Planning Essential 52
Impact of New York World Trade Center Terrorist Attacks on Building Safety 53
  February 26, 1993, Bombing 53
  September 11, 2001, Catastrophe 54
A Clear Message 55
Summary 55
Key Terms 56
Additional Reading 59

3. Security and Fire Life Safety Threats 61

What Is a Threat? 61
Security Threats 61
Fire Life Safety Threats 65
Building Emergencies 66
Aircraft Collisions 67
  September 11, 2001, New York World Trade Center 69
    Terrorist Attack 69
  Sequence of Events 71
  World Trade Center Building Performance 75
    Study and Final Report on the Collapse of the
    World Trade Center Towers 75
Bombs and Bomb Threats 95
  Bombs 96
    Suicide Bombers 96
    Vehicle-Borne Improvised Explosive Devices (VBIEDs) 97
  1993 New York World Trade Center, New York 98
  1993 Bishopsgate Financial Area, London 102
  1995 Alfred P. Murrah Federal Building, Oklahoma City 103
  1996 Khobar Towers Residential Military Complex,
    Dhahran, Saudi Arabia 105
  1998 U.S. Embassies in Nairobi, Kenya, and
    Dar es Salaam, Tanzania 105
  2002 Sheraton Hotel, Karachi, Pakistan 106
  2002 Nightclub, Bali, Indonesia 106
  2002 Hotel Mombassa, Kenya 107
  2003 Residential Compounds, Riyadh, Saudi Arabia 107
  2003 JW Marriott Hotel, Jakarta, Indonesia 108
  2003 HSBC Bank and British Consulate,
    Istanbul, Turkey 108
  2004 Train System, Madrid, Spain 109
  2004 Offices and Residences, Al Khobar, Saudi Arabia 109
  2005 London Transportation System 109
  2005 London Transportation System
    Attempted Bombings 110
  2006 Commuter Trains, Mumbai, India 110
  2007 London Incidents 110
  2008 JW Marriott Hotel, Islamabad, Pakistan 112
  2008 Taj Mahal Palace and Tower Hotel and
    Oberoi Hotel, Mumbai, India 112
  Bomb Threats 115
  Daredevils, Protestors, and Suicides 116
Daredevils 116
BASE Jumping 117
Protestors 117
Suicides 118
Elevator and Escalator Incidents 118
Elevators 118
Escalators 120
Fires 121
Basics of Fire Science 121
Principal Threat to Life Safety 123
Building Fires 124
  1911 Asch Building (Triangle Shirtwaist Company), New York City 126
  1946 Hotel LaSalle, Chicago, Illinois 128
  1946 Hotel Winecoff, Atlanta, Georgia 128
  1974 Joelma Building, São Paulo, Brazil 129
  1980 MGM Grand Hotel, Las Vegas, Nevada 130
  1981 Las Vegas Hilton Hotel, Las Vegas, Nevada 131
  1986 Dupont Plaza Hotel & Casino, Puerto Rico 132
  1988 First Interstate Bank Building, Los Angeles, California 134
  1989 Peachtree 25th Building, Atlanta, Georgia 136
  1991 One Meridian Plaza, Philadelphia, Pennsylvania 137
  1995 Residential Building, North York, Ontario, Canada 138
  1996 Garley Office Building, Hong Kong 138
  1997 Royal Jomtien Resort, Jomtien Beach, Thailand, Hotel 139
  2001 New York World Trade Center, New York 139
  2003 69 West Washington, Chicago, Illinois 139
  2004 Parque Central, Caracas, Venezuela 141
  2005 Windsor Building, Madrid, Spain 141
Fire Alarms 143
  When a Fire Emergency Is Faked 143
Hazardous Materials, Chemical and Biological Weapons, and Nuclear Attack 144
Hazardous Materials 144
Chemical and Biological Weapons 146
Nuclear Attack 147
Kidnappings and Hostage Situations 149
Labor Disputes, Demonstrations, and Civil Disorder 150
Labor Disputes 150
Demonstrations 150
Civil Disorder 151
Medical Emergencies 151
Natural Disasters 151
Earthquakes 151
Earthquake History 152
Case Study: 1994, Northridge Earthquake 157
Tsunamis 160
Volcanoes 162
Heat Waves 163
Storms (Noncyclone, Tornadoes, and Tropical Cyclones) 164
Noncyclone 164
Tornadoes 164
Tropical Cyclones (Cyclones, Hurricanes, and Typhoons) 165
Floods and Landslides 166
Contractible Diseases (Pandemic Influenza, Severe Acute Respiratory Syndrome, and Tuberculosis) 166
Pandemic Influenza 167
Severe Acute Respiratory Syndrome (SARS) 168
Tuberculosis 168
Power Failure 169
Slip-and-Falls 169
Stalking and Workplace Violence 169
Stalking 169
Workplace Violence 171
Workplace Violence Profiles 173
Prevention Measures 174
Traffic Accidents 176
Water Leaks 176
Summary 176
Key Terms 176
Additional Reading 184
## 4. Risk Assessments

### What Is a Risk Assessment?

185

### Risk Assessment Methodologies

187

### Systematic Ways to View a Building

188

- Interior Spaces
- Rings
- Layers of Defense

### Office Building Physical Security Survey

191

- Fact-Finding Process
- Survey Checklist
- Writing the Report
  - Title Pages
  - Cover Letter
  - Table of Contents
  - Introduction
  - Method of Compilation
  - Identification of Assets
  - Description of the Site, Building, and Surrounding Areas
  - Identification of Threats and Review of Past Incidents
  - Security Measures and Recommendations
  - Summary of Recommendations
  - Executive Summary
  - Appendices

### Building Fire Prevention Survey

200

- Fact-Finding Process
- Survey Checklist
- Writing the Report

### Risk Assessment to Mitigate Potential Terrorist Attacks against Buildings

203

- Step 1: Threat Identification and Rating
  - Identifying the Threats
  - Collecting Information
  - Determining the Design Base Threat
  - Determining the Threat Rating
Step 2: Asset Value Assessment
  Identifying the Layers of Defense
  Identifying the Critical Assets
  Identifying the Building Core Functions and Infrastructure
  Determining the Asset Value Rating

Step 3: Vulnerability Assessment
  Organizing Resources to Prepare the Assessment
  Evaluating the Site and Building
  Preparing a Vulnerability Portfolio
  Determining the Vulnerability Rating

Step 4: Risk Assessment

Step 5: Consider Mitigation Options
  Identifying Preliminary Mitigation Options
  Reviewing Mitigation Options
  Estimating Cost
  Reviewing Mitigation Options, Cost, and the Layers of Defense

Building Security Rating Program Promoting Logical Unified Security (PLUS™)
Use of Consultants and Specialists
  Reasons for Engaging a Consultant or Specialist
  Issues to Consider
  Sources of Consultants and Specialists

Summary

Key Terms

Additional Reading

5. Building Security Systems and Equipment
  Monitoring of Security Systems
  Physical Barriers and Perimeter Control
    Perimeter Landscaping, Walls, Fences, Sidewalks, and Pathways
    Fountains, Reflecting Pools, Sculpture, Boulders, Stairs, Concrete Planters, Concrete Barricades, Reinforced Light Poles, Bollards, Benches, Bus Shelters, and Rubbish Bins
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planters</td>
<td>239</td>
</tr>
<tr>
<td>Concrete Barriers</td>
<td>240</td>
</tr>
<tr>
<td>Bollards</td>
<td>240</td>
</tr>
<tr>
<td>Antiskateboard Barriers</td>
<td>241</td>
</tr>
<tr>
<td>Parking Controllers and Barriers</td>
<td>241</td>
</tr>
<tr>
<td>Guard Houses and Guard Booths</td>
<td>243</td>
</tr>
<tr>
<td>Right to Pass Signs or Plates</td>
<td>244</td>
</tr>
<tr>
<td><strong>Building Envelope</strong></td>
<td>244</td>
</tr>
<tr>
<td>Building Exterior Walls and Roof</td>
<td>245</td>
</tr>
<tr>
<td>Fire Escapes</td>
<td>245</td>
</tr>
<tr>
<td>Doors</td>
<td>246</td>
</tr>
<tr>
<td>Lobby Doors</td>
<td>246</td>
</tr>
<tr>
<td>Stairwell Exterior Fire Doors</td>
<td>248</td>
</tr>
<tr>
<td><strong>Vehicle Openings</strong></td>
<td>249</td>
</tr>
<tr>
<td>Openings for Ventilation, Natural Light, Utilities, Drains</td>
<td>252</td>
</tr>
<tr>
<td>and Sewers, and Outdoor Air Intakes</td>
<td></td>
</tr>
<tr>
<td>Windows and Glazing Protection</td>
<td>252</td>
</tr>
<tr>
<td>Windows</td>
<td>252</td>
</tr>
<tr>
<td>Weakness of Windows</td>
<td>255</td>
</tr>
<tr>
<td>Security Window Film</td>
<td>255</td>
</tr>
<tr>
<td>Blast Curtains</td>
<td>256</td>
</tr>
<tr>
<td>Security Bars, Grilles, Screens, and Shutters</td>
<td>256</td>
</tr>
<tr>
<td>Balconies</td>
<td>257</td>
</tr>
<tr>
<td>Atriums</td>
<td>257</td>
</tr>
<tr>
<td><strong>Building Floors, Ceilings, Interior Walls, and Interior</strong></td>
<td>257</td>
</tr>
<tr>
<td>Stairs or Stairways</td>
<td></td>
</tr>
<tr>
<td>Floors and Ceilings</td>
<td></td>
</tr>
<tr>
<td>Interior Walls</td>
<td></td>
</tr>
<tr>
<td>Interior Stairs or Stairways</td>
<td></td>
</tr>
<tr>
<td><strong>Building Interior Doors</strong></td>
<td>258</td>
</tr>
<tr>
<td>Doors to Offices, Hotel Rooms, Residences and Apartments,</td>
<td>258</td>
</tr>
<tr>
<td>and Interior Areas</td>
<td></td>
</tr>
<tr>
<td>Stairwell Doors</td>
<td>260</td>
</tr>
<tr>
<td>Won Doors</td>
<td>260</td>
</tr>
<tr>
<td>Doors to Maintenance Spaces</td>
<td>261</td>
</tr>
<tr>
<td>Restroom Doors</td>
<td>261</td>
</tr>
<tr>
<td>Elevators; Escalators; Moving Walks; Dumbwaiters; and</td>
<td>262</td>
</tr>
<tr>
<td>Rubbish, Mail, Laundry, and Linen Chutes</td>
<td></td>
</tr>
<tr>
<td>Elevators</td>
<td>262</td>
</tr>
</tbody>
</table>
Contents

Types of Elevators 262
Configuration of Elevator Systems 264
Escalators 266

Locks and Locking Systems 266
Pin Tumbler Locks 266
Bolts and Strikes 270
Master Keying of Pin Tumbler Locks 272

Key Control 277
Key Cabinet 277
Key Record 279
Key Blanks 279
Inventories 279
Audits 279

Perimeter Locking Devices 279
Electromagnetic Locks 280

Stairwell Locking Devices 281
Balancing Security and Fire Life Safety 283

Other Locking Devices 287
Electric Locks 287
Combination Locks 288

Electromagnetic Hold-Open Devices 290

Credential-Operated Locks 291
Magnetic Slug Cards 293
Magnetic Stripe Cards 293
Magnetic Sandwich or Barium Ferrite Cards 293
Wiegand Effect Cards 293
Insertion- and Swipe-Type Readers 293
Proximity Cards 295
Dual Technology Card 295
Smart Cards 296
Card Reader Applications 298
Antipassback Feature 298
Piggybacking and Tailgating 298
Identification Cards 298
Temporary Access Cards and Identification Badges 299

Biometric ID System–Operated Locks 299

Building Telephone or Voice-Over Internet Protocol Door Entry Systems 300
Turnstiles 300
Rapid Entry Systems 302
Property Control Systems 304
Safe Rooms 304
Filing Cabinets, Key Cabinets, Safes, Safe Deposit Boxes, and Vaults 305
Hotel Guest In-Room Safes 305
Metal Detectors and X-Ray Systems 305
Screening People and Property 305
Screening Vehicles and Containers 308
Asset Tracking Systems 308
Intrusion Detection Systems 309
Onsite Monitoring 309
Offsite Monitoring 310
Intrusion Detection Components 310
Sensors 310
Control Unit 312
Annunciation Device 313
Duress Alarm Systems 313
Security Mirrors 313
Lighting 314
Factors to Consider 314
General Types of Lighting 315
Incandescent 315
Mercury Vapor 316
Metal Halide 316
Fluorescent 316
High-Pressure Sodium Vapor 316
Low-Pressure Sodium Vapor 316
Light-Emitting Diodes (LEDs) 317
Appropriate Light Selection 317
Communication Systems 317
Telephones 317
Portable Two-Way Radio Systems 318
Transmitter and Receiver 318
Base Station 318
Use of a Repeater 318
Pagers 319
Public Address Systems 319

Monitoring of Fire Life Safety Systems
Voice Communication and Building Public Address System
Fire Department Voice Communication Systems
Public Telephone for Fire Department Use
Stairwell Intercom Systems
Fire Detection and Alarm System Annunciator and Control Panels
Manual Fire Alarm Stations
Sequence of Operations
Municipal Fire Alarm Box
Automatic Detection Systems
Smoke Detectors
   Ionization Smoke Detector
   Photoelectric Smoke Detector
   Placement of Smoke Detectors
   Addressable Devices
Heat Detectors
Gas Detectors
Automatic Sprinkler Systems
Water Supply for Sprinklers
   Gravity Tanks
   Suction Tanks
   Pressure Tanks
Fire Pump
Fire Department Connections
Sprinkler Pipes
Sprinklers
   Standard Spray Sprinklers
   Quick-Response and Residential Sprinklers
   Sidewall Sprinklers
Elevator Controls 388
Controls Inside Elevator Cars 389
Controls in Elevator Lobbies 390
Emergency Use of Elevators 392
Firefighter Controls 392
Present and Future Use of Elevators 393
State-of-the-Art Computerized Controls 394
Emergency and Standby Power 395
Emergency and Standby Power Systems Status Indicators 395
Emergency Power Systems 395
Standby Power Systems 396
Legally Required Standby Systems 396
Optional Standby Systems 396
Use of the Terms “Emergency Power System” and “Standby Power System” 396
Controls for Simultaneously Unlocking Stairwell Doors Locked from Stairwell Side 397
Other Building Systems and Equipment 397
Building Emergency Procedures Manual 397
Portable Fire Extinguishers 398
Classes of Fire and Recommended Extinguishing Agents 398
Water-Based Extinguishers 400
Carbon Dioxide Extinguishers 401
Halon and Halon Replacement Extinguishers 402
Dry Chemical Extinguishers 402
Wet Chemical Extinguishers 403
Positioning of Portable Fire Extinguishers 403
Exit Signs 403
Photoluminescent Lighting, Signs, Markers, and Exit Path Lighting Systems 406
Emergency Call and Assistance Stations 408
Personal Alarm, Personal Protection, Medical Alert Systems 409
Personal Alarm Systems 409
Personal Protection Devices 410
Medical Alert Systems 410
Automated External Defibrillators 410
Placement of AEDs 411
8. **Investigations** 447
   What Is an Investigation? 447
   Private Sector and Public Law Enforcement Investigations 448
      Rights of Public and Private Investigators 448
   Nature of Investigations 449
      Informal Investigation 449
      Formal Investigation 449
   Methods of Investigations 449
      a. Physical Surveillance 450
      b. Electronic Surveillance 450
      c. Research and Internal Audit 450
      d. Forensic Analysis 450
      e. Undercover 450
      f. Interviews and Interrogation 451
   Interviewing Techniques 451
      Planning the Interview 452
      Conducting the Interview 452
         Getting Acquainted 452
         Developing Rapport 452
         Motivating the Subject 453
         Keeping the Subject Talking 453
         Listening to “What Is Said” and “How It Is Said” 453
         Repeat the Process 453
   Obstacles to Conversation 454
      Specific Questions 454
      Yes/No Questions 454
      Leading Questions 454
      Rapid-Fire Questions 454
   Encouraging Conversation 455
      Open-Ended Questions 455
      The Use of the Long Pause 455
      Nondirective Approach 455
9. Office Buildings

Occupancy Characteristics

Assets, Threats, Vulnerabilities, and Countermeasures

Assets

Threats

Notable Incidents

Fire Risk in Office Buildings

Vulnerabilities

Countermeasures

Security Programs

Building Access Control

Vehicle Access to Parking Lots or Garages

Vehicle Access to Loading Dock/Shipping and Receiving Areas

Pedestrian Access to Buildings

Tenant Access Controls

Escorts of Building Users

Escorts to and from the Building

Escorts within the Building

Escorts within Tenant Space

Property Control

Objectives of a Property Control System

Property Removal Pass System

Asset Tracking Systems

Dangerous or Illicit Items

Couriers and Delivery Persons

Package Acceptance Policy

Lost and Found Property

Trash Removal Control
10. Hotel Buildings

Occupancy Characteristics
Assets, Threats, Vulnerabilities, and Countermeasures
    Assets
    Threats
        Threats to Guests
        Threats from Guests and Employees
        Notable Incidents
        Fire Risk in Hotel Buildings
    Vulnerabilities
    Countermeasures

Security Programs
    Hotel Building Access Control
        Parking of Hotel Guest and Patron Vehicles
        Parking of Hotel Staff and Vendor Vehicles
        Vehicle Access to Loading Dock/Shipping and Receiving Areas
    Pedestrian Access to Hotels
    Stairwell Access
    Access to Maintenance and Storage Areas
    Access to Guest Rooms
    Guest Room Security
    High-Profile VIP Guests
    Intoxicated Guests and Patrons
Guest Evictions 529
Escorts of Hotel Users 530
  Escorts to and from the Hotel 530
  Escorts within the Hotel 530
Property Control 530
  Objectives of a Property Control System 530
  Couriers and Delivery Persons 531
  Special Exhibits 531
  Construction and Remodel Activities 532
  Lost and Found Property 532
  Handling Property of Sick, Injured, or Deceased Guests 533
Housekeeping Operations 533
  Housekeeping Staff Screening 533
  Important Part of Security 534
Key and Electronic Access Card Control 534
  Key Points to Consider 535
Mobile Patrols 536
  When and Where? 536
  Patrolling Tips 537
Emergency Planning 538
  Key Concepts 538
  How to Develop a Building Emergency Management Plan 541
    Building Emergency Staff Organization 541
    Occupant Documentation and Training 542
    Evacuation Drills 546
    Important Consideration 546
Summary 547
Key Terms 547
Additional Reading 550

11. Residential and Apartment Buildings 551
  Occupancy Characteristics 552
  Assets, Threats, Vulnerabilities, and Countermeasures 553
    Assets 553
    Threats 554
    Fire Risk in Residential and Apartment Buildings 554
  Vulnerabilities 556
Countermeasures 556
Security Programs 557
Building Access Control 558
  Vehicle Access to Parking Lots or Garages 558
  Vehicle Access to Loading Dock/Shipping and Receiving Areas 559
Pedestrian Access to Buildings 559
Resident Systems 562
Visitor Systems 562
Apartment Access Controls 563
  Unwanted Solicitors 563
  Apartment Security Systems 564
  Doors Locked 564
  Resident Lock-Outs 564
Escorts of Building Users 564
  Escorts to and from the Building 565
  Escorts within the Building 565
Property Control 565
  Couriers and Delivery Persons 566
  Construction and Remodel Activities 567
  Lost and Found Property 567
  Trash Removal Control 568
Key and Electronic Access Card Control 568
  Key Control 568
  Key Points to Consider 569
Mobile Patrols 570
  When and Where? 570
  Patrolling Tips 571
Resident Security Education 572
Emergency Planning 573
  Key Concepts 573
  How to Develop a Building Emergency Management Plan 575
    Building Emergency Staff Organization 576
    Occupant Documentation and Training 577
    Important Consideration 579
Summary 579
Key Terms 580
Additional Reading 581
12. Mixed-Use Buildings
   Occupancy Characteristics
   Assets, Threats, Vulnerabilities, and Countermeasures
     Assets
     Threats
     Fire Risk in High-Rise Buildings
     Vulnerabilities
     Countermeasures
   Security Programs
   Emergency Planning
   Summary
   Key Terms
   Additional Reading

13. Liaison with Law Enforcement and Fire Authorities
    Liaison with Law Enforcement
    Liaison with Fire Authorities
    Fostering Relationships with Law Enforcement and
      Fire Authorities
      Communication
      Reporting Crimes
      Complying with Laws
      Enlisting Public Agency Support
      Hospitality
      Disaster Exercises
      Public Agency Presentations
      Professional Security and Fire Life Safety
        Organizations
        Community Service
    Summary
    References

14. Laws, Codes, Standards, and Guidelines
    Types of Standards
    Building Codes
    Fire Prevention Codes
    Who Enforces Building and Fire Prevention Codes?
Author’s Biography

Geoff Craighead is vice president of high-rise and real estate services for Securitas Security Services USA, Inc. For more than 25 years, he has been involved with the security and life safety operations of high-rise facilities, including the mixed-use Ocean Centre and Ocean Terminal in Hong Kong, the 62-story First Interstate Bank Building in Los Angeles, and numerous commercial buildings throughout North America. He has managed security staff, conducted risk assessments, carried out investigations, formulated security policies and procedures, written building emergency management plans, developed high-rise security training programs, and contributed chapters and articles on subjects ranging from high-rise security, emergency planning, and security consulting, to the use of computers in security management.

Craighead is a member of the ASIS International Board of Directors and chair of the ASIS Facilities Physical Security Measures Guideline Committee. He serves on the National Fire Protection Association (NFPA) International High-Rise Building Safety Advisory Committee (HRB-SAC) and the Building Security Council’s Building Rating System Committee. He is a former member of the Building Owners and Managers Association (BOMA) Greater Los Angeles Board of Directors; a past president of the ASIS Professional Certification Board that administers certification programs for security professionals throughout the world; and past chair of the ASIS Commercial Real Estate Council, 2005-2006. He is board certified in security management as a certified protection professional (CPP) by ASIS International, accredited as a building security certified professional (BSCP) by the Building Security Council, certified by the Los Angeles Fire Department to provide high-rise life safety services, and is a member of the Architectural Engineering Institute.

Craighead has spoken on high-rise security and fire life safety for leading security, commercial real estate, office, hotel and casino, multihousing, shopping center, banking and financial, mixed-use, and risk and insurance management groups, organizations, and property management firms.
HIGH-RISE SECURITY and FIRE LIFE SAFETY

Geoff Craighead

SECOND EDITION

HIGH-RISE SECURITY AND FIRE LIFE SAFETY

Geoff Craighead

HIGH-RISE SECURITY AND FIRE LIFE SAFETY

Third Edition

Geoff Craighead
Acknowledgments

Reviewers and Contributors

Many people have contributed to the field of security and fire life safety during the time that high-rise buildings have existed. I am above all indebted to those who took the time to document their thoughts so that others, such as me, could learn and benefit.

The following have contributed to my experience, learning, and understanding of the world of high-rise security and fire life safety: initially, Hong Kong, with its myriad of high-rise structures, followed by the United States of America, with its thousands of well-designed and well-operated buildings, the United Kingdom, and Australia; ASIS International, the preeminent global organization for security professionals, its board of directors, its Professional Certification Board that oversees its certification programs, its Commercial Real Estate Council, and the O.P. Norton Information Resources Center; Australian Standards; the International Professional Security Association (IPSA); the Security Institute; the Security Industry Association (SIA); the Building Security Council; the National Fire Protection Association (NFPA International), with its sound standards, comprehensive fire investigation reports, and training materials for fire life safety professionals; the Building Owners and Managers Association (BOMA International); the Institute of Real Estate Management (IREM); the International Facilities Management Association (IFMA); the Risk and Insurance Management Society, Inc. (RIMS); the Council on Tall Buildings and Urban Habitat (CTBUH); Access Control & Security Systems; Building Operating Management; Buildings; Security; Security Management; and Security Technology & Design.

I am very grateful to those firms, in particular, Securitas Security Services USA, Inc., that has employed me during my professional career and afforded me the privilege of experiencing the world of security.

In addition, there are many architects, building owners and managers, building inspectors, code developers, consultants, elevator technicians, engineers, investigators, lawyers, law enforcement and fire department personnel, security and life safety directors and managers, loss prevention and risk managers, security and fire life safety systems manufacturers and integrators, researchers, and friends from whom I have learned. It is not possible to name them all without overlooking someone; however, particular recognition is due to those individuals who have helped to make this third edition possible:

MARK J. BEAUDRY, CPP
Corporate Security
IBM
ACKNOWLEDGMENTS

BRIAN W. BIRNIE
Attorney at Law
LaFollette Johnson

JASON BROWN
National Security Director
Thales Australia

RICHARD A. “NICK” CANDEE
Candee & Associates
Former Executive Director, Global Operations
NFPA International

MATTHEW CATER
Developmental Editor
Elsevier

DENNIS O. CHALLINGER
Fellow of the Criminology Department
University of Melbourne
Consultant Criminologist
RLP Consulting

PAMELA CHESTER
Acquisitions Editor, BH Security
Butterworth-Heinemann, an imprint of Elsevier

JIMMY CHIN, CLSD
ASIS Lodging Security Council
Chairman, ASIS New York City Chapter

LEE CLONEY, CPP
Senior Regional Vice President
ASIS International

SARAH CRAIGHEAD
Proofreader

ERIC DECICCO
Senior Designer
Elsevier

EUGENE F. FERRARO, CPP, CFE, PCI
Member ASIS Commission on Standards and Guidelines
Chief Executive Officer
Business Controls, Inc.
JOHN R. HALL, JR., Ph.D.  
Division Director, Fire Analysis and Research  
National Fire Protection Association

CHUCK HUTCHINSON  
National Director, Security and Life Safety  
The Hanover Company

NORMA JEAN JOHNSON  
Regional Sales Manager Southwest  
Ving Card Elsafe

MICHAEL E. KNOKE, CPP  
Managing Editor  
Protection of Assets Manual (POA)  
ASIS International

JON A. SCHMIDT, PE, BSCP  
Director of Antiterrorism Services  
Burns & McDonnell

PETER N. SECCULL  
National Construction Manager (ret.)  
Babcock & Brown Communities Group

DAWNMARIE SIMPSON  
Senior Project Manager  
Elsevier

DAN SMITH, PSP, CPP  
Integrated Solutions Specialist Group  
ASSA ABLOY

ROBERT E. SOLOMON, PE  
Assistant Vice President for Building and Life Safety Codes Principal  
NFPA International

DON WALKER, CPP  
Co-Chair, CSO Roundtable Advisory Board  
Past President  
ASIS International

MARK WRIGHT  
Chair, ASIS Commercial Real Estate Council  
Director of Security and Life Safety-Houston  
Brookfield Properties
This page intentionally left blank
Darkness on the hallways. Voices echo. Silence holds... Watchmen walk slow from floor to floor and try the doors. Revolvers bulge from their hip pockets... Steel safes stand in corners. Money is stacked in them.

A young watchman leans at a window and sees the lights of barges butting their way across a harbor, nets of red and white lanterns in a railroad yard, and a span of glooms splashed with lines of white and blurs of crosses and clusters over the sleeping city.

By night the skyscraper looms in the smoke and the stars and has a soul.

—*Skyscraper* by Carl Sandburg
Preface

Due to their design and construction, high-rise buildings are unique structures with specialized needs. To protect the lives and property of the multitudes of people who daily use these facilities, it is essential that high-rise security and fire life safety programs be well planned and executed. Useful reference materials for commercial real estate owners and managers; security and life safety directors; security integrators and consultants; contract security companies; building and fire protection engineers; architects and builders; building, fire department, and law enforcement officials; and insurance firms include the following:

- High-rise building definition, development, and use
- Security and fire safety uniqueness of high-rise buildings
- Security and fire life safety threats
- How to conduct risk assessments
- Security and fire life safety systems and equipment in high-rise buildings
- How to effectively manage the security function, including investigations
- Security and emergency planning of office buildings, hotels, residential and apartment buildings, and mixed-use buildings
- Liaison with law enforcement and fire authorities
- Laws, codes, standards, and guidelines that govern security and fire life safety

The third edition of *High-Rise Security and Fire Life Safety* addresses these areas. In contrast to the previous two editions, which primarily focused on office buildings, this edition has been expanded to include hotel buildings, residential and apartment buildings, and mixed-use buildings.

Since this book was first published, there has been considerable change in the risk management of buildings. The disastrous events of September 11, 2001, when the Twin Towers of the New York World Trade Center were destroyed in a terrorist attack, were a watershed in the world of high-rise security and fire life safety. The attack on 9/11 has transformed the way we live and work in many facilities throughout the world. For obvious reasons, this event is given special treatment.

This book supplies material that can be adapted, modified, rejected, or used for the reader’s own purposes. I have endeavored to avoid errors, both of omission and commission. I will be glad to correct in future editions any inaccuracies that are brought to my attention.

It should be noted that, despite my professional affiliations and employment by a private security company, the observations expressed in this book are mine and do not necessarily reflect the viewpoints of those organizations.
In conclusion, I entrust this book to the kind consideration of building owners and managers in general, and security and fire life safety professionals in particular, with the desire that it will continue to benefit the high-rise community. Only when knowledge is applied specifically to the needs of a particular facility will it become of real value. Therein lies the reader’s part.

Geoff Craighead, CPP, BSCP
Certified Protection Professional
Building Security Certified Professional
LosAngeles, CA
Since the mid-1990s, we have seen a tall building boom unprecedented in the history of humankind. Whereas since the late 1800s we have witnessed specific “regionalized” periods of intense tall building construction—such as during late nineteenth century Chicago or art deco New York—this is the first time in history that we have seen tall buildings realized in unprecedented numbers on virtually all continents of the globe simultaneously. This is resulting in ever-denser, ever-taller cities from Moscow to the Middle East, from Shanghai to San Francisco. Some of the statistics are incredible; there are now more tall buildings in Asia than there are in North America—the traditional home of the skyscraper—and, by 2010, 59 of the 100 tallest buildings in the world will have been completed in the previous four years, since 2006. Not only is Burj Dubai in the United Arab Emirates set to smash all “tallest” records, with a height expected to be in excess of 800 meters/2600 feet (60% greater than the world’s current tallest building, Taipei 101 in Taiwan), but one in three of the world’s 100 tallest buildings is expected to be located in the Middle East region by 2010.

It is not only the height and geographic spread of tall buildings that has changed. Whereas the history of the world’s tallest buildings has been dominated by office buildings, many of the world’s new supertalls now contain residential or mixed-use functions. Similarly, whereas most tall buildings in the past were constructed of steel, we are now seeing a more significant use of concrete and composite (steel + concrete) construction. Additionally, whereas through the late 1980s or so, many of these buildings were built to project the prowess of an individual corporation, now they have taken on a new agenda: tall buildings are increasingly being built to project the vitality of a city on a global scale—creating skylines with brand recognition on an international level. This shift from corporate to city (or even government) ambition is reflected in the very titles of the world’s tallest buildings; formerly we had icons such as Chrysler, Sears (Willis), or Petronas; now we have Taipei 101, Burj Dubai, or the Chicago Spire, where the building itself takes on the responsibility of helping promote the city on the world stage.

This unassailed march of the tall building, after a decade or two of unbridled growth, is, of course, now under threat from the growing economic crisis gripping the globe. The question on everybody’s lips is, how bad is it going to get? Already we are seeing many high-profile proposals, some already under construction, slow down or stop completely. Perhaps this is not entirely a bad thing: perhaps it will give us, as an international community, a pause for reflection—on the cities we are creating and the merits or otherwise of some of the architectural excesses that have resulted as part of this unprecedented boom. Surely there is a need for reflection, especially with regard to the challenges of climate change and the need for more sustainable cities, buildings, and patterns of life in the future.
So the third edition of this seminal book comes at a pivotal time in the history of the tall building, not only in terms of whether these buildings will continue to grow in both size and number, but also whether they will evolve into the advanced entities they need to become to face the challenges of our time. Safety and security constitute an essential part of this equation. The decreasing political, ethnic, religious, resource, economic, and military stability of the world seems to have reached a new low, to the point where we now live in a world more unstable and dangerous than at any time since the late 1970s. The impact of terrorism and intentional acts of malice toward innocent people has massive implications for the design and construction of cities, buildings, and tall buildings specifically. It seems that nowhere is untouched—from New York to New Delhi, London to Lahore, Mumbai to Madrid. The increased “iconic-ness” of tall buildings gives them an increasing vulnerability to those who seek to get maximum publicity for their atrocious acts, as we have already seen to disastrous effect.

In the years since 9/11 and the World Trade Center tower collapses, we can certainly conclude that the event did not have the detrimental impact on the tall building typology as a continuing vital element in our urban centers that many feared. In fact, the exact opposite may indeed be true—the scale of the 9/11 event and the publicity given to the skyscraper may have contributed to its keen boost around the world since then. What the event did do, however, is initiate perhaps the largest introspective analysis of tall buildings ever, and this book is at the forefront of much of the state-of-the-art thought that resulted from that event, and the research conducted since then, in security and life-safety terms.

There is no doubt that the events of 9/11 are resulting in better designed, safer buildings throughout the world, but we need to ask ourselves if it is enough, in the unstable world we now inhabit. The twin challenges of terrorist-impacted security and a climate-changed urbanity put the tall building in a big spotlight. How can it evolve to meet these challenges? One thing is for sure—it seems unlikely that events such as 9/11 or Hurricane Katrina are going to abate any time soon.

This book is thus a departure point for this inquiry, posing the difficult questions that need to be asked and some of the possible solutions that building owners and managers, developers, architects, engineers and occupants will increasingly have to face in the coming years. Geoff Craighead brings into sharp focus many of the issues connected with this most complex of building types, and I fully recommend his book to you.

Antony Wood
Executive Director
Council on Tall Buildings and Urban Habitat
Chicago, Illinois
Foreword to the Second Edition

In the world of high-rise building design and construction, a variety of security and life safety questions are posed to the engineers and architects who must provide a functional building. The solutions should balance the design with the risks associated with any building—regardless of size and occupancy.

These are among the issues discussed throughout the second edition of High-Rise Security and Fire Life Safety. Most of these subjects apply to the entire range of high-rise building stock in the world—both new and existing. While we have always known that the life safety protection of the occupants of buildings is of paramount importance, today’s building tenants demand more: How secure is their space from a variety of threats, including theft of both real and intellectual property? Are tenant companies and their employees protected against personal harm by intruders, accidental fire and, now, terrorist attacks?

Achieving the proper level of protection is not possible with just one system or one procedure. It is the synergistic effect of all building systems and features working together that keeps facilities safe. Throughout the history of high-rise buildings, the norms for building safety have been derived from, and applied to, a great number of designs. World Trade Center 1 and 2 in New York; Petronas Tower 1 and 2 in Kuala Lumpur; Jin-Mao Building in Shanghai; Sears Tower in Chicago; and Emirates Tower in Dubai: all of these magnificent buildings have incorporated numerous systems and features that work, and have worked, to keep them safe during a wide range of events.

As building systems become more intricate and sophisticated, the overlap between systems is more pronounced now than ever before. The delineation between building security systems and fire alarm systems is just one example. Understanding the role, limitations, and interface between systems is fundamental to system selection. Complementing the systems side of building design is the operating feature, or human interface, that supplements these sophisticated systems. The best written plans and the highest quality building systems and components are meaningless if they are not exercised, tested, reviewed, checked, and updated on a periodic basis.

Geoff Craighead has provided us with a thorough description and review of all of these subjects as they relate to high-rise buildings. The public is now acutely aware of the importance of its own safety in high-rise buildings, and wants to know how building management teams are protecting them. As in the first edition of this book, we are given the road map of how to implement the best plan for a particular building.

The latest peril affecting design, namely the new level of hostile acts, is introduced in this edition of the text. Terrorist acts present unique threats that require new countermeasures.
High-rise buildings are not inherently dangerous structures, but they do require additional systems and features that other buildings do not. Keeping them safe and functional is what this text is all about.

Robert E. Solomon, PE
Assistant Vice President for Building and Life Safety Codes
NFPA International
Quincy, Massachusetts
Vertical cities—or high-rise buildings, as they are called—pose unique problems for security and safety professionals charged with the responsibility of protecting life and property. High-rise buildings, such as the Sears Tower in Chicago, the World Trade Center in New York, and thousands of others across the United States, are virtually cities within themselves. Just as the architecture within each varies, so do the regulations governing security and fire life safety programs for each building.

Every year, we see, hear, and read about the terrible tragedies caused by fires, earthquakes, tornadoes, bombings, disgruntled employees, terrorists, and the like. Every possible scenario must be accounted for. There is no substitute for an effective security and fire life safety program. Thousands of lives are dependent on it. Awareness and training are essential. Security and safety personnel must be trained for any and all eventualities.

The author includes here the terminology, the functions, the procedures, the equipment, and the standards for an effective program. *High-Rise Security and Fire Life Safety* is a comprehensive resource for everyone who manages, works in, or visits high-rise commercial office buildings.

Robert G. Lee, CPP, CFE, CDRP
Vice President and Corporate Security Director
Great Western Financial Corporation
Chairman of the ASIS National Standing Committee on Disaster Management
Northridge, California
This page intentionally left blank
High-Rise Building Definition, Development, and Use

The interesting question is why does man want to build to the sky. What is there about the desire for domination, or to reach God, or for private pride—the Pyramids are an example of that, but the tall building is certainly another.

—Skyscrapers Introductory Interview with Philip Johnson

Before entering the world of high-rise security and fire life safety, it is important to define what constitutes a high-rise building and to review the development and utilization of these unique structures.

What Is a High-Rise Building?

A building is an enclosed structure that has walls, floors, a roof, and usually windows. “A ‘tall building’ is a multi-story structure in which most occupants depend on elevators [lifts] to reach their destinations. The most prominent tall buildings are called ‘high-rise buildings’ in most countries and ‘tower blocks’ in Britain and some European countries. The terms do not have internationally agreed definitions.” However, a high-rise building can be defined as follows:

- “Any structure where the height can have a serious impact on evacuation” (The International Conference on Fire Safety in High-Rise Buildings).
- “For most purposes, the cut-off point for high-rise buildings is around seven stories. Sometimes, seven stories or higher define a high-rise, and sometimes the definition is more than seven stories. Sometimes, the definition is stated in terms of linear height (feet or meters) rather than stories.”
- “Generally, a high-rise structure is considered to be one that extends higher than the maximum reach of available fire-fighting equipment. In absolute numbers, this
has been set variously between 75 feet (23 meters) and 100 feet (30 meters), or about seven to ten stories (depending on the slab-to-slab distance between floors).

The exact height above which a particular building is deemed a high-rise is specified by fire and building codes for the country, region, state, or city where the building is located. When the building exceeds the specified height, then fire, an ever-present danger in such facilities, must be fought by fire personnel from inside the building rather than from outside using fire hoses and ladders.

For practicality and convenience such a multi-level or multi-story structure uses elevators as a vertical transportation system and, in addition, some utilize escalators to move people between lower floors.

Development of High-Rise Buildings

“From the individual ‘skyscraper’ to the urban clusters of ‘concrete canyons,’ the names for high-rise buildings have always combined a kind of admiration and reverence for the magnitude of the feat with a kind of fear about the threat to human values implicit in operating on so large a scale. The Tower of Babel is cited as a warning against pride and over-reaching, not as a goal to be sought.”

According to the Old Testament, after the Flood, people wanted to make a name for themselves by building a city called Babel with a tower that reached into heaven. The tower was constructed using brick for stone and tar (asphalt) for mortar.

“Come, let us build for ourselves a city, and a tower whose top will reach into heaven, and let us make for ourselves a name; lest we be scattered abroad over the face of the whole earth.”

And the Lord came down to see the city and the tower which the sons of men had built.

And the Lord said, “Behold, they are one people, and they all have the same language. And this is what they began to do, and now nothing which they purpose to do will be impossible to them.”

From the individual ‘skyscraper’ to the urban clusters of ‘concrete canyons,’ the names for high-rise buildings have always combined a kind of admiration and reverence for the magnitude of the feat with a kind of fear about the threat to human values implicit in operating on so large a scale. The Tower of Babel is cited as a warning against pride and over-reaching, not as a goal to be sought.”

According to the Old Testament, after the Flood, people wanted to make a name for themselves by building a city called Babel with a tower that reached into heaven. The tower was constructed using brick for stone and tar (asphalt) for mortar.

“Come, let us build for ourselves a city, and a tower whose top will reach into heaven, and let us make for ourselves a name; lest we be scattered abroad over the face of the whole earth.”

And the Lord came down to see the city and the tower which the sons of men had built.

And the Lord said, “Behold, they are one people, and they all have the same language. And this is what they began to do, and now nothing which they purpose to do will be impossible to them.”

The word skyscraper is just as it sounds: a fanciful, rather exaggerated term designed to communicate people’s awe and excitement about tall buildings. In reality, its meaning has changed radically in the hundred or so years since it came into our language. In the 1890s a building of ten stories more than qualified as a skyscraper, but today the word is rarely used to describe a building of fewer than fifty stories” (Sonder B. Skyscrapers. New York: MetroBooks, Michael Friedman Publishing Group; 1999:II).


“Come, let Us go down and there confuse their language, that they may not understand one another’s speech.”

So the Lord scattered them abroad from there over the face of the whole earth; and they stopped building the city.

Therefore its name was called Babel, because there the Lord confused the language of the whole earth.7

“During the rapid growth of the Roman Empire under the reigns of Julius and Augustus Caesar, the city of Rome became the site of a large number of hastily constructed apartment buildings—many of which were erected to considerable heights.● Because building collapse due to structural failure was frequent, laws were passed that limited the heights of buildings—first to 70 feet (21 m) and then 60 feet (18 m).”8 According to Sir Peter Hall’s Cities in Civilization,

Within Rome the old-style town house, domus, survived well into the early third century AD. But, at least as early as the third century BC, overcrowding in the city was producing a new urban form, the apartment block, or insula; Vitruvius commented that “the majesty of the city and the considerable increase in its population have compelled an extraordinary extension of the dwelling houses, and circumstances have constrained men to take refuge in increasing the height of the edifices.”9 Building heights rose to at least three storeys in the third century BC, to five or more by the first century BC; Julius Caesar set a limit of seventy Roman feet, Augustus reaffirmed it, Trajan reduced it to sixty feet for greater safety; later still, after the great fire, Nero prohibited the rebuilding of tenement houses and of narrow, winding lanes, laying out broad streets flanked with colonnades. In fact, from the Republic onwards the Romans found it necessary to make regulations to control the thickness of walls, the quality of building materials, and the roofs and height of buildings. Enforcement must have been a problem, for there seems to have been no requirement to notify the authorities, as opposed to possibly interested third parties, of any proposed new structure. Since there was no mechanism to require planning consent, any initiative had to be taken by some interested party.10

So, despite these edicts, new apartment houses continued to be built five or six storeys high...

8●“Residential buildings up to 5 or 6 stories have been common from the time of ancient Rome” (Mir M. Ali, ed. Catalyst for Skyscraper Revolution, Lynn S. Beedle: A Legend in His Lifetime. Chicago, IL: Council on Tall Buildings and Urban Habitat, Illinois Institute of Technology; 2004:194).
Apartments were mostly built with wood frames; and they were so high and poorly built that they were in constant danger of collapse or destruction by fire.11

Throughout subsequent history there have been other tall structures—pyramids and towers, castles and cathedrals—but it was not until the end of the 19th century that the skyscraper was born.

More than 150 years ago, cities looked very different from the way they look today. The buildings that housed people and their businesses were rarely over the height of a flagpole. Urban landscapes tended to be flat and uniform in pattern, apart from monuments, temples, and town halls; and cathedrals (adorned with domes, spires, or towers) which “towered above everything else in a city or town; they were visible from miles away.”12 “Historically, the word tower usually designated the church and the town hall until the birth of the skyscraper. The main evolutionary change has been in function, from a Campanile watchtower of the Renaissance or minaret of Islamic architecture to the office building.”13

Two major developments led to the skyscrapers that dominate major city skylines throughout the modern world:

1. In 1853, an American, Elisha Graves Otis, invented the world’s first safety lift or elevator.** This new form of vertical transportation*** enabled people to travel safely upward at a much greater speed and with considerably less effort than by walking (Figure 1–1).
2. In the 1870s, steel frames became available, gradually replacing the weaker combination of cast iron and wood previously used in construction. Until then, the walls had to be very thick to carry the weight of each floor.

It usually was agreed that a 12-inch wall was needed to support the first story, and four inches had to be added to the thickness of the base to support each additional story. The depth-to-height ratio precluded building structures above 10 stories. (An exception was the 16-story Monadnock Building [Figure 1–2] in Chicago, built in 1889 to 1891. Still standing, it is the last great monument to the age of load-bearing walls. At their base, the Monadnock Building’s walls are six feet thick.)

Steel frames were able to carry the weight of more floors, so walls became simply cladding for the purpose of insulating and adorning the building. This development, which included applying hollow clay tiles to the steel supports, resulted in a fireproof steel skeleton and

---

*The first method for mass-producing steel was called the Bessemer process. “Though named after Sir Henry Bessemer of England, the process evolved from the contributions of many investigators before it could be used on a broad commercial basis. It was apparently conceived independently and almost concurrently by Bessemer and by William Kelly of the United States. Bessemer developed and patented the process in 1856” (Bessemer. Encyclopædia Britannica Online. <www.britannica.com/EBchecked/topic/63067/Bessemer-process>; September 7, 2008).


**“A fire proof building will minimize the destruction of fire, whenever it strikes. In order to be termed fireproof, a building must offer 100% fire protection. Fireproof does not mean the absence of fire. It simply refers to proper building design and detail that effectively checks the spread of fire, while allowing access for occupants to escape” (Kruse T. Designing fireproof buildings. Skylines Magazine. Baltimore, MD: BOMA International; March 1993:12).
also permitted movable interior partitioning, which allowed office suites to be reconstructed to meet the demands of new tenants.\textsuperscript{15} “This new method of construction reduced the thickness of walls, increased valuable floor space, and because it weighed much less than masonry, allowed immense increases in height. Freed from the constraints

\textbullet A tenant can be a person, a group of persons, or a company or firm that rents or owns, and occupies space within a building.

\textsuperscript{15}Institute of Real Estate Management of the National Association of Realtors (IREM), “Office building industry: past, present, and future” (Harris RA, Revisions Author. Managing the Office Building. Rev. ed. Chicago, IL: IREM; 1985:3).
of traditional construction, the facade could now be opened with windows to maximize the amount of daylight reaching the interior of the building.\textsuperscript{16} Another factor that helped to make high-rises possible was the foundation upon which they stood. “The Egyptian method of spread footings didn’t work for skyscrapers since too much weight would bear down on too small an area. Modern builders had to switch to another ancient method, the Roman use of piles, which were driven into the ground all the way to the bedrock”\textsuperscript{17} to provide a strong supporting base.

According to the Institute of Real Estate Management,

\begin{quote}

The modern office building was created in response to rapid population increases and industrialization that occurred during the late nineteenth century. Between 1870 and 1920, the nation’s [United States] population doubled, and demand for office space increased fivefold. The first commercial structures were in the East [United States], but with railroads and a dynamic economy spurring national expansion, office buildings soon appeared in the Midwest, particularly in Chicago. In 1871, a fire destroyed this city. The disaster, combined with increased urban land values, the invention of the elevator, and the development of structural steel, gave rise to the skyscraper.\textsuperscript{18}
\end{quote}

Other developments, such as incandescent lamps, central heating, and forced-air ventilation, followed in the 20th century by fluorescent lights and air-conditioning,\textsuperscript{••} addressed the issue of providing adequate lighting, heating, ventilating, and air-conditioning

\begin{itemize}
  \item\textsuperscript{17} Sonder B. Skyscrapers. New York: MetroBooks, Michael Friedman Publishing Group; 1999:15.
  \item\textsuperscript{18} Institute of Real Estate Management of the National Association of Realtors (IREM), Office building industry: past, present, and future (Harris RA, Revisions Author. Managing the Office Building. Rev. ed. Chicago, IL: IREM; 1985:2–15).
  \item\textsuperscript{••} “The ‘Apparatus for Treating Air’ (U.S. Patent 808897) granted in 1906, was the first of several patents awarded to Willis Haviland Carrier. The recognized ‘father of air conditioning’ is Carrier, but the term ‘air conditioning’ actually originated with textile engineer, Stuart H. Cramer…. In 1921, Willis Haviland Carrier patented the centrifugal refrigeration machine. The ‘centrifugal chiller’ was the first practical method of air conditioning large spaces. Previous refrigeration machines used reciprocating-compressors (piston-driven) to pump refrigerant (often toxic and flammable ammonia) throughout the system. Carrier designed a centrifugal-compressor similar to the centrifugal turning-blades of a water pump. The result was a safer and
in large buildings. Such advancements in technology have not significantly affected the design of high-rise buildings but have contributed to their use, making them more convenient and comfortable.\textsuperscript{19}

High-Rises Arise

The 10-story Home Insurance Building (Figure 1–3), built in Chicago in 1885, is generally considered to be the world’s first skyscraper.\textsuperscript{19} As stated in the \textit{Architectural Record}, before the Home Insurance Building was demolished to allow construction of the New Field Building, “a committee of architects and others was appointed by the Marshall Field Estate to decide if it was entitled to the distinction of being the world’s first skyscraper. This committee, after a thorough investigation, handed down a verdict that it was unquestionably the first building of skeletal construction.”\textsuperscript{20} Engineer William Le Baron Jenney designed this 180-foot (55 meters) tall building using a steel frame to support the weight of the structure. Jenney stated in 1883, “we are building to a height to rival the Tower of Babel.”\textsuperscript{21}

In the 1890s, “most European cities like London, Paris, and Rome rejected tall buildings in their historical city centers meanwhile opting for height control regulations to maintain their low skylines. Today, however, we witness Paris and London giving away their horizontality in favor of the vertical scale.”\textsuperscript{22}

\textit{Although the term skyscraper is usually reserved for office buildings, by the turn of the twentieth century there was some justification for extending its application to hotels. Early on, hotels had played a precedent-setting role in the development of the high-rise building, with the eight-story Broadway Central Hotel [in New York] of 1869–70 worthy of “early skyscraper,” if not “first skyscraper,” designation. In 1890 the official hotel directory listed 128 hotels in the city [New York]; twenty or so were said to have been constructed since 1880, and hotel construction had entered a boom period. City more efficient chiller” (Bellis M. The father of cool: Willis Haviland Carrier–The history of air conditioning. <http://inventors.about.com/library/weekly/aa081797.htm>; June 14, 2008). Central air-conditioning became widespread in office buildings in the 1950s (Gillespie AK. “A city within a city,” and “Architecture.” In: \textit{Twin Towers: The Life of New York’s World Trade Center}. Piscataway, NJ: Rutgers University Press; 1999:207). “In the early 1950s, air-conditioning systems were reduced to very small electric-powered units capable of cooling single rooms. These were usually mounted in windows to take in fresh air and to remove heat to the atmosphere. These units found widespread application in the retrofitting of existing buildings—particularly houses and apartment buildings—and have since found considerable application in new residential buildings” (Building construction. \textit{Encyclopædia Britannica Online}. <www.britannica.com/EBchecked/topic/83859/building-construction>; August 30, 2008).


directories listed 183 in 1895, and by 1912 there were 222 that had fifty rooms or more. Although London and Paris had more hotel buildings, New York City could accommodate more people in its hotels than any other city in the world.23,24


An example of a hotel of this era was the Waldorf-Astoria (Figure 1–4) in New York City.

At the turn of the century, tall buildings began to spring up in New York City—in 1903, the triangular-shaped 22-story Flatiron (Fuller) Building, 285 feet (87 meters) high; in 1909, the 50-story Metropolitan Life Insurance Building, 700 feet (213 meters) high; and in 1913, the 57-story Woolworth Building, 792 feet (241 meters) high.

“Residential high-rises were also built near [city centers] so people could live close to their place of employment.”

According to Mierop,

---


People have lived in apartment buildings with elevators since the 1860s. But until the [nineteen] twenties they did not exceed about 15 floors. These “skyscrapers” were laughable to Emery Roth. To him is owed the Ritz Tower [Figure 1–5], built in 1926, the first modern residential skyscraper, 41 stories, 165 meters (540 feet) high. The Ritz Tower rapidly became the prototype for a new lifestyle. Half hotel, half apartment block, it was particularly suited to the nomadic world of business and to people who were already deciding to move to the country and to maintain only a pied-a-terre in town.

By the early thirties New York had about 150 skyscrapers of this type. Better yet, the model was exported to other cities and other continents. In 1934, the Park Hotel* was built in Shanghai on the same principle of small apartments with hotel service—22 stories high and tower-shaped; it was the tallest building in the Far East.** In Buenos Aires the Kavanagh,*** at 33 stories the highest skyscraper of the period to be built in reinforced concrete, is a residential tower.

FIGURE 1–5 First Modern Residential High-Rise. The 41-story skyscraper, Ritz Tower, 465 Park Avenue, whose architect was Emery Roth, was built in New York in 1926. Courtesy of Emery Roth Architectural Print Collection, PR 170, Department of Prints, Photographs, and Architectural Collections, the New-York Historical Society.

*“The construction of apartment hotels was much more profitable than single apartments. The hotels were not submitted to any regulations concerning sanitation, ventilation or natural light” (Mierop C. Skyscraper Higher and Higher. Paris, France: Institut Francais D’Architecture; 1995:87).


***“The Kavanagh was built in Buenos Aires in 1936…. It was the tallest building in the city” (Mierop C. Skyscraper Higher and Higher. Paris, France: Institut Francais D’Architecture; 1995:87).
In 1930 and 1931, two of the tallest buildings in the world were constructed in New York City: the 77-story Chrysler Building (1,046 feet, 319 meters) and the 102-story Empire State Building (1,250 feet, 381 meters). The latter, considered the “Eighth Wonder of the World,” was built in the record time of one year and 45 days.\(^\text{27}\) Both the Chrysler Building and the Empire State Building eclipsed the Woolworth Building as the world’s tallest skyscrapers. After these buildings were erected, 40-, 50-, and 60-story structures were built all over the United States.

“Skyscrapers began to appear in Shanghai, Hong Kong, São Paulo, and other major Asian and Latin American cities in the 1930s, with Europe and Australia joining in by mid-century.”\(^\text{28}\)

In the early 1970s, the 110-story Twin Towers of the New York World Trade Center (WTC) were built: the north tower, One World Trade Center (WTC 1), 1,368 feet (417 meters) in height, was completed in 1972; the south tower, Two World Trade Center (WTC 2), 1,362 feet (415 meters), was completed in 1973. At that time, the WTC towers were the tallest buildings in the world (taking the title from the Empire State Building, which for more than 40 years was the world’s tallest building). In 1974, the world’s tallest building became the Sears Tower. Located in Chicago, it has 110 floors, beginning at street level and ending 1,450 feet (442 meters) in the air.

The “World’s Tallest” Race

Since 1885, 17 buildings have staked claim to the title “The World’s Tallest Building.” According to information obtained from Skyscraper,\(^\text{29}\) these buildings are as follows:

<table>
<thead>
<tr>
<th>Date</th>
<th>Building</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1885</td>
<td>Home Insurance Building</td>
<td>Chicago, Illinois</td>
</tr>
<tr>
<td>1890</td>
<td>World Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1892</td>
<td>Masonic Temple Building</td>
<td>Chicago, Illinois</td>
</tr>
<tr>
<td>1894</td>
<td>Manhattan Life Insurance Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1898</td>
<td>St. Paul Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1899</td>
<td>Park Row Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1908</td>
<td>Singer Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1909</td>
<td>Metropolitan Life Tower</td>
<td>New York City</td>
</tr>
<tr>
<td>1913</td>
<td>Woolworth Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1930</td>
<td>Manhattan Company</td>
<td>New York City</td>
</tr>
<tr>
<td>1930</td>
<td>Chrysler Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1931</td>
<td>Empire State Building</td>
<td>New York City</td>
</tr>
<tr>
<td>1971–1973</td>
<td>World Trade Center</td>
<td>New York City</td>
</tr>
<tr>
<td>1974</td>
<td>Sears Tower</td>
<td>Chicago, Illinois</td>
</tr>
<tr>
<td>1998</td>
<td>Petronas Towers</td>
<td>Kuala Lumpur, Malaysia</td>
</tr>
<tr>
<td>2004</td>
<td>Taipei 101</td>
<td>Taipei, Taiwan</td>
</tr>
<tr>
<td>2009</td>
<td>Burj Dubai</td>
<td>Dubai, United Arab Emirates</td>
</tr>
</tbody>
</table>

\(^\text{27}\)Wright LM. *Spiders in the Sky.* Palm Coast, FL: Smithsonian; January 2002:18.


In 1972, the Council on Tall Buildings and Urban Habitat (CTBUH)* first compiled a list of “The One Hundred Tallest Buildings in the World.” In compiling the data “height is measured from the sidewalk** level of the main entrance to the architectural top of the building.”

CTBUH’s website (www.ctbuh.org) provides a wealth of information on high-rise buildings. In addition to “100 Tallest Buildings in the World” (see “The World’s Tallest Buildings” section at the back of this book), it lists the following (also provided in “The World’s Tallest Buildings” section at the back of this book):

- Tallest Single-Function Office Buildings in the World
- Tallest Single-Function Hotel Buildings in the World
- Tallest Single-Function Residential Buildings in the World
- Tallest Mixed-Use Buildings in the World

Also, CTBUH lists detail the “Tallest Steel Structure Buildings in the World,” the “Tallest Concrete Structure Buildings in the World,” and the “Tallest Mixed Structure Buildings in the World,” as well as the tallest completed, under construction, proposed, and demolished/destroyed buildings in the world.

“The number of skyscrapers, their height, [and] their pace of construction are barometers of business prosperity. The history of skyscrapers shows an astonishing parallel with the geographical evolution of capital movement on the map of the world. It would be possible, as an exercise, to suggest an economic interpretation of the list of ‘the hundred tallest buildings in the world.’”

“The Sept. 11, 2001, destruction of the World Trade Center’s 110-story twin towers did not put a damper on high-rise development. On the contrary, ‘over the last five years, there has been an unprecedented world-wide construction boom in tall buildings and urban development,’ said [CTBUH chairman, David] Scott.”

The current CTBUH “100 Tallest Completed Buildings in the World” list (see “The World’s Tallest Buildings” section at the back of this book) was used to compile the following information.

The tallest completed building is Taipei 101, the 101-story, 1670-foot (509 meters) mixed-use, pagoda-style structure completed in Taipei, Taiwan, in 2004.

This building is followed by Shanghai World Financial Center, the 101-story, 1641-foot (492 meters) mixed-use building completed in Shanghai, China, in 2008.

The next tallest are the mixed-use Petronas Towers (Petronas Tower I and Petronas Tower 2) in Kuala Lumpur, Malaysia. Built in 1998, each 88-story tower is 1483 feet (452 meters) high, connected at the 41st and 42nd floors by a distinctive, glass-enclosed pedestrian “skybridge.”

---

*The Council on Tall Buildings and Urban Habitat studies and reports on all aspects of the planning, design, and construction of tall buildings. Also of a major concern is the role and impact of tall buildings on the urban environment. <www.ctbuh.com>; June 14, 2008.

**The sidewalk is a paved walkway [for pedestrians] along the side of a street (The Free Dictionary by Farley, Sidewalk. <www.thefreedictionary.com/sidewalk>; September 6, 2008) or road in an urban area. Also known as a pavement in Britain and a footpath in Australia, India, Ireland, and New Zealand (The Free Dictionary by Farley, Sidewalk. <www.thefreedictionary.com/sidewalk>; September 6, 2008).

††The Council on Tall Buildings and Urban Habitat, LeHigh University, Bethlehem, PA.

The Council on Tall Buildings and Urban Habitat, Chicago, IL; 2008.


These buildings are followed by the 110-story office building Sears Tower (Willis Tower) at 1451 feet (442 meters); the 88-story, 1,381 feet (421 meters) mixed-use Jin Mao Building in Shanghai, China; and the 88-story office building Two International Finance Centre at 1362 feet (415 meters) in Hong Kong (Figure 1–6).

Cities in the elite 100 are Atlanta, Bangkok, Charlotte, Chicago, Chongqing, Cleveland, Dallas, Doha, Dubai, Frankfurt, Gold Coast (Australia), Guangzhou, Hong Kong, Houston, Izumisano, Kaohsiung, Kuala Lumpur, Los Angeles, Makati, Manama, Melbourne, Moscow, Nanning, New York, Philadelphia, Pittsburgh, Riyadh, San Francisco, Seattle, Seoul, Shanghai, Shenzhen, Singapore, Taipei, Toronto, Wuhan, and Yokohama.

Of the tallest 100 buildings, 64 are located outside of North America. Of these, 41 are in Asia and 16 are in the Middle East.

Burj Dubai (in Arabic “Burj” means tower) (Figure 1–7), located in Dubai, the United Arab Emirates, is the tallest structure in the world. Scheduled to be completed in 2009, this 160+-story monolith will stand at a stunning height (at the time of publication of this book, the estimated height of Burj Dubai was over 800 meters or 2600 feet).

---

It is projected to be the world’s tallest mixed-use building, with a hotel, corporate suites, apartments, and an observation deck.

On the drawing board, the tallest building in the world is Illinois Tower, a 528-story, 5,280-foot (1,610 meters), plus a 400-foot (122 meters) aerial, office building (see book cover for an image of this building). In 1956, architect Frank Lloyd Wright conceived this “mile-high” office building with the intention that it would be constructed on Chicago’s lakefront.34

Why Tall Buildings?

Leaving aside the belief that “mankind’s aspiration to reach the sky, the ‘Tower of Babel Complex,’ drives us to erect higher and higher buildings,”35 there are many other reasons why tall buildings are given

FIGURE 1–7 Burj Dubai. The world’s tallest structure located in Dubai, United Arab Emirates (UAE). Courtesy of Emaar Properties, Burj Dubai (www.burjdubai.com).

34Fortune JW. Wright to the top. Adapted from a paper presented at the International Association of Elevator Engineers’ Elevcon ’92 Conference; first published in Elevator Technology (The Construction Specifier. September 1992:87).

emphasis in modern urban architecture. According to *The Skyscraper and the City*, two reasons are paramount:

*First, the exploding population, largely urban, creates an increasing demand for tall buildings. The ever increasing population and growing economies in major cities of the world mean increasing urbanization globally and the continuing rise in population density in urban areas. Arable land areas are constantly being eaten away by urban spreading through suburban developments. The tall building can accommodate many more people on a smaller land than would be the case with low-rise building on the same land. A tall building is in effect a vertical transformation of horizontal expansion. Second, it is generally acknowledged that there has been evident neglect of the human factors in urban design at the expense of livability and quality of life. The outward expansion of cities into the suburbs has resulted in increased travel time and traffic gridlock. The prospect of traveling for a long time, to and from work, is detrimental to social well-being of the commuter and results in losses of fuel and productivity. Clustering of buildings in the form of tall buildings in densely built-up areas is the opportunity for creating open spaces like playgrounds, plazas, parks, and other community spaces by freeing up space at the ground level. Besides the impact on the city skyline, tall buildings thus influence the city fabric at the level where they meet the ground. The improvement of the “public realm” has become a necessity exerted by planning authorities in major cities.*

Three Generations of High-Rise Buildings

Since the first appearance of high-rise buildings, there has been a transformation in their design and construction. This has culminated in glass, steel, and concrete structures in the international and postmodernist styles of architecture prevalent today.

The following information, adapted largely from *High Rise/Fire and Life Safety* by the late John T. O’Hagan, former fire commissioner and chief of the New York City Fire Department, describes three generations of high-rise buildings in the United States since their inception.

First Generation

The exterior walls of these buildings consisted of stone or brick, although sometimes cast iron was added for decorative purposes. The columns were constructed of cast iron, often unprotected; steel and wrought iron was used for the beams; and the floors

---


* A column is “a structural member that carries its load in compression along its length. Most frequently, as in a building, the column is in a vertical position transmitting gravity loads from its top down to its base” (Answers.com, “Column” [February 18, 2007] definition from Sci-Tech Encyclopedia, The McGraw-Hill Companies, <www.answers.com/topic/column>; September 10, 2008).

** A beam is “a term generally applied to the principal horizontal members of a building so installed to support the load of the structure” (*Construction Dictionary*. 9th ed. [Greater Phoenix, Arizona, Chapter 98. Phoenix, AZ: The National Association of Women in Construction; 1996:48]).
were made of wood. “In a fire, the floors tend to collapse, and the iron frame loses strength and implodes.”

Elevator shafts were often unenclosed. The only means of escape from a floor was through a single stairway usually protected at each level by a metal-plated wooden door. There were no standards for the protection of steel used in the construction of these high-rises.

Second Generation

“The second generation of tall buildings, which includes the Metropolitan Life Building (1909), the Woolworth Building (1913), and the Empire State Building (1931), are frame structures, in which a skeleton of welded- or riveted-steel columns and beams, often encased in concrete, runs through the entire building. This type of construction makes for an extremely strong structure, but not such attractive floor space. The interiors are full of heavy, load-bearing columns and walls.”

As Brannigan described them,

Pre-World-War II buildings were universally of steel-framed construction. Floor construction and fireproofing of steel were often of concrete or tile, both good heat sinks and slow to transmit heat to the floor above. The construction was heavy but no feasible alternative existed.

Relatively small floor areas were dictated by the need for natural light and air. Advertisements for the RCA Building in New York proclaimed, “no desk any farther than 35 feet from a window.” This limited both the fire load and the number of occupants.... The typical office was quite spartan, though executive suites and eating clubs often were paneled with huge quantities of wood. Nevertheless, most fire loads were low.

Each floor was a well-segregated fire area in these buildings. Wall construction was frequently of wet masonry, joined to the floor so that there was an inherent firestop at the floor line. Masonry in the spandrel area (the space between the top of one window and the bottom of another) was adequate to restrict outside extension.

In these buildings vertical shafts were enclosed in solid masonry with openings protected with proper enclosures. Fire department standpipes of adequate capacity were usually provided. These were wet and immediately pressurized by gravity from a tank in the building.

Exterior fire tower stairways with an atmospheric break between the building and the stairway, the finest escape device available, were provided in many of the buildings. Such a stairway can be compared to an enclosed tower located away from the building which is reached by a bridge open to the weather, so that smoke cannot pollute the tower.

Windows could be opened in buildings of this era. This provided local ventilation and relief from smoke migrating from the fire.

---

39 ibid., p.66

*Fire load or fuel load is defined by the Fire Safety Institute as “the amount of material that is contained in a building, including both contents and combustible parts of the structure” (Abbott RJ. Lesson 3. In: Fire Science Institute Office Buildings Fire Safety Directors Course. 212/237–8650, New York; 1994:3–59). Included in the contents are furniture and furnishings such as draperies, curtains, carpets, and mats.
The windows leaked, often like sieves, therefore there was no substantial stack effect.40●

In this generation of buildings, developments such as the following occurred:

- The use of noncombustible construction materials that reduced the possibility of the collapse of structural members during a fire.
- The inclusion of assemblies** rated for a particular fire resistance. The enclosure of vertical shafts with protected openings.
- The use of compartmentation.***

Third Generation

Buildings constructed from after World War II until today make up the most recent generation of high-rise buildings. Within this generation there are those of steel-framed construction (core construction and tube construction), reinforced concrete construction, and steel-framed reinforced concrete construction.****

Steel-Framed Core Construction

These structures are built of lightweight steel or reinforced concrete frames, with exterior all-glass curtain walls. As Salvadori stated, “The so-called curtain walls***** of our high-rise buildings consist of thin, vertical metal struts or mullions, which encase the large glass panels constituting most of the wall surface. The curtain wall, built for lighting and temperature-conditioning purposes, does not have the strength to stand by itself and is supported by a frame of steel or concrete, which constitutes the structure of the building.”41


** Stack effect results from the temperature differences between two areas, usually the inside and outside temperatures, which create a pressure difference that results in natural air movements within a building. In a high-rise building, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke through the building” (Quiter JR. High-rise buildings. In: Fire Protection Handbook. 20th ed. Quincy, MA: National Fire Protection Association; 2008:20–80).

*****Assemblies are barriers that separate areas and provide a degree of fire resistance determined by the specific fire resistance rating of the assembly itself. An assembly may consist of a floor, a ceiling, a wall, or a door.

Compartmentation or compartmentalization is the use of walls, floors, and ceilings to create barriers against the spread of smoke and fire.

*******“Generally, a reinforced concrete (RC) construction, a steel-frame (S) construction, and a steel-framed reinforced concrete (SRC) construction are typically used to construct buildings. In recent years, as the buildings are large-sized and high-storied, a combination of three constructions has been widely used” (“Construction method for SRC structured high-rise,” [October 30, 2003], World Intellectual Property Organization. <www.wipo.int/pctdb/en/wo.jsp?IA=KR2003000643&DISPLAY=DESC>; September 2, 2008).


In the center of these buildings, or infrequently to the side, there is an inner load-bearing core constructed of steel or reinforced concrete. Most building utilities and services—stairway shafts (stairwells); passenger and service/freight elevator shafts; air-conditioning supply and return shafts; communication systems (telephones, public address systems, and computer networks); water, electrical power, and gas; and restrooms (toilets)—are enclosed in this central core. The core braces the building against wind.

Steel-Framed Tube Construction

Tube structures represented a change in the design of steel-framed buildings to enable them to be built über tall and yet remain strong enough to resist the lateral forces of winds and the possible effects of an earthquake. Tube construction used load-bearing exterior or perimeter walls to support the weight of the building.

“The key to stability is a resistance to lateral wind or earthquake forces, which grow dramatically in magnitude with the building’s height.”

“If not counteracted by proper design, these forces would cause a tall building to slide on its base, twist on its axis, oscillate uncontrollably, bend excessively or break in two.”

As Mierop explained,

The height of a skyscraper has always been determined by the capacity of its structure to resist the lateral forces of wind and earthquake; 15 to 20 stories for a steel framework system made rigid by masonry walls; up to 60 stories, 200 meters (650 feet) high for a steel framework system made rigid by a load-bearing core, 30 meters (100 feet) wide; higher still with a bigger core, but this would be to the detriment of the economic viability of the building [since the amount of leaseable floor space would be reduced]. When the structural role is shifted from the core to the outside walls of the building, resistance is increased together, proportionally, with possible height…. This system of load bearing exterior walls or “tube structure” was developed in the early sixties in the academic context of the Illinois Institute of Technology (IIT) by the engineers Myron Goldsmith and Fazlur Khan, both of the Skidmore, Owings & Merrill Chicago Office. No spectacular advance has subsequently revolutionized the skyscraper from a structural point of view.

“Because the core and perimeter columns carry so much of the load, the designers could eliminate interior columns, with the result that there is more open floor space

---

42 ibid., p. 116.
45 A load-bearing wall is defined as “a supporting wall that sustains its own weight as well as other weight. A wall that supports a portion of the building above it, usually a floor or roof; also called bearing wall” (Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:97).
46 “When the exterior walls are made rigid the building behaves like a huge hollow tube. As the interior columns no longer have to resist lateral pressure their position becomes optional and the floor layout more flexible” (Mierop C. Skyscraper Higher and Higher. Paris, France: Institut Francais D’Architecture; 1995:74).
for tenants.”

Floor areas tend to be larger, with little compartmentation using floor-to-ceiling walls and barriers.

**Reinforced Concrete Construction**

“Concrete that has been hardened onto imbedded metal (usually steel) is called reinforced concrete, or ferroconcrete. The reinforcing steel, which may take the form of rods, bars, or mesh, contributes tensile strength.”

Reinforced concrete is “concrete containing reinforcement and [is] designed on the assumption that the two materials act together in resisting forces.”

Also, according to *Encyclopædia Britannica,*

*High-rise structures in concrete followed the paradigm of the steel frame. Examples include the 16-story Ingalls Building (1903) in Cincinnati, which was 54 metres (180 feet) tall, and the 11-story Royal Liver Building (1909), built in Liverpool by Hennebique’s English representative, Louis Mouchel. The latter structure was Europe’s first skyscraper, its clock tower reaching a height of 95 metres (316 feet). Attainment of height in concrete buildings progressed slowly owing to the much lower strength and stiffness of concrete as compared with steel.*

“Parallel to the development of tall steel structures, substantial advancements in high-rise structural systems of reinforced concrete have been made since 1945. The first of these was the introduction of the shear wall as a means of stiffening concrete frames against lateral deflection, such as results from wind or earthquake loads; the shear wall acts as a narrow deep cantilever beam to resist lateral forces.”

“Concrete requires no additional fireproofing treatments to meet stringent fire codes, and performs well during both natural and manmade disasters. Because of concrete’s inherent heaviness,
mass, and strength, buildings constructed with cast-in-place reinforced concrete can resist winds of more than 200 miles [322 kilometers] per hour and perform well even under the impact of flying debris.”

Steel-Framed Reinforced Concrete Construction
These structures are a mixture of reinforced concrete construction and steel-framed construction, hence the name steel-framed reinforced construction. An example would be “a steel framed structure with a concrete shear core and composite floors built with steel decking.” The term mixed construction is sometimes used to describe this type of high-rise construction.

Types of High-Rise Buildings
The use of a building has considerable influence on its security and fire life safety needs. There are different types of high-rise buildings classified according to their primary use. This book addresses the following ones:

1. Office buildings. An office building is a “structure designed for the conduct of business, generally divided into individual offices and offering space for rent or lease.”

2. Hotel buildings. “The term ‘hotel’ is an all-inclusive designation for facilities that provide comfortable lodging and generally, but not always food, beverage, entertainment, a business environment, and other ‘away from home’ services.” There are also hotels that contain residences. Known as hotel-residences, this type of occupancy is later addressed in mixed-use buildings.

3. Residential and apartment buildings. A residential building contains separate residences where a person may live or regularly stay. Each residence contains independent cooking and bathroom facilities and may be known as an apartment, a residence, a tenement, or a condominium. An apartment building is “a building
containing more than one dwelling unit.”54 “Apartment buildings are those structures containing three or more living units with independent cooking and bathroom facilities, whether designated as apartment houses, ... condominiums, or garden apartments.”55

4. **Mixed-use buildings.** A mixed-use building may contain offices, apartments, residences, and hotel rooms in separate sections of the same building. Hotel-residences are another type of mixed-use occupancy. “The hotel residences trend is notably different from its predecessors such as fractional/time share hotel units, which are not wholly owned, or condo hotels, which are wholly owned hotel rooms without, for example, kitchens. Not only do hotel residences have kitchens and everything else an owner would expect in a typical abode, they also include amenities such as maid and room service, plus restaurants, spas and gyms.... Typically, [these] residences are on the top floors of hotels.”56

In addition, there are two types of structures commonly associated with buildings that technically are classified as high-rises but usually are not required to conform to high-rise building laws, codes, and standards (particularly the laws requiring the installation of approved automatic sprinkler systems). These structures are (1) buildings used solely as open parking structures and (2) buildings where all floors above the high-rise height limit are used for open parking.

**Summary**

- Since their first appearance toward the end of the 19th century, the design and construction of high-rise buildings have changed considerably.
- The use of a building impacts its security and fire life safety needs. There are different types of high-rise occupancies classified according to their primary use. This book primarily addresses office buildings, hotel buildings, residential and apartment buildings, and mixed-use buildings, with some mention of the other types of high-rise occupancies.

**Key Terms**

**Apartment.** “An individual dwelling unit, usually on a single level and often contained in a multi-unit building or development.”57 See also **condominium** and **residential building**.

**Apartment building.** “A building containing more than one dwelling unit.”58

56 Olmsted L. Hotel residences: all the perks, none of the work. *USA Today.* McLean, VA; September 19, 2008:8D.
58 ibid.
with independent cooking and bathroom facilities, whether designated as apartment houses, … condominiums, or garden apartments.”\(^{59}\) See also condominium and residential building.

**Assemblies.** Barriers that separate areas and provide a degree of fire resistance determined by the specific fire resistance rating of the assembly itself. An assembly may consist of a floor, ceiling, wall, or door.

**Beam.** “A term generally applied to the principal horizontal members of a building so installed to support the load of the structure.”\(^{60}\)

**Building.** An enclosed structure that has walls, floors, a roof, and usually windows.

**Cantilevered beam.** “A projecting beam that is supported and restrained at one end only.”\(^{61}\)

**Column.** “A structural member that carries its load in compression along its length. Most frequently, as in a building, the column is in a vertical position transmitting gravity loads from its top down to its base.”\(^{62}\)

**Compartmentation.** The use of walls, floors, and ceilings to create barriers against the spread of smoke and fire. Also known as compartmentalization.

**Composite floor.** “Comprise[d] of [a slab] and beams acting compositely together. Composite slabs consist of profiled steel decking working together with in situ reinforced concrete. The decking not only acts as permanent formwork to the concrete, but also provides sufficient shear bond with the concrete, so that the two materials act compositely together. Although principally for use with steel frames, composite slabs can also be supported on brick, masonry or concrete components.”\(^{63}\)

**Condominium.** “A multiple-unit structure in which the units and pro rata shares of the common areas are owned individually; a unit in a condominium property. Also, the absolute ownership of an apartment or unit, generally in a multi-unit building, which is defined by a legal description of the air space the unit actually occupies plus an undivided interest in the common elements that are owned jointly with other condominium unit owners.”\(^{64}\) Residential condominiums are commonplace in today’s society. See also apartment and residential building.

**Curtain wall.** “Non-load-bearing sheets of glass, masonry, stone, or metal that are affixed to the building’s frame through a series of vertical and horizontal members called mullions.”\(^{65}\) “Thin, vertical metal struts or mullions, which encase the large glass panels constituting most of the wall surface.”\(^{66}\)

**Elevator.** A means of vertical transportation in a building. Two main types of elevators are used in high-rise buildings: traction and hydraulic. An elevator is also known as a lift.

---


\(^{61}\) ibid., p. 87.


\(^{63}\) Composite Flooring Systems: Sustainable Construction Solutions. MCRME, UK and The Steel Construction Institute, Berkshire, UK; August 2003.

\(^{64}\) Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:32.


Escalator. “An escalator is just a simple variation on the conveyor belt. A pair of rotating chain loops pull a series of stairs in a constant cycle, moving a lot of people a short distance at a good speed.”

Fire load. “The amount of material that is contained in a building, including both contents and combustible parts of the structure.” Included in the contents are furniture and furnishings such as draperies, curtains, carpets, and mats. Also known as fuel load.

Fireproof. “Fireproof does not mean the absence of fire. It simply refers to proper building design and detail that effectively checks the spread of fire, while allowing access for occupants to escape.”

Footpath. See sidewalk.

Fuel load. See fire load.

High-rise. A building “that extends higher than the maximum reach of available firefighting equipment. In absolute numbers, this has been set variously between 75 feet (23 meters) and 100 feet (30 meters), or about 7 to 10 stories (depending on the slab-to-slab distance between floors). The exact height above which a particular building is deemed a high-rise is specified by the fire and building codes in the area in which the building is located.

Hotel. “The term ‘hotel’ is an all-inclusive designation for facilities that provide comfortable lodging and generally, but not always food, beverage, entertainment, a business environment, and other ‘away from home’ services.”

Hotel-residences. “Hotel residences have kitchens and everything else an owner would expect in a typical abode, they also include amenities such as maid and room service, plus restaurants, spas and gyms…. Typically, [these] residences are on the top floors of hotels.”

Hydraulic elevator. “The cabs of these elevators are moved by a telescoping tubular piston underneath, which is raised and lowered by pumping oil in and out of it with an electric pump. Hydraulic elevators move slowly, but they are the least expensive type and are well suited for low buildings.”

Lessee. “The tenant in a lease.” See also tenant.

Load-bearing wall. “A supporting wall that sustains its own weight as well as other weight. A wall that supports a portion of the building above it, usually a floor or roof; also called bearing wall.”

---

72Olmsted L. Hotel residences: All the perks, none of the work. USA Today. McLean, VA; September 19, 2008:8D.
74Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:94.
75Ibid., p. 97
Mixed-use building. A building that may contain commercial offices, apartments, residences, and hotel rooms in separate sections of the same building. Hotel-residences are another type of mixed-use occupancy.

Mullion. “Thin, vertical struts ... which encase the large glass panels constituting most of the wall surface”76 of a curtain wall.

Occupancy. “The purpose for which a building or other structure, or part thereof, is used or intended to be used.”77

Office building. A “structure designed for the conduct of business, generally divided into individual offices and offering space for rent or lease.”78

Pavement. See sidewalk.

Reinforced concrete. “Concrete that has been hardened onto imbedded metal (usually steel) is called reinforced concrete, or ferroconcrete.... The reinforcing steel, which may take the form of rods, bars, or mesh, contributes tensile strength.”79

Rent. “Payment for the use of space or personal property owned by another. In real estate, a fixed periodic payment by a tenant to an owner for the exclusive possession and use of leased property.”80

Residence. A place where a person may live or regularly stay.

Resident. “One who lives (or resides) in a place. Referring to residential tenants as ‘residents’ is preferred by many real estate professionals.”81 See also tenant.

Residential building. A building containing separate residences where a person may live or regularly stay. Each residence contains independent cooking and bathroom facilities and may be known as an apartment, a residence, or a condominium. See also apartment building and condominium.

Shear wall. “A wall composed of braced panels (also known as shear panels) to counter the effects of lateral loads acting on a structure. Wind and earthquake loads are the most common loads braced wall lines are designed to counteract.”82

Sidewalk. “A paved walkway [for pedestrians] along the side of a street”83 or road in an urban area. Also known as a pavement in Britain and a footpath in Australia, India, Ireland, and New Zealand.84

Skyscraper. A very tall building consisting of many floors. “Today the word is rarely used to describe a building of fewer than fifty stories.”85

Slab. “A flat, usually horizontal or nearly so, molded layer of plain or reinforced concrete usually of uniform thickness, but sometimes of variable thickness; the flat

78 Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:120.
80 Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:146.
81 Ibid., p. 149.
84 Ibid.
section of floor or roof either on the ground or supported by beams, columns, or other framework.”^86

**Slab floor.** “A reinforced concrete floor.”^87

**Stack effect.** “Results from the temperature differences between two areas, usually the inside and outside temperatures, which create a pressure difference that results in natural air movements within a building. In a high-rise building, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke through the building.”^88

**Tenant.** A person, a group of persons, or a company or firm that rents or owns and occupies space within a building. “A legal term for one who pays rent to occupy or gain possession of real estate; the lessee in a lease. Real estate managers often limit the use of the term tenant to commercial tenants and refer to residential tenants as residents.”^89 See also [lessee](#) and [resident](#).

### Additional Reading


### Additional Resources

1. The Council on Tall Buildings and Urban Habitat provides “studies and reports on all aspects of the planning, design, and construction of tall buildings.” <www.ctbuh.org>.

2. The Emporis.com website provides information, including photographs, on buildings over 12 stories tall located throughout the world. <www.emporis.com/en>.


---


^87Ibid.


^89*Glossary of Real Estate Management Terms*. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:171.
Security and Fire Life Safety
Uniqueness of High-Rise Buildings

What Is Security and Fire Life Safety?

For the purposes of discussion and to address issues in a systematic way, this book treats **security** and **fire life safety** in high-rise structures as two different disciplines. However, at times these subjects are so closely interwoven that they appear to be one and the same. Before addressing the security and fire life safety of high-rise buildings, it is important to understand what these terms mean.

What Is Security?

Security is a noun derived from the Latin word *securus*, which means, “free from danger” or “safe.” The *New Webster Dictionary* defines security as “the state of being secure; confidence of safety; freedom from danger or risk; that which secures or makes safe; something that secures against pecuniary loss.”¹ Fischer and Green wrote, “Security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury.”²

Public security involves the protection of the lives, property, and general welfare of people living in the public community. This protection is largely achieved by the enforcement of laws by police funded by public monies.

Private security, on the other hand, involves the protection of the lives and property of people living and working within the private sector. The primary responsibility for achieving this rests on an individual, the proprietor of a business employing an individual, the owner or agent of the owner of the facility where a business is conducted, or an agent of the aforementioned who specializes in providing protective services. As Post and Kingsbury have stated, “In providing security for specific applications, the purpose of private security may be described as providing protection for materials, equipment, information, personnel, physical facilities, and preventing influences that are undesirable, unauthorized, or detrimental to the goals of the particular organization being secured.”³

---

Physical security is defined as “that part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against espionage, sabotage, damage, theft and loss.”

What Is Fire Life Safety?

Safety is a noun derived from the Latin word salus, which means safe (salvation is also from this root). The New Webster Dictionary defines safety as “the state or quality of being safe; freedom from danger.” Obviously, there is little distinction between the terms security and safety.

Fire life safety involves minimizing the possible danger to life and property from various threats, including that of fire. Fire and life safety, fire safety, and life safety are synonymous terms commonly in use in high-rise structures.

Security of High-Rise Buildings versus Low-Rise Buildings

From a security perspective, high-rise buildings differ from low-rise buildings in these ways:

1. The existence of multiple, occupied floors, one on top of another, usually means a higher concentration of occupants and therefore more property that could be damaged or stolen as compared with that in low-rise buildings. The potential for theft can increase because the concentration of property makes the site more attractive to a criminal; also, the greater the concentrations of people, the better the chances of a thief’s anonymity, particularly if he or she dresses and behaves like other building users. Kitteringham noted that, “many tall buildings, and high-rises are located in the central business districts of cities. Their proximity to mass transit facilities and ease of access to the general public puts them at particular risk from professional thieves.”

---


2. The more individuals assembled in one location at any one time, the higher the possibility that one of these persons will commit a crime against another. One of the difficulties in making statements is the lack of crime pattern analyses for high-rise buildings. The incidence of crime in any building, whether it is a high-rise or low-rise, is impacted by factors such as the neighborhood in which it is located, the design of the building, its use and type of tenants, and the security program that is in place.

3. In addition, although this may seem self-evident, all high-rise buildings have stairwells and elevators, and a low-rise, single-story building does not. A stairwell, because it is a relatively unused area (apart from use in emergency evacuations), could be the site of a crime, such as an assault (including that of a sexual nature) or a robbery. An elevator also could be the scene of vandalism and crimes against persons (see later comment in this chapter regarding the absence of elevator attendants).

Fire Life Safety of High-Rise Buildings versus Low-Rise Buildings

From a fire life safety perspective, high-rise buildings differ from lower-height buildings in the following ways:

1. The existence of multiple, occupied floors, one on top of another, usually means a higher concentration of occupants and therefore more property, hence, a greater potential fuel load of the building.
2. The probability of a large uncontrolled fire moving upward is of concern in a high-rise building because of its vertical nature.
3. The more individuals assembled in one location at any one time, the more likely it is that some of these people could be injured or killed, particularly by an incident occurring close to them.
4. Depending on the location of an emergency, there may be a delay in reaching the area to provide assistance. For example, a medical emergency that occurs on

---

*A crime is “an act or omission which is in violation of a law forbidding or commanding it for which the possible penalties for an adult upon conviction include incarceration, for which a corporation can be penalized by a fine or forfeit, or for which a juvenile can be adjudged delinquent or transferred to criminal court for prosecution. The basic legal definition of crime is all punishable acts, whatever the nature of the penalty” (ASIS Online Glossary of Terms. June 5, 2008. <www.asisonline.org/library/glossary/index.xml>; November 27, 2008).

**Glen W. Kitteringham in his masters of science in security and crime risk management thesis, commenting on statements made in the first edition of this book, pointed out that “previous studies involving low and high-rise residential buildings draw a correlation that the higher the building the higher the crime rate, however the author fails to provide data that would either prove or refute any of the statements he made in regard to commercial structures” (A study of two types of vertical crime pattern analysis in the commercial, multi-tenanted high rise structure. Masters of Science Thesis in Security and Crime Risk Management. University of Leicester (UK): The Scarman Centre for the Study of Public Order; February 2001:24).

***Glen W. Kitteringham noted that “crime pattern analysis is a process that encompasses a number of techniques, all of which can assist crime risk management. It is therefore best regarded as a generic term, covering a number of approaches and techniques for analyzing the incidence and distribution of crime” (A pattern for crime: an overview of the two dimensional mapping process for crime risk evaluation. Canadian Security, Facility Management Supplement, Aurora, Ontario, Canada; November 2001:12).
the uppermost floor of a skyscraper will require considerably more travel time for the responding medical team than a similar incident occurring in a building lobby.

5. Evacuation of occupants when an emergency occurs is hampered by the fact that large numbers of people (sometimes hundreds, but possibly thousands when it is a large office building) cannot all leave the structure at once via elevators and emergency exit stairwells. (High-rises have never been designed for total evacuation—i.e., the capacity for all occupants to evacuate all at once from a building to an outside area of refuge or safety. Alternative evacuation strategies are discussed later in this book.)

6. Access by the fire department—from both outside and inside the building—may be restricted. According to the International Fire Service Training Association (IFSTA), \(^7\) external access may be limited by the following:

- Setback of the building from public access roads and driveways, landscaping, berms, and fountains; and surfaces covering under-building or subterranean parking garages that will not support the weight of fire fighting vehicles. These factors may restrict the proximity to the building that fire department aerial ladder apparatus can attain.
- External features of the structure such as decorative walls, sunscreens, and building offsets (where an upper floor is set back from the floors beneath it) may inhibit the use of aerial ladders.
- Fire department aerial ladders have a limited reach. “The usual height limitation for aerial ladder operations is about 75 feet [23 meters].” \(^8\)

Internal access may be restricted to the use of stairwells and elevators that are approached through the building lobby or lower levels such as basements. Internal access may be complicated by the time required for fire department personnel to reach, and equipment to be transported to, an incident occurring in the upper levels of a structure.

The effectiveness of the response to an incident, such as a fire, may be affected by the availability of fire department personnel and equipment: hoses, forcible entry tools, breathing apparatus, lights, and power supplies. Only the largest fire departments are able to provide the several hundred fire fighters that may be necessary to control an advanced high-rise fire. The number of fire department staff required for response will depend on the type of tenancy and pattern of use of the building, the size and type of fire, its location within the structure, and whether an extensive search of the building needs to be conducted. Much of this information will be ascertained onsite, when fire department personnel have had an opportunity to evaluate the incident. “Also, the delivery of personnel and equipment to the fire may be blocked by very hazardous falling glass which may cut hose lines and injure personnel. The glass hazard may make evacuation from the building impossible.” \(^9\) Because modern high-rise building floors are often


very large, interior hose lines that firefighters run from stairwells may not reach every part of a floor.

7. According to Quiter,\textsuperscript{10}

The high-rise building often has natural forces affecting fire and smoke movement that are not normally significant in lower buildings. Stack effect and the impact of winds can be very significant, and very different, in high-rise buildings.

Stack effect results from the temperature differences between two areas, usually the inside and outside temperatures, which create a pressure difference that results in natural air movements within a building. In a high-rise building, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke through the building.

No manual fire-fighting techniques are known to counter stack effect or to mitigate its effect during a fire.

In completing this discussion as to how the fire life safety of high-rise buildings differs from that for lower-height buildings, it is important to note an idea raised by Quiter about fire protection requirements for high-rises of varying heights:

Additional protection is required in some buildings as they get higher. Few people, when they walk into a 7- to 10-story building, picture that building as a high-rise. Yet the level of protection traditionally required is the same in that building as in a 50- or 100-story building down the street. Similarities between the two buildings are that exterior rescue above 75 feet (23 meters) is difficult, if not impossible (depending on local fire department apparatus and access to the building). However, the dynamics of air movement (and therefore smoke movement), the viability of total evacuation versus staged evacuation, and the level of information needed by occupants and the fire service are clearly different in a very tall building than in a mid-level, but still “high-rise,” building. These ideas are beginning to be addressed in a piecemeal fashion in the [building and life safety] codes, but often with little technical analysis or evaluation of risk.\textsuperscript{11}

Security of Modern Steel-Framed High-Rise Office Buildings

The changes in the design and construction of high-rises since their first appearance have impacted the security needs of these facilities. For example, modern office buildings have inherent security hazards that differ from those of the earliest commercial buildings because of the following:

- Open-style floors with little compartmentation and fewer individual offices that can be secured have made it easier for a potential thief to gain access to business


and personal property. The advent of modern telecommunications with portable telephones, voicemail, and answering services has meant that the presence of a tenant receptionist to screen persons entering an office is now not always the standard. The open-style floor plan has made it easier for an unauthorized person, having once gained access, to move unchallenged throughout an entire floor.

- The concealed or interstitial space often located above the suspended or drop-down ceiling and the floor slab above on each floor of many high-rise office buildings has provided a possible means of ingress to a tenant office. This space could also be used to hide unauthorized listening or viewing devices such as microphones or cameras.
- The higher number of occupants per floor in a modern office building means a greater concentration of business equipment and personal items and therefore a more desirable target for a potential thief.
- The greater number of occupants per floor in a modern office building means the increased potential for these individuals to be perpetrators or targets of a crime and an increased likelihood that some of these people could be injured or killed, particularly by an incident occurring close to them.

In addition to these changes, other factors have added to the security risks of modern high-rise office buildings. For one thing, tenant offices often house highly successful corporations that have designed and furnished their places of business in a style to reflect their status. This has resulted in very high-quality furnishings, including, in some instances, expensive works of art and state-of-the-art business systems. The tenant employees themselves are generally well paid, often carry cash and valuables, and tend to drive and park expensive vehicles in the building parking garage. Hence, these facilities are a potential target for criminal activity.

Next, the computer revolution with its proliferation of compact business machines (such as personal digital assistants and desktop and laptop computers) has resulted in equipment and proprietary information that a potential thief can carry away relatively easily. Computer networks have presented a unique set of risks because crimes can now be committed without the perpetrator ever setting foot on the premises where sensitive information is stored.

Finally, the development in the mid-1950s of completely automatic control systems for the operation of elevators eliminated the need for elevator attendants and, in effect, did away with an important access control and screening measure for high-rise buildings. With the elevator attendant gone, it is often possible for people to travel unchecked.

*Previously only found in computer data centers where underfloor power and data cabling is run, some modern office buildings now have raised floors that house electrical, plumbing, and air-conditioning systems, as well as cables, telephone wiring conduits, and computer wiring. Of course, this concealed space could also be used to hide unauthorized listening or viewing equipment such as microphones or cameras.

**It is understood that an occupancy permit or certificate of occupancy determines the number of persons that can occupy a facility and areas within that facility. Occupancy is “the purpose for which a building or other structure, or part thereof, is used or intended to be used” (NFPA 101: Life Safety Code Handbook. 10th ed. Quincy, MA: National Fire Protection Association; 2006:32 citing ASCE [American Society of Civil Engineers] 7:1.2).
throughout a structure once they have entered an elevator. Such unchecked travel can be curtailed by the use of other security measures such as security personnel, locking off certain “secured” floors from elevator access, and the installation of access control systems in elevator cars and lobbies. Also, with the attendants now absent, vandalism and crimes against persons—such as an assault (including that of a sexual nature) or a robbery—could occur within an elevator car, where, unless viewed by a video camera inside the car or by someone outside the elevator car if it has transparent side walls in a transparent elevator shaft, no one (apart from the victim of the assault or robbery) is usually present to witness the incident.

The technological advances that have occurred in the security field, particularly since the 1960s, have mitigated some of the aforementioned security risks. High-performance microprocessors have considerably extended and improved the application of basic security measures such as the following:

- Barriers, locks, and property control systems
- Intrusion detection and duress alarm systems
- Lighting systems
- Communication systems (telephones, portable two-way radios, pagers, public address systems, intercoms, and personal digital assistants)
- Closed-circuit television systems and audio/video recording equipment
- Patrol monitoring devices
- Security staff to oversee the operation of these systems and equipment

These changes have all contributed to making improved and better-designed building security programs possible.

**Impact of New York World Trade Center Terrorist Attacks on Building Security**

Before leaving the subject of the security of modern high-rise buildings, it is appropriate to discuss the impact on building security of the February 26, 1993, and the September 11, 2001, terrorist attacks on the Twin Towers of the New York World Trade Center. (The incidents are detailed in Chapter 3.) Understandably, the incidents, particularly “9/11,” have created a heightened awareness throughout the world of the vulnerability of high-rise buildings to hostile acts.

**New York World Trade Center Profile**

The New York World Trade Center was located on New York City’s lower west side, next to the Hudson River at the southern end of Manhattan. The World Trade Center (WTC) was on a 16-acre site with seven buildings (WTC 1 through WTC 7) grouped

---

around a 5-acre plaza (Figure 2–1). The WTC complex consisted of these buildings, the Port Authority Trans-Hudson (PATH) and the New York Metropolitan Transit Authority (MTA) WTC stations, and associated Concourse areas.

Of the 110-story Twin Towers, the north tower (WTC 1), 1,368 feet (417 meters) in height, was completed in 1972, and the south tower (WTC 2), 1,362 feet
(415 meters) in height, was completed in 1973. According to The 9/11 Commission Report, 13

Each tower contained three central stairwells, which ran essentially from top to bottom, and 99 elevators. Generally elevators originating in the lobby ran to “sky lobbies” on higher floors, where additional elevators carried passengers to the tops of the buildings.

Stairwells A and C ran from the 110th floor to the raised mezzanine level of the lobby. Stairwell B ran from the 107th floor to level B6, six floors below ground, and was accessible from the West Street lobby level, which was one floor below the mezzanine. All three stairwells ran essentially straight up and down, except for two deviations in Stairwells A and C where the staircase jutted out toward the perimeter of the building. On the upper and lower boundaries of these deviations were transfer hallways contained within the stairwell proper. Each hallway contained smoke doors to prevent smoke from rising from lower to upper portions of the building; they were kept closed but not locked. Doors leading from tenant space into the stairwells were never kept locked; reentry from stairwells was generally possible on at least every fourth floor.

Doors leading to the roof were locked. There was no rooftop evacuation plan. The roofs of both the north tower and the south tower were sloped and cluttered surfaces with radiation hazards, making them impractical for helicopter landings or as staging areas for civilians. Although the south tower had a helipad, it did not meet 1994 Federal Aviation Administration guidelines.

The WTC towers were the fifth and sixth tallest buildings in the world. WTC 3 was the 22-story Marriott Hotel, WTC 4 and 5 were 9-story office buildings, WTC 6 was an 8-story office building, and WTC 7 was a 47-story office building. Underneath a large portion of the main WTC Plaza and WTC 1, 2, 3, and 6 was a 6-story subterranean structure.

The Port Authority of New York and New Jersey, a public agency, developed the WTC complex. It owned and operated it up until 2001 when a private party, Silverstein Properties, acquired a 99-year capital lease for the complex. The WTC provided approximately 12 million square feet of rentable office space for government and commercial tenants. Many of the commercial tenants were prominent in the financial and insurance industries.

About three blocks southeast of the WTC Complex is the New York Stock Exchange and the Wall Street financial district. In addition to the World Financial Center (WFC) complex, surrounding the site were other prominent buildings such as the Bankers Trust building, the 1 Liberty Plaza building, the Verizon building, and a historic Cass Gilbert-designed building at 90 West Street.


*A sky lobby (or sky-lobby) is a floor where occupants can cross over from an express elevator to another group of elevators serving local floors. Also known as a cross-over floor.

**These deviations were necessary because of the placement of heavy elevators and machine rooms, and were located between the 42nd and 48th floors and the 76th and 82nd floors in both towers* (The 9/11 Commission Report; 2004:541 [note]).
February 26, 1993, Bombing

As a result of the 1993 bombing in the subterranean parking garage of the World Trade Center, over the next seven years the WTC spent $60 million in capital funds to upgrade the security of the complex.\textsuperscript{14} According to Doug Karpiloff, the late security and life safety director for the World Trade Center, “Prior to the bombing, the WTC was an open building during the day, but closed at night. After the bombing, the Center was relegated to a closed facility, in which public parking was completely eliminated.”\textsuperscript{15} As reported by SECURITY,\textsuperscript{16} the security upgrades included the following measures:

Forming a ring of 250 ten thousand–pound steel-reinforced planters surrounding the WTC complex, with a custom movable gate that permitted emergency vehicle access to the plaza. Then, according to Karpiloff, “If the gate is opened, the CCTV [closed-circuit television] cameras lock onto the gate and can’t be moved until the gate is closed.” Once the gate was closed, the cameras unlocked and resumed regular surveillance. [According to Access Control & Security Systems,\textsuperscript{17} bomb-resistant trash containers were also provided as part of the perimeter protection system.]

Providing total closed-circuit television (CCTV) coverage of the plaza and perimeter of the WTC.

Restricting parking beneath the WTC to authorized tenants with special vehicle identification. [According to Access Control & Security Systems,\textsuperscript{18} the parking access control system utilized auto vehicle identification (AVI) tags on car windshields and driver’s proximity cards to make sure that both the vehicle and the driver were authorized to enter the garage.]

Equipping the underground parking garage with bullet-resistant guard booths, anti-ram barriers and explosives-detection trained (bomb-sniffing) dogs.

Stopping trucks one block from the buildings for inspection (after being cleared to proceed to the truck dock, the drivers were photographed along with their driver’s license, bill of lading, and registration information for storage on the WTC main server).

Installing a stopped vehicle detection system to sense cars stopping around the perimeter and within the WTC plaza. (When a stopped vehicle was sensed, the CCTV cameras locked onto that area, the WTC police were alerted and a video print of the vehicle could be taken. The cameras did not unlock until the vehicle was moved. This information was stored on the WTC server at the Security Command Center.)

Creating a “closed” building, whereby all people entering the building had to pass through an optical turnstile or register at the visitor’s desk. At all times, all tenants and visitors were required to carry a photo ID proximity card. Visitors had to be authorized by a WTC tenant in order to enter the building. Once authorized, the visitor was photographed and issued an ID card


\textsuperscript{17}Towering Team Leader. Atlanta, GA: Access Control & Security Systems; September 2000:42.

\textsuperscript{18}ibid.
to be used one time, or for one day or one week or up to six months. (If someone jumped over the waist-high optical turnstile, CCTV motion detectors in the lobby caused CCTV cameras to lock onto the violator, the WTC police were alerted and a video print of the jumper was taken. This information was stored on the WTC server at the Security Command Center.)

Color coding of all photo proximity cards for tenants and visitors: green for tenants, red for long-term visitors, and yellow for contractors. (When a tenant failed to bring their access card to work, they were issued a visitor’s card. If the tenant’s regular access card were presented for entry on the same day as the visitor’s card was issued, it would not work.)

A “mystery shopper” program utilizing an outside contractor to test at various points if security could be breached.\footnote{ibid, p. 46.}


Using optical fiber cable to provide high-speed security transmissions with “limitless bandwidth, long distance, low-loss transmission, immunity to electromagnetic interference and radio frequency interference and long-term stability.”\footnote{ibid.} (The fiber-optic cable was run in a ring in two directions and was therefore completely redundant. According to Alan Reiss, Director of the World Trade Center at the time, “If there is a fiber that is severed or cut somehow, you don’t shut down the whole system, it automatically switches to an alternate path.”)

Providing, in case of an emergency, duplicate security command and operation centers that ran the WTC security systems.

Other measures were undertaken to secure the WTC, according to an article by Michael Gips, “Building in Terrorism’s Shadow”:

With its $60 million security upgrade since the 1993 bombing, the World Trade Center has set the standard for building security. When determining what security measures should be in place for a given building in the post-bombing environment, Doug Karpiloff, manager of life safety and security at the World Trade Center, says that one must now ask whether the building is a significant or signature structure in the city where it resides. For example, is it the tallest building in the city, is it a symbol of the city itself, or does it house an organization whose activities are inimical to a large group of people? “If you answer yes to any [of these],” Karpiloff says, “visitors and tenants may expect more security than would normally be provided.” Karpiloff says that he would advise such properties to commission a comprehensive threat assessment and master plan for the building, which would weight threats and risks and explore vulnerabilities.\footnote{Gips, MA. “Building in terrorism’s shadow,” a May 2000 Security Management article republished in Counterterrorism and Contingency Planning Guide (a special publication from Security Management and ASIS International, Alexandria, VA, post–September 11, 2001:11).}

Although the World Trade Center’s destruction was not a building security issue, Doug Karpiloff’s words still ring loud and true. To evaluate the security of any high-rise
building, one needs to identify what assets are at risk, what are the threats to those assets, and what are the vulnerabilities or weaknesses of that particular facility. Only then can effective countermeasures be selected to eliminate or mitigate the identified risks.

Today, many high-rise owners and managers are looking for concrete suggestions to relieve their fears and those of their tenants. Many concerns can be addressed by going back to basics and conducting a security survey [described in Chapter 4] to determine a building’s security status, then making recommendations for improvements. Before conducting this survey, its scope needs to be clearly defined. What exactly is to be achieved by surveying the building, and what are the underlying reasons for it? Are we assessing the potential for a terrorist [incident], or are we just unnerved by what has happened in society? If it is a terrorist threat that we are concerned with, then part of the process should be to evaluate the building and its tenants to determine if either may draw attention from extremist groups. Only after the real motivating factor has been identified can a meaningful review be conducted.23

September 11, 2001, Disaster

The loss of the WTC has changed the face of high-rise building security. Before the incident, access controls in office buildings were generally loose during normal business hours, Monday to Friday, although they usually tightened up after hours. Since this incident, many high-rise office buildings throughout the United States (and in various overseas countries), particularly major facilities, some of which could be considered as “significant or signature structures” in the cities where they are located, implemented strict access controls 24 hours per day, seven days per week. Such controls include the following:

- Not permitting public parking in under-building or subterranean parking garages, parking being restricted to tenants and building users who have preauthorization (for some sensitive facilities, a background check is required of such drivers before permission is granted).
- Asking vehicle drivers, who do not have an electronic access card that enables them to enter building parking garages, to state their destination within the building to a security officer or a parking attendant and then be directed to a valet parking service.
- Checking passenger vehicles, particularly those accessing underbuilding parking garages, for suspected bombs as they enter. For high-risk facilities such inspections might include the use of security or parking personnel inspecting vehicles (including their trunks and boots), or using a small hand-held mirror or a small CCTV camera attached to a 3- to 4-foot (0.91 to 1.21 meters) long metal pole to inspect under vehicles, undervehicle scanning systems, and the use of explosive trace detectors or explosives-detection trained (bomb-sniffing) dogs.
- Requiring vehicles, particularly vans and trucks, to undergo on-street inspections, before entering loading dock/shipping and receiving areas. For high-risk facilities, inspections include procedures such as performing X-rays of entire vehicles, using undervehicle scanning systems and explosive trace detectors or explosives-detection trained (bomb-sniffing) dogs.

Visually inspecting delivery vehicles and checking their manifests before their entry to loading docks. Keeping loading dock doors and gates closed between deliveries and pickups. Installing retractable bollards at loading dock entrances and lowering them to permit an authorized vehicle to enter.

Installing optical turnstiles in building main lobbies to screen persons before granting them access to building elevators.

Placing passenger elevators on card access and requiring tenants to use electronic access cards to gain access to their floors.

Security personnel in building lobby reception areas asking visitors for photo identification (including, in some buildings, establishing a separate visitor center for processing visitors) before signing them in, giving them a temporary identification badge or access card, and permitting their entry. Also, in some buildings, to save time, the process includes giving tenants prior authorization (in the form of a letter, a memorandum, an e-mail, or by using a web-based visitor management software system\(^*\)). In others, building security staff telephone the tenant to request permission for the person to enter; then either the tenant or building security escorts the visitor to the tenant, or building security “cards up” (using an electronic access card to select the floor that the person is authorized to access) the visitor in an elevator to the floor that the person is authorized to visit.

Asking couriers and delivery persons for photo identification, and the tenant giving authorization before the person is provided by building security a temporary access badge and permitted to perform the delivery. (In some buildings, security staff retains the photo identification document of the person until the person is about to exit the facility and may even video or photograph the person being granted entry. In other buildings, security staff, or a courier company with messengers dedicated to the building, is responsible for delivering and picking up items for the tenants on behalf of outside courier and delivery services.)

Some landmark buildings are using metal detectors and X-ray machines, explosives trace detectors or explosives-detection trained (bomb-sniffing) dogs, to screen for weapons and explosive devices concealed on people or in items they carry.

In addition, some buildings have implemented the following measures:

- Prohibiting parking of vehicles close to the building, including enforcement of no-stopping zones of vehicles on streets and driveways adjacent to the building (sometimes requesting permission from the local city authority so that security personnel are authorized to write parking violation tickets) and eliminating taxi stands.
- Establishing an adequate stand-off distance of buildings from vehicles using fountains, sculpture, boulders, stairs, embankments, park benches, concrete planters, concrete barricades, and bollards.
- Installing CCTV cameras, with video motion detector capabilities to view a building’s perimeter and neighboring streets and positioning cameras at building parking garage entrances and exits to record closeup images of the driver and the license plate of every vehicle entering and the license plate of all vehicles exiting these areas (if an incident occurs, this can help to identify vehicles that may

---

\(^*\)Visitor management software is a password-protected, web-based management system that permits authorized users of the system to preregister visitors online before they arrive at a building.
have been involved; also, optical recognition software can be used for real-time recognition of license plates).

- Applying security window film on lower floor glass windows; installing bomb blast curtains in building lobbies; providing blast-resistant trash or garbage receptacles; strengthening exposed building support columns in areas such as pedestrian lobbies and loading docks by wrapping them with layers of bomb-blast protective material.
- Increasing security staffing to implement additional security measures, including increasing building perimeter patrols and providing a more visible security presence.
- Deploying undercover police officers and armed plainclothes civilians.

In addition, the design and construction of high-rise buildings, including their ability to withstand explosions, is under close scrutiny. The nature of subsequent events that occur in society will determine the permanency and pervasiveness of many of these aforementioned measures.

Fire Life Safety of Modern Steel-Framed High-Rise Office Buildings

The following features often distinguish third-generation buildings built since World War II:

- Skin-type curtain walls that do not support any of the weight of the building are usually found on the outside of core construction high-rises. “They are like a shower curtain—designed to keep the rain out. These curtain walls are usually glass and stone cladding supported on the structure by lightweight metal frames. Skin-type refers to a continuous wall that covers the surface like skin on a body.”

  In pre-1945 buildings, “exterior walls were of masonry construction.”

- Modern buildings make much greater use of exterior glass and therefore, if a bomb is detonated in or around these buildings, unless glazing protection is provided there is an increased chance of casualties and injuries caused by flying glass.

- Curtain walls of core construction high-rises are attached to the exterior wall columns, sometimes creating an empty space (of width varying from 6 to 12 inches, or 0.15 to 0.30 meters) between the interior of these walls and the outer edges of the floors. If there is such a gap, it is usually filled with fire-resistant material to restrict the vertical spread of fire. However, according to Brannigan and Brannigan (1995), “the reliability of much perimeter firestopping is open to serious question.” In pre-1945 buildings “exterior walls were substantially tied to all floors.”

---

*Three generations of high-rise buildings are described in Chapter 1. Third-generation buildings are those structures built after 1945. Of these, there are those of steel-framed construction (core construction and tube construction), reinforced concrete construction, and steel-framed reinforced concrete construction. This discussion focuses on steel-framed high-rise buildings.

24 Gorman M, Structural Engineer, URS Corporation. Comments to the author in an e-mail regarding the core and tube construction of high-rises (Los Angeles, CA; March 2002).


Suspended or drop-down ceilings, the most common type of ceiling in high-rise office buildings, create a concealed or interstitial space that often extends throughout an entire floor area. Apart from mandatory firewalls extending from a base floor slab to the floor slab of the floor above, and in restrooms and corridors where fire-rated plasterboard ceilings are used for fire protection, these ceilings lack firestopping material. This uninterrupted space is about 30 inches (0.76 meters) in depth and consists of noncombustible acoustical ceiling tiles that are supported in a metal grid hung on metal hangers attached to the floor above. It often is used to house electrical, plumbing, and air ducting systems, as well as cables, telecommunications wiring, and conduits for each floor (Figure 2–2).


*Interstitial space is the space between the suspended or drop-down ceiling and the floor slab above or, in some buildings, below a raised floor. Previously only found in computer data centers where underfloor power and data cabling is run, some modern office buildings now have raised floors that house electrical, plumbing, and air-conditioning systems, as well as cables, telephone wiring conduits, and computer wiring. “Hotels are one [type of] building that often do not have a suspended ceiling—the concrete floor slab above is the ceiling below and all the electrical is cast in the slab” (Gorman, M, Structural Engineer, URS Corporation. Comments to the author in an e-mail regarding the core and tube construction of high-rises. Los Angeles, CA; March 2002).

**A restroom is “a room or suite of rooms in a public or semipublic building or a business establishment provided with lavatory, toilet and other facilities for clients’, visitors’, employees rest or comfort.” (Webster’s Third New International Dictionary, Springfield, MA: Merriam-Webster, Incorporated; 1993).

***Fire protection means the “materials, measures, and practices for preventing fire or for minimizing the probable loss of life or property resulting from a fire, by proper design and construction of buildings, by the use of detection and extinguishing systems, by the establishment of adequate fire fighting services, and by the training of building occupants in fire safety and evacuation procedures” (Answers.com. <www.answers.com/topic/fire-protection?cat=technology>; June 19, 2008).
In some buildings it is also used as a return plenum for the HVAC systems. “Plenum type ceilings are generally not found in pre-1945 buildings.”

- Floor beams and girders are often covered with corrugated steel panels or plates and are then covered with a layer of concrete to form the floor itself. “The floors in most of the high-rise buildings erected since the sixties are much lighter in weight than the floors in the older buildings. In a typical high-rise office floor, three to four inches [0.07 to 0.10 meters] of concrete covers a corrugated-steel deck, whose weight is supported by I-beams or, in the case of the [WTC] Twin Towers, by long ‘trusses’—lightweight strips of steel that are braced by crosshatched webs of square or cylindrical bars, creating a hollow space below each floor surface. This space allows builders to install heating and cooling ducts within the floors, rather than in a drop [suspended] ceiling below them—an innovation that means the developer can increase the number of floors in the entire building.”

- Fireproofing insulation is sprayed directly onto steel columns, floor beams, and girders to protect these structural members from distortion due to heat. It is applied in accordance with the requirements of the local building code. If the insulation is not correctly applied (for example, if the steel is rusted and the surface has not been properly prepared or if the insulation has not been applied at the specified thickness or density) or if the insulation has been dislodged during construction or high winds, heating an exposed steel floor beam to high temperatures can cause vertical deflection (because the secured beam has no space to move horizontally when it elongates) and failure of the connection used to secure the beam to other beams or to the main girders. In pre-1945 buildings, “structural steel components were encased in concrete.”

- Multiple stairwells provide primary and secondary means of egress and are often equipped with automatic stairshaft pressurization and smoke evacuation systems.

---

*The plenum is “a separate space provided for air circulation for heating, ventilation, and air-conditioning and typically provided in the space between the structural ceiling and a drop-down ceiling. A plenum may also be under a raised floor. In buildings with computer installations, the plenum space is often used to house connecting communication cables” (SearchDataCenter.com Definition by Lomas TE, February 1, 2005), <http://searchdatacenter.techtarget.com/sDefinition/0,,sid80_gci213716,00.html>; August 14, 2008).


**Unlike the earlier generation of skyscrapers, which used concrete and masonry to protect the structural steel, many of the newer buildings employed sheetrock [gypsum plasterboard between paper sheets] and spray-on fire protection. The spray-on protection generally consisted of either a cement-like material that resembles plaster or a mineral-fibre spray, such as the one used to protect the floor joists in the World Trade Center. Ibid.


***In the United States, according to NFPA 101, Life Safety Code, “Two means of egress, as a minimum, shall be provided in every building or structure, section, and area where size, occupancy, and arrangement endanger occupants attempting to use a single means of egress that is blocked by fire or smoke. The two means of egress shall be arranged to minimize the possibility that both might be rendered impassable by the same emergency condition” (NFPA Section 4.5.3.1, NFPA International, Quincy, MA. 2000 ed., Fundamental Requirements).
Because these stairwells are located in the central core area, they are less distant from each other than those in pre–World War II buildings in which “stairways were remote from each other, located at the opposite ends of the building.”

- Stair and elevator shaft openings are equipped with protective assemblies and horizontal openings are protected.
- Floor areas tend to be larger and generally open-plan design, with little compartmentation using floor-to-ceiling walls and barriers. Aluminum-framed, cloth-covered foam partitioning is often used to construct cubicles to be used as individual offices. This partitioning is cheaper than the hardwood partitioning used in the past, and it is just as effective as a sound barrier. However, it is more combustible. Pre-1945 buildings were “well compartmented with slab to slab partitions of at least 2 hour fire rating.”

- The number of occupants usually tends to be high in office buildings, resulting in a high concentration of property and hence high fire or fuel load. Much of this property (in office buildings it includes office supplies, plastic wastepaper baskets, files, paper, and the personal computer systems that now equip most workstations) is made of synthetic materials that are flammable and, in a fire, produce toxic gases. As Bathurst wrote, “Over the past several years, there have been many changes in the furnishings put into [office] buildings. At one time, desks and chairs were routinely made of wood. Then metal became popular. Now, any combination of wood, metal, thermoplastics, and foamed plastics can be found. In addition, the increased use of computers has also added to the fuel load.” To mitigate this threat to life safety, office furniture and interior furnishings in all offices, conference and waiting rooms, and reception and assembly areas should be of fire-resistive quality and treated to reduce combustibility.

- Heating and air-conditioning is usually by a central HVAC system that serves multiple floors. Pre-1945 buildings are “usually not centrally air conditioned… normally [they are] steam heated.”

- There is the potential during fires for the stack effect described earlier in this chapter. Brannigan noted of pre-World War II buildings: “Windows could be opened in buildings of this era. This provided local ventilation and relief from smoke migrating from the fire. The windows leaked, often like sieves, therefore there was no substantial stack effect.”

---

33 ibid., p. 5–17.
provide some resistance to heat and are often made of tempered safety glass; they usually cannot be opened (although many residential and apartment buildings have openable windows and doors that serve as balconies) and are well insulated. “No manual fire-fighting techniques are known to counter stack effect or to mitigate its effect during a fire. Stack effect cannot be eliminated because of the temperature differential [that exists between areas] and building height. As a result, potential stack effect will exist and may vary with climatic conditions. The only way to mitigate the potential of stack effect is to design and construct the building to minimize the effect.”

- Automatic fire detection systems and automatic fire suppression systems are often incorporated into building design. As Brannigan and Brannigan stated:

Most new high-rise office buildings are sprinklered. The huge losses suffered in such fires as Philadelphia’s One Meridian Plaza and Los Angeles’ First Interstate Tower [First Interstate Bank Building] leave little room for argument. But there is still much opposition to any requirement for retroactive installation of sprinklers in existing buildings. While much of the opposition is financial, the specious argument that such requirements are unconstitutional has found some favor. This argument is without merit with respect to United States law. Much of the cost, particularly of a retroactive installation, is caused by hiding the sprinkler system. If the argument of overall sprinkler cost is an issue, the opposing argument is that safety requires only the cost of a bare bones system. Aesthetic costs such as hiding the sprinklers and the piping are the option[s] of the owner, not a fire protection requirement.

Are Modern Steel-Framed High-Rises Less Fire Resistant Than Previous Generation Buildings?

Both Francis L. Brannigan, in Building Construction for the Fire Service, and John T. O’Hagan, in High-Rise/Fire and Life Safety, put forth the opinion that modern high-rise steel-framed buildings are less fire resistive than those of the previous generation.

Brannigan defined a fire-resistive building as one “that to some degree will resist fire-caused collapse.” He further defined the limits of fire resistance by stating, “Fire resistance is intended to provide, within limits, resistance to collapse by structural members and floors, and resistance to the passage of fire through floors and horizontal barriers.” He went on to say that buildings built after World War II

---

* The terms fire resistance and fire resistive appear to have similar meanings.
have poorer fire protection features than the previous [second•] generation of buildings built before World War II.\textsuperscript{41} He asserted that modern high-rise buildings are lighter than previous generation high-rises, “The Empire State Building [a second-generation steel building] weighs about 23 pounds [10.4 kilograms] per cubic foot. A typical modern high-rise weighs approximately eight pounds [3.6 kilograms] per cubic foot.”\textsuperscript{42} He also stated, “The development of fluorescent lights and air conditioning helped to remove limits to the floor area. Thus, building populations could be enormously increased. As a result, many floors have substantial areas beyond the reach of hand hose streams.”\textsuperscript{43}

O’Hagan\textsuperscript{44} wrote that modern steel-framed high-rise buildings,

- Due to their lightweight kind of construction are less fire resistive than the previous generation
- Have greater potential for bigger fires because of their open-floor design
- Have greater heat retention due to better insulation

O’Hagan also expressed concern about the effectiveness of firestopping material located between the inner edge of the curtain wall and the outer edge of each floor, the effectiveness of spray-on insulation, and the presence of return plenums for HVAC systems that can quicken lateral fire spread.\textsuperscript{••}

Add to these factors the greater fuel loads caused by a higher concentration of business and personal property, and it appears that modern steel-framed high-rise office buildings may be higher-risk occupancies than those of previous generations. The destruction of the World Trade Center has added considerable weight to the arguments put forth by Brannigan and O’Hagan.

John Seabrook, writing in \textit{The New Yorker}, noted that,

\textit{One indication that older high-rise buildings may be more fire-resistant than the newer high-rise buildings is the performance of the twenty-three-story building at 90 West Street—a Cass Gilbert-designed building, finished in 1907 (Gilbert also designed the Woolworth Building), whose structure was protected by concrete and masonry—compared with the performance of 7 World Trade Center, an all-steel building, from the nineteen-eighties, that had spray-on fire protection. Both buildings were completely gutted by fires

\textsuperscript{•}The late John T. O’Hagan, former fire commissioner and chief of the New York City Fire Department, in \textit{High Rise/Fire and Life Safety} (O’Hagan, 1977, pp. 145, 146), described three generations of high-rise buildings in the United States. The second generation appears to be similar to those buildings referred to by Brannigan in \textit{Building Construction for the Fire Service}. 2nd ed.


\textsuperscript{42}ibid., p. 462.

\textsuperscript{43}ibid., p. 462.


on September 11th, but 90 West Street is still standing, and may eventually be restored. 7 World Trade, which had a gas main beneath it, collapsed after burning for seven hours.45

New York World Trade Center of Investigation

The National Institute of Standards and Technology (NIST) investigation of the collapse of World Trade Center Building 746 revealed the following:

World Trade Center Building (WTC 7)

WTC 7 was a 47 story office building located immediately to the north of the main WTC Complex. It had been built on top of an existing Consolidated Edison of New York electric power substation, which was located on land owned by The Port Authority of New York and New Jersey. On September 11, 2001, WTC 7 endured fires for almost seven hours, from the time of the collapse of the north WTC tower (WTC 1) at 10:28:22 a.m. until 5:20:52 p.m., when WTC 7 collapsed. This was the first known instance of the total collapse of a tall building primarily due to fires.

WTC 7 was unlike the WTC towers in many respects. It was a more typical tall building in the design of its structural system. It was not struck by an airplane. The fires in WTC 7 were quite different from those in the towers. Since WTC 7 was not doused with thousands of gallons of jet fuel, large areas of any floor were not ignited simultaneously. Instead, the fires in WTC 7 were similar to those that have occurred in several tall buildings where the automatic sprinklers did not function or were not present. These other buildings did not collapse, while WTC 7 succumbed to its fires.46

Principal Findings of the Investigation

The fires in WTC 7 were ignited as a result of the impact of debris from the collapse of WTC 1, which was approximately 370 ft [113 meters] to the south. The debris also caused some structural damage to the southwest perimeter of WTC 7. The fires were ignited on at least 10 floors; however, only the fires on Floors 7 through 9 and 11 through 13 grew and lasted until


*Addressing this observation, the report states that “WTC 7 collapsed due to uncontrolled fires with characteristics similar to previous fires in tall buildings. The fires in WTC 7 were similar to those that have occurred previously in several tall buildings (One New York Plaza, 1970, First Interstate Bank, 1988, and One Meridian Plaza, 1991) where the automatic sprinklers did not function or were not present. However, because of differences between their structural designs and that of WTC 7, these three buildings did not collapse” (NIST NCSTAR 1A Federal Building and Fire Safety Investigation of the World Trade Center Disaster. Final Report on the Collapse of World Trade Center Building 7. National Institute of Standards and Technology; August 2008:46).
the time of the building collapse. These uncontrolled fires had characteristics similar to those that have occurred previously in tall buildings. Their growth and spread were consistent with ordinary building contents fires. Had a water supply for the automatic sprinkler system been available and had the sprinkler system operated as designed, it is likely that fires in WTC 7 would have been controlled and the collapse prevented. However, the collapse of WTC 7 highlights the importance of designing fire-resistant structures for situations where sprinklers are not present, do not function (e.g., due to disconnected or impaired water supply), or are overwhelmed.

Eventually, the fires reached the northeast of the building. The probable collapse sequence that caused the global collapse of WTC 7 was initiated by the buckling of a critical interior column in that vicinity. This column had become unsupported over nine stories after initial local fire-induced damage led to a cascade of local floor failures. The buckling of this column led to a vertical progression of floor failures up to the roof and to the buckling of adjacent interior columns to the south of the critical column. An east-to-west horizontal progression of interior column buckling followed, due to loss of lateral support to adjacent columns, forces exerted by falling debris, and load redistribution from other buckled columns. The exterior columns then buckled as the failed building core moved downward, redistributing its loads to the exterior columns. Global collapse occurred as the entire building above the buckled region moved downward as a single unit. This was a fire-induced progressive collapse, also known as disproportionate collapse, which is defined as the spread of local damage, from an initiating event, from element to element, eventually resulting in the collapse of an entire structure or a disproportionately large part of it.

Factors contributing to the building failure were: thermal expansion occurring at temperatures hundreds of degrees below those typically considered in design practice for establishing structural fire resistance ratings; significant magnification of thermal expansion effects due to the long-span floors, which are common in office buildings in widespread use; connections that were designed to resist gravity loads, but not thermally induced lateral loads; and a structural system that was not designed to prevent fire-induced progressive collapse.

Within the building were emergency electric power generators, whose fuel supply tanks lay in and under the building. However, fuel oil fires did not play a role in the collapse of WTC 7.

Hypothetical blast events did not play a role in the collapse of WTC 7. NIST concluded that blast events did not occur, and found no evidence whose explanation required invocation of a blast event.

There were no serious injuries or fatalities, because the estimated 4,000 occupants of WTC 7 reacted to the airplane impacts on the two WTC towers and began evacuating before there was significant damage to WTC 7. The occupants were able to use both the elevators and the stairs, which were as yet not damaged, obstructed, or smoke-filled. Evacuation of the building took just over an hour. The potential for injuries to people leaving the building was mitigated by building management personnel holding the occupants in the lobby until they identified an exit path that was safe from the debris falling
from WTC 1. The decision not to continue evaluating the building and not to fight the fires was made hours before the building collapsed, so no emergency responders were in or near the building when the collapse occurred.

Recommendations

Based on the findings of this Investigation, NIST identified one new recommendation (B, below) and reiterated 12 recommendations from the Investigation of the WTC towers. These encompass increased structural integrity, enhanced fire endurance of structures, new methods for fire resistant design of structures, improved active fire protection, improved emergency response, improved procedures and practices, and education and training. [The NIST WTC Towers recommendations are addressed in the next chapter.]

The urgency of these recommendations is substantially reinforced by their pertinence to the collapse of a tall building that was based on a structural system design that is in widespread use.

The partial or total collapse of a building due to fires is an infrequent event. This is particularly true for buildings with a reliably operating active fire protection system such as an automatic fire sprinkler system. A properly designed and operating automatic sprinkler system will contain fires while they are small and, in most instances, prevent them from growing and spreading to threaten structural integrity.

The intent of current practice, based on prescriptive standards and codes, is to achieve life safety, not collapse prevention. However, the key premise of NIST’s recommendations is that buildings should not collapse in infrequent (worst-case) fires that may occur when active fire protection systems are rendered ineffective, e.g., when sprinklers do not exist, are not functional, or are overwhelmed by the fire, or where the water supply is impaired.

Fire scenarios for structural design based on single compartment or single floor fires are not appropriate representations of infrequent fire events. Such events have occurred in several tall buildings resulting in unexpected substantial losses. Instead, historical data suggests that infrequent fires which should be considered in structural design have characteristics that include: ordinary combustibles and combustible load levels, local fire origin on any given floor, no widespread use of accelerants, consecutive fire spread from combustible to combustible, fire-induced window breakage providing ventilation for continued fire spread and accelerated fire growth, concurrent fires on multiple floors, and active fire protection systems rendered ineffective. The fires in WTC 7 had all of these characteristics.

The subjects of the NIST recommendations are as follows:

A. Development of methods for prevention of progressive collapse and for reliable prediction of the potential for complex failures in structural systems subjected to multiple hazards.

B. (New). Explicit evaluation of the fire resistance of structural systems in buildings under worst-case design fires with any active fire protection systems rendered ineffective. Of particular concern are the effects of
thermal expansion in buildings with one or more of the following features: long-span floor systems, connections not designed for thermal effects, asymmetric floor framing, and composite floor systems.

C. Evaluation and improvement of the technical basis for determining appropriate construction classification and fire rating requirements (especially for tall buildings), and making of related code changes.

D. Improvement of the technical basis for the standard for fire resistance testing of components, assemblies, and systems.

E. Broadening the scope of the “structural frame” approach to fire resistance ratings by including, as part of the structural frame, floor systems and other bracing members that are essential to the vertical stability of the building under gravity loads.

F. Enhancement of the fire resistance of structures by requiring a performance objective that uncontrolled building fires result in burnout without partial or global (total) collapse.

G. Development of performance-based standards and code provisions to enable the design and retrofit of structures to resist real building fire conditions, and the tools necessary to perform the building evaluations.

H. Enhancement of the performance and redundancy of active fire protection systems to accommodate higher risk buildings.

I. Establishment and implementation of codes and protocols for ensuring effective and uninterrupted operation of the command and control system for large-scale building emergencies.

J. Requirement that building owners retain building documents over the entire life of the building.

K. Inclusion of all appropriate technical professionals in the building design team.

L. Development and implementation of continuing education curricula for training building professionals in each others’ skills and practices.

M. Development and delivery of training materials in the use of computational fire dynamics and thermostructural analysis tools.

Building owners, operators, and designers should immediately act upon the new recommendation (B). Industry should also partner with the research community to fill critical gaps in knowledge about how structures perform in real fires.

The preceding discussion focused on modern steel-framed high-rise buildings, it is of note that O’Hagan also suggested in his book, *High Rise/Fire and Life Safety*, that high-rise residential building fires, including those in hotel rooms, to some extent are different in nature and not as severe as fires in high-rise office buildings. Three of his stated reasons for this are (1) high-rise residential buildings are typically of masonry construction and lack the empty spaces between the interior of their exterior walls and the outer edges of their floors (that typify the curtain walls of steel-framed core

---

*Typical floor span lengths in tall office buildings range from 12 m to 15 m (40 ft to 50 ft); this range is considered to represent long-span floor systems. Thermal effects (e.g., thermal expansion) that may be significant in long-span buildings may also be present in buildings with shorter span lengths, depending on the design of the structural system.*
construction] buildings); (2) they do not have common ceiling plenums [which, as mentioned previously, lack fire stopping material]; and (3) for privacy and usage reasons, residential buildings are typically compartmentalized with walls and partitions that have adequate fire resistance to withstand the fire until the arrival of the fire department, and as a result individual fires are considerably smaller in area.47

Fire Risk in High-Rise Buildings

Fire is an ever-present risk in buildings. In discussing fire risk* in high-rise buildings, it is helpful to analyze fire incident data** for the four property classes—office buildings, hotels and motels,*** apartment buildings, and hospitals (and other facilities that care for the sick)—that account for the majority of high-rise building fires.48 Even though these data pertain only to the United States, the information is worth considering because it includes three of the types of commercial buildings that are addressed in this book (namely, office, hotel, and residential and apartment buildings).

A study by Dr. John Hall, Jr., of the National Fire Protection Association’s (NFPA) Fire Analysis and Research Division, using statistics from the U.S. Fire Administration’s National Fire Incident Reporting System (NFIRS), stated that from 1987 to 1991, office buildings, hotels and motels, apartment buildings, and facilities that care for the sick averaged 13,800 high-rise building fires per year and associated annual losses of 74 civilian deaths, nearly 720 civilian injuries, and $79 million in direct property damage. However, “most high-rise building fires and associated losses occur in apartment buildings.”49 Dr. Hall added that for this period:

Only a small share of high-rise building fires spread beyond the room of origin, let alone the floor of origin.

In high-rise buildings [office buildings and hotels and motels], electrical distribution system fires rank first in causes of fire-related property damage.50

The most recent published study by Dr. Hall shows that “in 2002,**** high-rise buildings in these four property classes combined had 7,300 reported structure fires and associated

**“Tracking of the fire experience in [U.S.] high-rise buildings, however, has been less than systematic because the nationally representative fire incident data bases did not originally include reporting of height of structure. Reasonably good reporting began with 1985 fires…. NFPA and other analysts have long used lists of particularly memorable incidents to study the high-rise fire problem, but these and other available special data bases are heavily weighed towards larger and more severe incidents” (Hall Jr JR. High-Rise Building Fires. Quincy, MA: National Fire Protection Association; September 2001:1).
***“The term ‘motel’ is a general designation for lodging establishments that specialize in attracting the motoring public by offering parking accommodations. The distinctions between hotels and motels are gradually disappearing, however” (Beaudry MH. Contemporary Lodging Security. Newton, MA: Butterworth-Heinemann; 1996:ix).
50 Ibid., p. 53.
****2002 is the most recent year for which data was available for this report.
losses of 15 civilian deaths, 300 civilian injuries, and $26 million in direct property damage. From these statistics Dr. Hall concluded that “these statistics generally show a declining fire problem over the nearly two decades covered” and, similar to his previous findings, “most high-rise building fires and associated losses occur in apartment buildings.” He further commented pertaining to the latter, “this may seem surprising, but it shouldn’t. Homes dominate the U.S. fire problem so completely that it is always a good bet that any newly examined fire problem, unless it is one that cannot occur in homes, will have its largest share in homes.” However, Hall did caution that, due to a number of factors (one being lower participation in national fire incident reporting in recent years) “the patterns shown in data available so far should be given limited weight.”

Other Fire Life Safety Features

Despite the opinions put forth by both Francis L. Brannigan, in *Building Construction for the Fire Service*, and John T. O’Hagan, in *High-Rise/Fire and Life Safety* (that modern steel-framed high-rise buildings are less fire resistive than those of the previous generation), from a life safety standpoint the picture may be different. Modern buildings that have properly designed, installed, operated, tested, and maintained automatic fire detection and suppression systems, and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes, and automatic smoke control systems to restrict the spread of smoke—do have the necessary early warning systems to quickly detect fires and warn occupants of their presence and the necessary automated sprinkler systems to quickly extinguish a fire in its early stages.

Fire detection systems trace their origin to the mid-19th century. Since then, the performance and reliability of “a number of mechanical, electrical, and electronic devices [that] have been developed to mimic human senses in detecting the environmental changes created by fire” have constantly improved.

Also, “since they were introduced in the latter part of the 19th century, the performance and reliability of automatic sprinklers have been improved continually through experience and the efforts of manufacturers and testing organizations.”

One of the key issues here is the presence or absence of sprinklers. The probability of a serious fire in any given office building or other building with many occupants is extremely low. It is also a fact, however, that in the typical unsprinkled glass-enclosed office building with interior stairways

---

52 Ibid., p. 3.
53 Ibid., p. 4.
54 Ibid., p. 4.
55 Ibid., p. 3.
56 Ibid., p. 4.

*Unsprinkled* means the absence of a sprinkler system. Also known as *nonsprinkled*. 
and a substantial fire load, the consequences of a serious fire during working hours could be very severe—with multiple fatalities.  

In the study mentioned in the previous section on “Fire Risk in High-Rise Buildings,” Dr. Hall commented on fire protection features in high-rise buildings:

In several instances, the value of these fire protection features [i.e., automatic extinguishing systems (primarily sprinklers), fire detection equipment, and fire-resistant construction] may be seen clearly in a statistical analysis of 1994–1998 loss per fire averages, with and without the protection. For high-rise buildings, automatic extinguishing systems are associated with a reduction of at least 88% in the rate of deaths per 1,000 fires for each of the three property classes (excluding office buildings, which had no deaths recorded in NFIRS in high-rise buildings) and at least 44% in the average dollar loss per fire for each of the four property classes. Fire detection equipment is associated with a reduction of 55% in the rate of deaths per 1,000 fires in apartment buildings. Fire-resistant construction is associated with a reduction of 30% in average dollar loss per fire in apartment buildings. This probably is produced not directly by the construction but indirectly by the compartmentation features that tend to be used with fire-resistant construction, features that keep more fires smaller and so keep property losses lower. (Note, though, that compartmentation practices probably vary more by type of occupancy than by type of construction.) Because high-rise buildings often use all three systems, it is very difficult to try to separate their effects on loss rates, and many rates are very sensitive to deaths or large dollar loss in individual incidents.

Automatic extinguishing systems and fire detection equipment and the compartmentation features associated with fire-resistant construction all contribute to fire protection by helping to keep fires small, with extinguishing and construction doing so directly and detection doing so by providing early warning that can lead to earlier manual suppression....

Finally, the effectiveness of these fire protection systems and features and their widespread use in high-rise buildings mean that when people are killed in high-rise residential fires, they are much more likely to have been close to the fire, where it is more likely that fatal injury could occur before [the] fire could be stopped or blocked by these systems and features.  

Emergency Planning Essential

In modern high-rise buildings, special fire protection requirements (automatic sprinklers, detection and alarm systems, and compartmentation features associated with fire-resistant construction) are reflected in strict laws, codes, and standards. These special requirements, although they are designed to provide sufficient time for occupants to escape, are not in themselves sufficient: The life safety of occupants also depends critically on how ready people are to react appropriately at the time of an incident. If building management has

---


provided a sound fire life safety program, then a building can be considered well-prepared. A sound fire life safety program will assist all building staff and occupants to be in a constant state of readiness to react to an emergency, particularly one that involves fire, in a way that will help provide for everyone’s safety.

Impact of New York World Trade Center Terrorist Attacks on Building Safety

Before leaving the subject of the fire safety of modern high-rise buildings, it is appropriate to discuss the impact on building safety of the February 26, 1993, and the September 11, 2001, terrorist attacks on the Twin Towers of the New York World Trade Center. (The incidents are detailed in Chapter 3.)

February 26, 1993, Bombing

As a result of the 1993 bombing in the subterranean parking garage of the World Trade Center (WTC), improvements to the evacuation plan for the towers included the following measures:

- Providing four levels of power—the primary power source, emergency diesel generators, battery backups, and backup power from the state of New Jersey—to provide power to the command centers, one freight elevator in each building, emergency radios, and emergency lighting.\(^{61}\)
- Installing battery backup lighting systems on emergency exit stairwell landings at every second floor,\(^{62}\) “in elevator lobbies, and all elevator cabs.”\(^{63}\)
- Installing phosphorescent (photoluminescent) exit signs to guide the way to floor entry doors in the emergency exit stairwells and phosphorescent (photoluminescent) tape-paint on all stairwell stair treads, hand rails, and the perimeters of doorways, as a backup to primary and emergency lighting in the stairwells.\(^{64}\)
- Adding “bright [directional] arrows to guide people along corridors to stairway connections.”\(^{65}\)
- Providing, in case of an emergency, duplicate security command and operation centers to run the WTC security systems.\(^{66}\)
- Retrofitting the fire system with new fire protection devices such as smoke detectors, strobe lights in public and tenant spaces, a new public address system (that reached beyond common area hallways into office areas), new floor warden telephones, and fully sprinklering the retail mall.\(^{67}\)

---

\(^{61}\)Towering Team Leader. Atlanta, GA: Access Control & Security Systems; September 2000:44.


\(^{64}\)ibid.

\(^{65}\)For many on September 11, survival was no accident” (USA Today. December 20, 2001), authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix 1V” conducted in San Francisco by Mark Schofield and Douglas P. Forsman (March 6, 2002:4).


\(^{67}\)Litwak D. Keeping the Twins Safe. Security Technology & Design: Cumming, GA; October 1999:57.
Giving every disabled or mobility-impaired person an evacuation chair that could accommodate the person when carried by two others.  

Providing well-planned and executed fire life safety training of all building occupants, particularly in emergency evacuation procedures (this included, “Appointment of Fire Wardens, specially trained and equipped with flashlights, whistles, and identifying hats”) and conducting semiannual fire drills in conjunction with the Fire Department of the city of New York.

A consequence of the 1993 bombing was that system designers of mega-high-rise buildings gave renewed attention to providing zoning and redundancy of life safety systems, so that if one portion of a building was destroyed, critical life safety systems would not fail in the entire building. For example, emergency and standby electrical power, emergency lighting, fire suppression, and mechanical smoke evacuation systems could be zoned so that their controls are not isolated to one particular area of the building.

September 11, 2001, Catastrophe

The collapse of the World Trade Center towers caused much concern among owners, developers, architects, engineers, code officials, and firefighters regarding the safety of high-rise buildings and their vulnerability to such hostile acts. In the light of the collapse of the Twin Towers and considering the aforementioned discussion of “Modern High-Rises Are Less Fire-Resistive,” one could argue that had the towers been more fire resistive and able to remain standing longer, then fewer people would have died.

As reported in The New Yorker, Guy Nordenson, a New York structural engineer and a Princeton professor, wrote a letter to the Times, “praising the towers’ structural

---

68 For many on September 11, survival was no accident” (USA Today. December 20, 2001), authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix 1V” conducted in San Francisco by Mark Schofield and Douglas P. Forsman (March 6, 2002:4).


---

In the city of New York, fire codes for office buildings require that “Fire drills shall be conducted, in accordance with the Fire Safety Plan, at least once every three months for existing buildings during the first two years after the effective date of these rules, or for new buildings during the first two years after the issuance of the certificate of occupancy. Thereafter, fire drills shall be conducted at least every six months” (RCNY 1625, 6-30-91, 6-01, “Fire drill and evacuation in office buildings and buildings classified as occupancy group E (Business), (d)” Drills (10), New York). A drill is defined by the NFPA Glossary of Terms, National Fire Code as “An exercise involving a credible simulated emergency that requires personnel to perform emergency response operations for the purpose of evaluating the effectiveness of the training and education programs and the competence of personnel in performing required response duties and functions” (National Fire Protection Association, Quincy, MA; 2005). A fire drill is such an exercise for a simulated fire emergency.


** A mega-high-rise building is defined by the NFPA Fire Investigation Report on the 1993 New York World Trade Center Bombing (Isner MS, Klem TJ. Discussion. Fire Investigation Report, World Trade Center Explosion and Fire. Quincy, MA: National Fire Protection Association; 1993:55) as “a large, tall (greater than 50 stories), densely populated structure where emergency evacuation is difficult or impractical. They are further characterized in that the ordinary fuels which they contain may result in rapid fire growth, development, and spread because of their geometric arrangement, and in extensive smoke spread throughout the structure which threatens occupants in remote areas from the fire origin. Further, the time required for fire fighters to establish effective fire fighting operations can be extensive because of the vertical arrangement of the structure.”
design for keeping them standing as long as they did, and allowing some twenty-five thousand people to escape.” In response, Leslie E. Robertson, the structural engineer who, with his then-partner, John Skilling, was largely responsible for the structure of the Twin Towers, wrote an e-mail to Nordenson that read,

> Your words do much to abate the fire that writhes inside
> It is hard
> But that I had done a bit more …
> Had the towers stood up for just one minute longer …
> It is hard.

A Clear Message

One clear message for all high-rise buildings, whether they are evaluated to be at risk to a terrorist event or not, is that all tenants should be well trained in evacuation procedures. On September 11, in each tower there were people who perished on the floors that sustained the direct impact of the aircraft and those who were inextricably trapped above the crash site because all three stairwells in the north tower, two stairwells in the south tower, and most elevators were made inoperable by the impact, explosions, and ensuing fires. The World Trade Center had a comprehensive, well-executed fire life safety program and emergency plan that helped prepare building emergency staff and occupants to react appropriately to the catastrophic events that unfolded. All indications are that the occupants who were able to evacuate did so in an orderly and competent manner (there is an in-depth treatment of the occupant evacuation in Chapter 3). According to a *USA Today* study,

> The evacuation was a success. Nearly everyone who could get out did get out. The Port Authority had revised its evacuation plan for the buildings after a terrorist bomb exploded in the Trade Center garage in 1993. On September 11, those changes saved hundreds, possibly thousands, of lives. The buildings, sturdily constructed, exquisitely engineered and equipped with stairwells bigger than building codes require, stood just long enough to give potential survivors a chance to get out.

Summary

- The terms *security* and *fire life safety* are synonymous but can be addressed separately for the purposes of systematic analysis and discussion.

---

72 ibid.
73 *USA Today* spent two months finding out precisely what happened in the 1 hour, 42 minutes and 5 seconds from the first jet crash to the last building collapse. The newspaper identified where 95% of the victims worked or were located at the time of the attacks. In addition, it matched floor plans, architectural drawings and photographs to the accounts of survivors and victims” (p. 2). Their findings indicated that, “in each tower, 99% of the occupants below the crash site survived” (p. 1). These findings were published in the article, “For many on Sept. 11, survival was no accident” (*USA Today*. December 20, 2001), authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. These particular quotations were from pages 1 and 2. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix 1V” conducted in San Francisco by Mark Schofield and Douglas P. Forsman (March 6, 2002).
From a security and fire life safety standpoint, high-rise buildings have unique requirements that distinguish them from low-rise buildings.

There are ways that the security and fire safety of modern steel-framed high-rise office buildings differ from earlier generation high-rises.

The February 26, 1993, attack on and the September 11, 2001, destruction of the New York World Trade Center has significantly affected the world of high-rise security and fire life safety.

Key Terms

Building offset. An upper floor is set back from the floors beneath it.\(^{73}\) Sometimes a building offset is referred to as a building setback (or set-back). See setback.

Central business district (or CBD). “The central district of a city, usually typified by a concentration of retail and commercial buildings.”\(^{74}\)

Certificate of occupancy. “Document issued by governmental authority certifying that all or a designated portion of a building complies with the provisions of applicable statutes and regulations, and permitting occupancy for its designated use.”\(^{75}\) Also known as occupancy permit.

Crime. “An act or omission which is in violation of a law forbidding or commanding it for which the possible penalties for an adult upon conviction include incarceration, for which a corporation can be penalized by a fine or forfeit, or for which a juvenile can be adjudged delinquent or transferred to criminal court for prosecution. The basic legal definition of crime is all punishable acts, whatever the nature of the penalty.”\(^{76}\)

Crime analysis. “The study of information about criminal incidents to detect patterns or trends of criminal activity that may be used to predict the need for specific police techniques, such as aggressive patrol of a given geographic area; analysis which seeks to determine what crimes are likely to impact particular targets, the criminals likely to commit the crimes, how the crimes are likely to occur, and when they are likely to occur.”\(^{77}\)

Crime pattern analysis. “A process that encompasses a number of techniques, all of which can assist crime risk management. It is therefore best regarded as a generic term, covering a number of approaches and techniques for analyzing the incidence and distribution of crime.”\(^{78}\)

Cross-over floor. See sky-lobby.

Drill. “An exercise involving a credible simulated emergency that requires personnel to perform emergency response operations for the purpose of evaluating the effectiveness of the training and education programs and the competence of personnel in


\(^{77}\) ibid.


**Fire brigade.** “A group of people organized to engage in rescue, fire suppression, and related activities.”\footnote{Ibid.} Fire brigades are usually public agencies. However, if a facility is large enough it may have a proprietary or an in-house fire brigade.

**Fire drill.** A fire drill is an exercise for a simulated fire emergency. See drill.

**Fire life safety.** Minimizing the possible danger to life and property from various threats, including that of fire. Synonymous terms are fire and life safety, fire safety, and life safety.

**Fire protection.** “Materials, measures, and practices for preventing fire or for minimizing the probable loss of life or property resulting from a fire, by proper design and construction of buildings, by the use of detection and extinguishing systems, by the establishment of adequate fire fighting services, and by the training of building occupants in fire safety and evacuation procedures.”\footnote{Brannigan FL. Building Construction for the Fire Service. 3rd ed. Quincy, MA: National Fire Protection Association; 1992:452.}


**Fire-resistive building.** A building “that to some degree will resist fire-caused collapse.”\footnote{Glossary of Terms. National Fire Code. Quincy, MA: National Fire Protection Association; 2005.}

**Fire watch.** Patrols at appropriate intervals determined by the fire department may be required when a building has exceptional hazards or the fire protection equipment or system is malfunctioning or has been taken out of service. A fire watch is “the assignment of a person or persons to an area for the express purpose of notifying the fire department and/or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety dangers.”\footnote{Ibid.}

**Interstitial space.** The space between the suspended or drop-down ceiling and the floor slab above, or, in some buildings below a raised floor. See also plenum.

**Means of egress.** “A continuous and unobstructed way of travel from any point in a building or structure to a public way consisting of three separate and distinct parts: (1) the exit access, (2) the exit, and (3) the exit discharge.”\footnote{NFPA 101. Life Safety Code Handbook. 10th ed. Quincy, MA: National Fire Protection Association; 2006:31.}

**Mega-high-rise.** “A large, tall (greater than 50 stories), densely populated structure where emergency evacuation is difficult or impractical. They are further characterized in that the ordinary fuels which they contain may result in rapid fire growth, development, and spread because of their geometric arrangement, and in extensive smoke spread throughout the structure which threatens occupants in remote areas from the
fire origin. Further, the time required for fire fighters to establish effective fire fighting operations can be extensive because of the vertical arrangement of the structure.”87

**Occupancy.** “The purpose for which a building or other structure, or part thereof, is used or intended to be used.”88

**Occupancy permit.** See certificate of occupancy.

**Physical security.** “That part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against espionage, sabotage, damage, theft and loss.”89

**Plenum.** “A separate space provided for air circulation for heating, ventilation, and air-conditioning and typically provided in the space between the structural ceiling and a drop-down ceiling. A plenum may also be under a raised floor. In buildings with computer installations, the plenum space is often used to house connecting communication cables.”90 See also **interstitial space.**

**Private security.** The protection of the lives and property of people living and working within the private sector. The primary responsibility for achieving this rests on an individual, the proprietor of a business employing an individual, the owner or agent of the owner of the facility where a business is conducted, or an agent of the aforementioned who specializes in providing protective services.

**Progressive collapse.** “The spread of local damage, from an initiating event, from element to element, eventually resulting in the collapse of an entire structure or a disproportionately large part of it.”91 Also known as **disproportionate collapse.**

**Public security.** The protection of the lives, property, and general welfare of people living in the public community. This protection is largely achieved by the enforcement of laws by police funded by public monies.

**Restroom.** “A room or suite of rooms in a public or semipublic building or a business establishment provided with lavatory [i.e., a washbasin or a washbowl], toilet and other facilities for clients’, visitors’, employees’ rest or comfort.”92

**Safety.** Derived from the Latin word *salvus,* which means “safe.” “The state or quality of being safe; freedom from danger.”93

**Security.** Derived from the Latin word *securus,* which means, “free from danger” or “safe.” “In providing security for specific applications, the purpose of private security may be described as providing protection for materials, equipment, information, personnel, physical facilities, and preventing influences that are undesirable, unauthorized, or detrimental to the goals of the particular organization being secured.”94
Setback (or set-back). “The distance of a structure or other feature from the property line or other feature”\(^{95}\) or the “placing of a face of a building on a line some distance to the rear of the building.”\(^{96}\) Sometimes the latter definition refers to a building offset where an upper floor is set back from the floors beneath it.\(^{97}\) See building offset.

Sky-lobby (or sky lobby). A floor where occupants can cross over from an express elevator to another group of elevators serving local floors. Also known as a cross-over floor.

Smoke. “The total airborne effluent from heating or burning a material.”\(^{98}\)

Threat. “Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.”\(^{99}\)

Unsprinklered. The absence of sprinklers. Also known as nonsprinklered.

Visitor management software. A password-protected, web-based management system that permits authorized users of the system to preregister visitors online before they arrive at a building.

Additional Reading


\(^{96}\)ibid.


There are many security and fire life safety threats that have the potential to cause loss or harm to high-rise buildings and their occupants.

What Is a Threat?

A threat is “any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.” Threats may be intentional, accidental, or natural disasters. Also, some of these may be considered asymmetric in nature.

Security Threats

In the high-rise setting, security threats come in many forms. Threats to people include the following:

- **Aberrant behavior.** Behavior that deviates from the norm, such as that caused by substance (drug or alcohol) abuse, may be a threat to the personal safety of not only the individual exhibiting it, but also to other persons.

- **Assault.** “Any willful attempt or threat to inflict injury upon the person of another, when coupled with an apparent present ability so to do, and any intentional display of force such as would give the victim reason to fear or expect immediate...”

---

---
bodily harm, constitutes an assault. An assault may be committed without actually touching, or striking, or doing bodily harm, to the person of another.”

- **Assault and battery.** “Any unlawful touching of another which is without justification or excuse.”

- **Kidnapping.** “The forcible abduction or stealing and carrying away of a person from own country to another…. A person is guilty of kidnapping if he unlawfully removes another from his place of residence or business … or if he unlawfully confines another for a substantial period in a place of isolation.”

- **Manslaughter.** “The unjustifiable, inexcusable, and intentional killing of a human being without deliberation, premeditation and malice.”

- **Mayhem.** “A type of injury which permanently render[s] the victim less able to fight offensively or defensively; it might be accomplished either by the removal of (dismemberment), or by the disablement of, some bodily member useful in fighting. Today, by statute, permanent disfigurement has been added.”

- **Murder.** “The unlawful killing of a human being by another with malice aforethought, either express or implied.”

- **Robbery.** “Felonious taking of money, personal property, or any other article of value, in the possession of another, from his [or her] person or immediate presence, and against his [or her will], accomplished by means of force or fear.”

- **Sex offenses** (including rape, sexual harassment, and lewd behavior). **Rape** is “unlawful sexual intercourse with a female without her consent.” Under some statutes, this crime may now include intercourse between two males. **Sexual harassment** is “a type of employment discrimination, includes sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature prohibited by … law.” **Lewd behavior** relates to morally impure or wanton conduct, including indecent exposure.

- **Stalking.** “A pattern of repeated, unwanted attention, harassment, and contact.”

- **Suicide.** The taking of one’s own life.

Threats to property and information include the following:

- **Arson.** The malicious burning of another’s house. This definition, however, has been broadened by statutes and criminal codes to include starting a fire or causing an explosion with the purpose of (a) destroying a building or occupied structure of another or (b) destroying or damaging any property, whether one's own or another's, to collect insurance for such loss. Other statutes include the destruction of property by other means (e.g., an explosion).

---


3ibid., p. 115.

4ibid., p. 870.

5ibid., p. 964.

6ibid., p. 979.

7ibid., p. 1019.

8ibid., p. 1329.

9ibid., p. 1260.

10ibid., p. 1375.


12*Black’s Law Dictionary*, p. 111.
• **Burglary.** Entering a vehicle or “building or occupied structure, or separately secured or occupied portion thereof, with purpose to commit a crime therein, unless the premises are[,] at the time, open to the public or the [perpetrator] is licensed or privileged to enter.” 13

• **Cyberattack.** “An assault against a computer system or network.” 14

• **Disorderly conduct.** “If, with purpose to cause public inconvenience, annoyance or alarm, or recklessly creating a risk thereof, he: (a) engages in fighting or threatening, or in violent or tumultuous behavior; or (b) makes unreasonable noise or offensively coarse utterance, gesture or display, or addresses abusive language to any person present; or (c) creates a hazardous or physically offensive condition.” 15 Depending on the nature of the offense, it can be considered a threat to people or property.

• **Espionage.** “The crime of ‘gathering, transmitting or losing’ information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the [country], or to the advantage of any foreign nation.” 16 A business competitor could also perpetrate this threat by engaging in industrial espionage.

• **Larceny.** “The unlawful taking and carrying away of property of another with intent to appropriate it to use inconsistent with the latter’s rights.” 17 Theft is a popular name for larceny. Larceny-theft includes offenses such as shoplifting, pickpocketing, auto theft, and other types of stealing where no violence occurs.

• **Sabotage.** In commerce, sabotage includes the “wil[l]ful and malicious destruction of employer’s property during a labor dispute or interference with his normal operations.” 18 This act could also be perpetrated by a disgruntled employee or ex-employee seeking revenge, or by a business competitor.

• **Theft.** “A popular name for larceny. The act of stealing. The taking of property without the owner’s consent…. It is also said that theft is a wider term than larceny and that it includes swindling and embezzlement and that generally, one who obtains possession of property by lawful means and thereafter appropriates the property to the taker’s own use is guilty of a ‘theft.’” 19 Larceny-theft includes offenses such as shoplifting, pickpocketing, auto theft, and other types of stealing where no violence occurs.

• **Trespass.** “Any unauthorized intrusion or invasion of private premises or land of another…. Criminal trespass is entering or remaining upon or in any land, structure, vehicle, aircraft or watercraft by one who knows he [or she] is not authorized or privileged to do so.” 20 This includes remaining on a property after permission to do so has been revoked.

---

13 ibid., p. 197.
15 Black’s Law Dictionary, p. 469.
16 ibid., p. 545.
17 ibid., p. 881.
18 ibid., p. 1335.
19 ibid., p. 1477.
20 ibid., p. 1503.
• **Vandalism.** “Such willful or malicious acts intended to damage or destroy property.”\(^{21}\)

Included among these acts is the use of graffiti, whereby often a sharp instrument (such as a key or a pocket knife) is used to scratch initials or symbols; whereby the graffiti is written using color markers, crayons, lipstick, pencils, correction fluid, or spray paint; or whereby the graffiti is etched into glass using acid (all such instances being commonly known as “tagging”). In buildings, graffiti can be found in restrooms and toilets, on walls of elevator lobbies and on walls and doors of elevator cars (particularly those of service or freight elevators), on walls adjacent to public telephones, and on exterior glass windows. Vandalism may also involve tampering with equipment (for example, standpipes on upper floors to cause flooding inside a building).

Although it may not be technically “willful” damage, the use of bicycles, scooters, skateboards, roller skates, and similar devices can lead to the destruction of property in building exterior areas and parking structures. “Skateboarders regularly wear down concrete surfaces, scuff up painted exteriors, and damage planters, handrails, [park benches,] and fountains.”\(^{22}\) Also, inadvertently, bicyclists, skateboarders, and roller skaters may collide with other people or seriously injure themselves.\(^{23}\)

In addition, there may be the disruption of building utilities such as water; electrical power; natural gas; sewer; heating, ventilation, and air-conditioning (HVAC); telecommunication; security; and life safety systems. This interference may involve a *cyberattack*, whereby unauthorized access is gained to networks that control these systems. Such an attack is becoming increasingly possible as many building systems are placed on networks, and the ability of persons to attack such networks is becoming progressively more sophisticated.

Some security threats may involve *terrorism*. “Terrorism is considered an unlawful act of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”\(^{24}\) A person is guilty of a *terroristic threat* “if he [or she] threatens to commit any crime of violence with purpose to terrorize another or to cause evacuation of a building, place of assembly, or facility of public transportation, or otherwise to cause serious public inconvenience, or in reckless disregard of the risk of causing such terror or inconvenience.”\(^{25}\)

*Cyberterrorism* is

\[
\text{[T]he convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people to further political or social objectives. Moreover, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death}
\]

\(^{21}\)ibid., p. 1533.


\(^{23}\)ibid.


\(^{25}\)Black’s *Law Dictionary*, p. 1473.
Security threats to people and property include bombs, hazardous materials, chemical and biological weapons, nuclear attack, civil disturbances, fires and fire alarms, natural disasters, and power failures.

Fire Life Safety Threats

In the high-rise setting, life safety threats, listed in alphabetical order, may include the following:

- Aircraft collisions
- Bombs and bomb threats
- Daredevils, protestors, and suicides
- Elevator and escalator incidents
- Fires and fire alarms
- Hazardous materials, chemical and biological weapons, and nuclear attack
- Kidnappings and hostage situations
- Labor disputes, demonstrations, and civil disorder
- Medical emergencies
- Natural disasters (earthquakes, tsunamis, volcanoes, heat waves, storms, floods and landslides)
- Contractible diseases (pandemic influenza, severe acute respiratory syndrome, and tuberculosis)
- Power failures
- Slip-and-falls
- Stalking and workplace violence
- Traffic accidents
- Water leaks

Again, some of these threats may involve terrorism. The September 11, 2001, attacks on the New York World Trade Center and the Pentagon using hijacked commercial aircraft and the subsequent mailing of anthrax-tainted envelopes on the U.S. East Coast were acts of terrorism, each using different means to carry out diabolical objectives.

Because of the vertical nature of high-rise structures, a building's height may actually constitute a threat. For example, an upper floor room with openable windows or a balcony, or a tall atrium, could be the scene of an accident if a child climbs onto a window sill or a railing and accidentally falls, or the means to intentionally throw or drop objects.

---


*Or the scene of other tragic accidents such as once when a young lady guest in a hotel upper room furnished with twin beds was jumping back and forth from bed to bed when she inadvertently leapt out of the room’s open window to her death. (J. Galinelo, former city of New York police officer, in personal conversation with the author, September 2008).
onto people below, or the location for a sniper to shoot at a target located a considerable distance away. Such a room, an atrium, or the building's rooftop could be used as an observation point, either for legal or illegal purposes, depending on the nature of the surveillance being conducted. Likewise, a multi-level parking structure could be similarly used.

The most critical threats in high-rise structures include fire, explosion, and contamination of life-support systems such as air and potable water supplies. These threats can be actuated accidentally or intentionally, and because they propagate rapidly, they can quickly develop to catastrophic levels.\(^\text{27}\)

### Building Emergencies

Threats may become events that develop into emergencies. An emergency is “an event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response.”\(^\text{28}\) (Whereas, a disaster is “a serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources.”\(^\text{29}\) In the high-rise setting, an emergency can pose a danger to a building, its occupants, or, depending on its nature, to surrounding buildings.

The following sections describe some emergencies that can occur at high-rise buildings. The emergencies addressed are aircraft collisions; bombs and bomb threats; daredevils, protestors, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstrations, and civil disorder; medical emergencies; natural disasters such as earthquakes, tsunamis, volcanoes, heat waves, storms\(^\text{*}\) (noncyclone, tornadoes, and tropical cyclones [cyclones, hurricanes and typhoons]), floods and landslides; contractible diseases (pandemic influenza, severe acute respiratory syndrome, and tuberculosis); power failures; slip-and-falls; stalking and workplace violence; traffic accidents; and water leaks. Each one must be properly handled according to preplanned procedures.

The impact of such threats on a building will largely depend on the nature of the incident and other factors such as the geographical and topographical location of the facility, its design and construction, its security and fire life safety systems and equipment, the location of the emergency within the facility, and the emergency preparedness of building staff and occupants.

---


\(^*\)Although not addressed here, in some countries (for example, in the Middle East) storms can be dust or sand generated. Depending on its intensity, a dust storm or sandstorm can cause serious problems, particularly relating to visibility and a building’s equipment such as HVAC systems and exterior video cameras.
Aircraft Collisions

A high-rise building, like any other facility, is vulnerable to the remote possibility that an aircraft could collide with it. Obviously, the additional height, as compared with other structures, makes high-rises more susceptible.

July 28, 1945, New York City—On a rainy, foggy Saturday, an off-course U.S. Army Air Corps B-25 bomber accidentally crashed into the north wall of the 102-story Empire State Building (Figure 3–1). The impact tore a large hole in the exterior wall of the building at the 78th and 79th floors, and a portion of the plane actually crossed one floor and exited through the south wall. The crash, along with several fires that resulted from flaming gasoline, resulted in the deaths of 3 crew members of the plane and 11 building occupants, injuries to 25 persons including several with severe burns, and property damage estimated at half a million dollars. A severed standpipe and damaged elevators caused by the crash restricted New York City Fire Department fire fighters’ efforts; however, within an estimated half hour they were able to control the fire. Despite the severity of the collision, the structural integrity of the building held.※

Because the majority of today’s airplanes travel at higher speeds and are much larger, heavier, and carry far greater fuel loads than the B-25 that collided with the Empire State Building, a similar incident today involving a modern high-rise building would have far more devastating consequences.

The response to such an incident should be similar to that required for an explosion or fire. There would need to be an immediate call to the fire department to request assistance and rapid evacuation of any building occupants from the affected area; this would include any injured persons who, if remaining, would be subjected to more serious injury. Any fire would have to be contained and suppressed if safe to do so. Unauthorized persons would be restricted from entering the building or the actual incident scene, and a command center would be set up to oversee operations.

Before specifically addressing the World Trade Center, it is noteworthy that after September 11, 2001, there were three other notable incidents involving light aircraft crashing into high-rise buildings.

January 5, 2002, Tampa, Florida—Late on Saturday afternoon, a stolen Cessna 172 plane piloted by a 15-year-old boy crashed into the 28th floor of the 42-story Bank of America building. The single-engine plane was reportedly deliberately flown into the building causing damage to an office and the death of the pilot. None of the six to eight people in the high-rise at the time of the incident were injured. 30


April 18, 2002, Milan, Italy—At 5:50 p.m., a small aircraft piloted by an elderly businessman crashed into the 25th floor of 30-story Pirelli Tower, the tallest building in Milan, killing a cleaning woman, a government lawyer and the pilot. At least 60 people were injured. The pilot reported mechanical trouble shortly before impact. The cause

---

of the accident has not been finally determined, although suicide of the pilot has been widely suggested.

October 11, 2006, New York—Mid-afternoon, a small single-engine plane, with New York Yankees pitcher Cory Lidle and his flight instructor, Tyler Stanger, aboard crashed into the 30th and 31st floors of a 40-story apartment building. Both occupants were killed in the crash, and flaming debris, including parts of the aircraft, rained down on sidewalks.  

In each incident, the structural damage to the building was localized to the point of impact of the plane.

September 11, 2001, New York World Trade Center Terrorist Attack

On the morning of September 11, 2001, within a 42-minute time frame, four commercial airliners fully loaded with fuel for transcontinental flights departed from Boston, Newark, and Washington, DC, airports. Within minutes of takeoff, four- to five-man teams on board hijacked these planes. Two of these aircraft, each with a fuel-carrying capacity of 23,980 U.S. gallons (90,770 liters) of aviation fuel and a maximum take-off weight of 395,000 pounds (179,170 kg), rammed into the Twin Towers of the World Trade Center in New York City (Figure 3–2). “It is estimated that, at the time of impact, each aircraft had approximately 10,000 gallons of unused fuel on board (compiled from government sources).” The resulting fire soon led to the total collapse of both these 110-story buildings. One other plane smashed into the Pentagon in Washington, DC. The fourth, reportedly bound for the White House, crashed in an open field in Pennsylvania after several of its passengers fought against the hijackers. “The events in New York City (NYC) on September 11, 2001, were among the worst building disasters and loss of life from any single building event in the United States.”

Shockwaves from these acts reverberated throughout the United States and the world. Within 22 minutes of the second plane hitting the World Trade Center, all U.S. domestic flights were grounded. Within hours, owners and managers of major U.S. high-rises, including the Sears Tower in Chicago, advised occupants to leave their buildings. The Los Angeles Times reported that even in Europe, authorities evacuated high-rise buildings as a safety measure. U.S. markets closed and foreign stock markets plummeted. U.S. President George W. Bush declared the attacks in New York and Washington “acts of war.” In October 2001, a U.S.-led coalition began bombing Afghanistan, the country harboring the Al Qaeda terrorist organization and its infamous leader, Osama bin Ladin, who had been identified as the instigator of the
FIGURE 3–2 Unbelievable Horror. Plumes of smoke pour from the World Trade Center buildings in New York on Tuesday, September 11, 2001. Planes crashed into the upper floors of both World Trade Center towers 16 minutes and 29 seconds apart in a horrific scene of explosions and fires that led to the collapse of the 110-story buildings. The Empire State Building is seen in the foreground. Used with permission of AP IMAGES.
attacks. The terrorist-supporting Taliban regime was ousted from power and a new government established.

**Sequence of Events**

The events that occurred in a fateful 1 hour, 41 minutes, and 55 seconds, were as follows:

8:46:30 a.m.—American Airlines Flight 11, a Boeing 767 airliner, with 76 passengers and 11 crew on board a scheduled flight from Boston to Los Angeles, crashed into the north face of the north tower (WTC 1) of the World Trade Center. The north tower was struck between the 93rd and 99th floors. “Evidence suggests that all three of the building’s stairwells became impassable from the 92nd floor up. Hundreds of civilians were killed instantly by the impact. Hundreds more remained alive but trapped.”

9:02:59 a.m.—United Airlines Flight 175, a Boeing 767 airliner, with 51 passengers and nine crew on board, also on a scheduled flight from Boston to Los Angeles, crashed into the south face of the south tower (WTC 2) of the World Trade Center and struck between the 77th and 85th floors. “The plane banked as it hit the building, leaving portions of the building undamaged on impact floors. As a consequence—and in contrast to the situation in the North Tower—one of the stairwells (A) of the three initially remained passable from at least the 91st floor down, and likely from top to bottom.”

Figure 3–3 depicts the approximate flight paths of the two aircraft. “Each plane banked steeply as it was flown into the building, causing damage across multiple floors. According to government sources, the speed of impact into the north tower was estimated to be 410 knots, or 470 miles per hour (mph) [756 kilometers per hour], and the speed of impact into the south tower was estimated to be 510 knots, or 590 mph [950 kilometers per hour]. As the two aircraft impacted the buildings, fireballs erupted.

---

37Information about the events, including exact times (Eastern Daylight Time) of the impact of the planes, was obtained from the National Institute of Standards and Technology Final Report on the Collapse of the World Trade Center Towers (NIST NCSTAR 1, 2005). Some information was also obtained from The 9/11 Commission Report, 2004.

38Columbia University scientists using a seismograph determined that the plane that hit the north tower “registered magnitude-0.9 on the seismograph, equal to a small earthquake” (“For many on September 11, survival was no accident” [USA Today. December 20, 2001:3], authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix IV” conducted in San Francisco by Mark Schofield and Douglas P. Forsman [March 6, 2002:4]).

39The World Trade Center had an excellent stair system, much better than required by building codes—both when it was built 30 years ago and now. Each tower had three stairwells. New York City building codes require two. Stairways A and C, on opposite sides of the building’s core, were 44 inches wide. In the center, Stairway B was 56 inches wide. The bigger the stairway, the faster an evacuation can proceed. In 44-inch stairways, a person must turn sideways to let another pass—for example, a rescuer heading up. In a 56-inch stairway, two people can pass comfortably (“For many on September 11, survival was no accident” [USA Today. December 20, 2001:4], authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix IV” conducted in San Francisco by Mark Schofield and Douglas P. Forsman [March 6, 2002:4]).


39Ibid., p. 293.
The term *fireball* is used to describe deflagration, or ignition, of a fuel vapor cloud. "Part of this fuel immediately burned off in the large fireballs that erupted at the impact floors. Remaining fuel flowed across the floors and down elevator and utility shafts, igniting intense fires throughout upper portions of the buildings. As these

---

fires spread, they further weakened the steel-framed structures, eventually leading to total collapse.” 41 Figure 3–4 shows the areas where aircraft debris landed outside of the towers.

9:58:59 a.m.—56 minutes after it was hit, the top floors of the south tower collapsed, causing the entire building to fall down.
10:28:25 a.m.—1 hour and 42 minutes (or 1 hour, 41 minutes, and 55 seconds to be precise) after it was struck, the north tower collapsed.

According to the Federal Emergency Management Association report, FEMA 403: The World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations, the following then occurred:

As the towers collapsed, massive debris clouds consisting of crushed and broken building components fell onto and blew into surrounding structures, causing extensive collateral damage and, in some cases, igniting fires and causing additional collapses. 42

Most of the fires went unattended as efforts were devoted to rescuing those trapped in the collapsed towers. 43

The 22-story Marriott World Trade Center Hotel (WTC 3) was hit by a substantial amount of debris during both tower collapses. Portions of WTC 3 were severely damaged by debris from each tower collapse, but progressive collapse of the building did not occur. However, little of WTC 3 remained standing after the collapse of WTC 1. WTC 4, 5, and 6 had floor contents and furnishings burn completely and suffered significant partial collapses.

41 ibid., p. 1.
42 ibid.
43 ibid., pp. 1–8.

According to the National Institute of Standards and Technology (NIST) Best Practices for Reducing the Potential for Progressive Collapse in Buildings, “The term ‘progressive collapse’ has been used to describe the spread of an initial local failure in a manner analogous to a chain reaction that leads to partial or total collapse of a building. The underlying characteristic of progressive collapse is that the final state of failure is disproportionately greater than the failure that initiated the collapse. ASCE Standard 7-05 defines progressive collapse as ‘the spread of an initial local failure from element to element resulting, eventually, in the collapse of an entire structure or a disproportionately large part of it’ (ASCE 2005).… Based on the above description, it is proposed that the professional community adopt the following definition, which is based largely on ASCE 7-05: progressive collapse—the spread of local damage, from an initiating event, from element to element resulting, eventually, in the collapse of an entire structure or a disproportionately large part of it; also known as disproportionate collapse” (NISTIR 7396 Best Practices for Reducing the Potential for Progressive Collapse in Buildings. Washington, DC: National Institute of Standards and Technology, U.S. Department of Commerce; February 2007:1).

“The concept of progressive collapse can be illustrated by the famous 1968 collapse of the Ronan Point apartment building. The structure was a 22-story precast concrete-bearing wall building. A gas explosion in a corner kitchen on the 18th floor blew out the exterior wall panel and failure of the corner bay of the building propagated upward to the roof and downward almost to the ground level. Thus, although the entire building did not collapse, the extent of failure was disproportionate to the initial damage” (NISTIR 7396 Best Practices for Reducing the Potential for Progressive Collapse in Buildings; February 2007:1).

Also, the collapse of WTC 7 on September 11, 2001, has been defined as progressive collapse by the National Institute of Standards and Technology (NIST) investigation of the collapse of World Trade Center Building 7 (NIST NCSTAR 1A Federal Building and Fire Safety Investigation of the World Trade Center Disaster. Final Report on the Collapse of World Trade Center Building 7. Executive Report. Washington, DC: National Institute of Standards and Technology; August 2008:xxxii)).
from debris impacts and from fire damage to their structural frames. WTC 7, a 47-story building that was part of the WTC complex, burned unattended for 7 hours before collapsing at 5:20 P.M.44 (See Figure 3–5.)

---

In total, 10 major buildings experienced partial or total collapse and approximately 30 million square feet of commercial office space was removed from service, of which 12 million belonged to the WTC Complex.\(^{45}\)

**World Trade Center Building Performance Study and Final Report on the Collapse of the World Trade Center Towers**

Since September 11, there was much discussion\(^\star\) about the design and performance of high-rise buildings. Two major studies\(^\star\) have been designed to evaluate

\(^{45}\)ibid., p. 1.

\(^\star\) For example, the question has been asked as to whether tall buildings should continue to be built in the future and whether they should be designed to resist all hazards, including explosions (the issue of designing buildings to resist explosions was also raised after the 1993 World Trade Center and the 1995 Oklahoma City bombings). Also, there have been suggestions to change future high-rise building design to include lower heights, more stairwells, lower occupancies, upgraded refuge areas, and safe elevators that could be used during emergencies such as fire (Fahy R, Proulx G. A Comparison of the 1993 and 2001 Evacuations of the World Trade Center. *Presentation to the NFPA World Safety Congress & Exhibition*. Minneapolis, MN: May 21, 2002). Even the threat from the air led to a policy change in Chicago—approved by the Federal Aviation Administration (FAA)—expanding “the ‘no-fly zone’ over the city to an area significantly larger than that mandated by the FAA immediately after September 11. This expansion was temporary, and the area has since been reduced” (Archibald R, Medby JJ, Rosen B, Schachter J. Security and Safety in Los Angeles High-Rise Buildings After 9/11. *RAND Documented Briefing*. Santa Monica, CA; April 2002:53).

\(^\star\) In addition, soon after September 11, the Council on Tall Buildings and Urban Habitat and the National Science Foundation announced the following studies:

1. The Council on Tall Buildings and Urban Habitat (CTBUH) formed a task force to explore options “to further increase the level of safety in tall buildings including the establishment of guidelines to better educate

World Trade Center Building Performance Study

The Federal Emergency Management Association (FEMA) and the Structural Engineering Institute of the American Society of Civil Engineers (SEI/ASCE), in collaboration with New York City and a number of other federal agencies and professional organizations, organized a Building Performance Study (BPS) Team** of specialists in tall building design and engineering to evaluate the performance of the buildings at the World Trade Center site.46 In May 2002, the Building Performance Study Team issued building management on safety procedures and decision-making and communication during an emergency."

(CTBUH. “Council organizes task force” [The Times. Council on Tall Buildings and Urban Habitat. LeHigh University: Bethlehem, PA; November 21, 2001:1]). In 2004, the CTBUH published an Emergency Evacuation Elevator Systems Guideline. As stated in its introduction, “This guideline will identify key issues that design teams should consider in the development of emergency evacuation systems. It is intended to serve as a tool for design teams who are considering the use of elevators as part of the egress system serving their designed structure. The goal of this publication is not to provide technical solutions but rather to bring forth issues for debate and to generate awareness of emergency evacuation needs related to tall buildings” (Emergency Evacuation Elevator Systems Guideline. Chicago, IL: Council on Tall Buildings and Urban Habitat; 2004: 7, 8). The final task force comprised “some of the world’s leading architects, engineers, building owner representatives, elevator consultants, life safety consultants, fire engineers, and elevator companies involved in the design of structures” (Emergency Evacuation Elevator Systems Guideline. Chicago, IL: Council on Tall Buildings and Urban Habitat; 2004: 8). Subsequent to this guideline there has been much discussion regarding the question whether elevators can be used for evacuation of occupants (particularly disabled/physically impaired persons), and for fire service use (by emergency responders), during emergency situations. See “Controls in Elevator Lobbies” in Chapter 6 for additional information regarding the use of elevators during building emergencies.

(2) The National Science Foundation (NSF), within weeks of the terrorist attacks, provided grants for postdisaster studies. One grant was to Frederick Mowrer, associate professor in the Department of Fire Protection Engineering at the University of Maryland. “Within the next year, Mowrer plans to compare the WTC incident to two other multi-floor burnouts in high-rise buildings, the 1988 First Interstate Bank building fire in Los Angeles, California, and the 1991 fire at One Meridian Plaza in Philadelphia, Pennsylvania. [Both these building fires are discussed later in the chapter.] Neither of these buildings collapsed, despite fire on multiple floors” (Weiger PR, Nicholson J. Learning from 9–11. NFPA Journal. National Fire Protection Association: Quincy, MA; May/June 2002: 103).

*The National Institute of Standards and Technology, a unit within the U.S. Department of Commerce, produces standards and technical reports, and a Building Science Series, which “disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems” (NIST. List of Publications by Subject Category, SP305-22 Abridged [U.S. Department of Commerce, National Institute of Standards and Technology: Washington, DC; revised July 1991]).

**Sometimes referred to as the Building Performance Assessment Team (BPAT), the team included personnel from the National Institute of Standards and Technology, the U.S. Fire Administration, the Worcester Polytechnic Institute, the Fire Department of New York, the New York City Office of Emergency Management, the Port Authority of New York and New Jersey, and the Structural Engineers Association of New York. Report reviewers included the American Institute of Steel Construction, various structural engineering groups, and the National Fire Protection Association.

its report, called the *World Trade Center Building Performance Study: Data Collection, Preliminary Observations and Recommendations*, “fulfilling its goal ‘to determine probable failure mechanisms and to identify areas of future investigation that could lead to practical measures for improving the damage resistance of buildings against such unforeseen events.’”\(^47\)

**Observations and Findings**

The following observations and findings are from the *World Trade Center Building Performance Study*:\(^48\)

*The structural damage sustained by each of the two buildings [WTC 1 and WTC 2] as a result of the terrorist attacks was massive. The fact that the structures were able to sustain this level of damage and remain standing for an extended period of time is remarkable and is the reason that most building occupants were able to evacuate safely. Events of this type, resulting in such substantial damage, are generally not considered in building design, and the ability of these structures to successfully withstand such damage is noteworthy.*

Preliminary analyses of the damaged structures, together with the fact the structures remained standing for an extended period of time, suggest that, absent other severe loading events such as a windstorm or earthquake, the buildings could have remained standing in their damaged states until subjected to some significant additional load. However, the structures were subjected to a second, simultaneous severe loading event in the form of the fires caused by the aircraft impacts.

*The large quantity of jet fuel carried by each aircraft ignited upon impact into each building. A significant portion of this fuel was consumed immediately in the ensuing fireballs. The remaining fuel is believed either to have flowed down through the buildings or to have burned off within a few minutes of the aircraft impact. The heat produced by this burning jet fuel does not by itself appear to have been sufficient to initiate the structural collapses. However, as the burning jet fuel spread across several floors of the buildings, it ignited much of the buildings’ contents, causing simultaneous fires across several floors of both buildings. The heat output from these fires is estimated to have been comparable to the power produced by a large commercial power generating station. Over a period of many minutes, this heat induced additional stresses into the damaged structural frames while simultaneously softening and weakening these frames. This additional loading and the resulting damage were sufficient to induce the collapse of both structures.*

The ability of the two towers to withstand aircraft impacts without immediate collapse was a direct function of their design and construction characteristics, as was the vulnerability of the two towers to collapse a


result of the combined effects of the impacts and ensuing fires. Many buildings with other design and construction characteristics would have been more vulnerable to collapse in these events than the two towers, and few may have been less vulnerable. It was not the purpose of this study to assess the code-conformance of the building design and construction, or to judge the adequacy of these features. However, during the course of this study, the structural and fire protection features of the buildings were examined. The study did not reveal any specific structural features that would be regarded as substandard, and, in fact, many structural and fire protection features of the design and construction were found to be superior to the minimum code requirements.

Several building design features have been identified as key to the buildings’ ability to remain standing as long as they did and to allow the evacuation of most building occupants. These included the following:

- robustness and redundancy of the steel framing system
- adequate egress stairways that were well marked and lighted
- conscientious implementation of emergency exiting training programs for building tenants

Similarly, several design features have been identified that may have played a role in allowing the buildings to collapse in the manner that they did and in the inability of victims at and above the impact floors to safely exit. These features should not be regarded either as design deficiencies or as features that should be prohibited in future building codes. Rather, these are features that should be subjected to more detailed evaluation, in order to understand their contribution to the performance of these buildings and how they may perform in other buildings. These include the following:

- the type of steel floor truss system present in these buildings and their structural robustness and redundancy when compared to other structural systems
- use of impact-resistant enclosures around egress paths
- resistance of passive fire protection to blasts and impacts in buildings designed to provide resistance to such hazards
- grouping emergency egress stairways in the central building core, as opposed to dispersing them throughout the structure....

WTC 5, WTC 7, 90 West Street, the Bankers Trust building, the Verizon building, and World Financial Center 3 were impacted by large debris from the collapsing towers and suffered structural damage, but arrested collapse to localized areas. The performance of these buildings demonstrates the inherent ability of redundant steel-framed structures to withstand extensive damage from earthquakes, blasts, and other extreme events without progressive collapse.

**What Future Changes May Result from the World Trade Center’s Destruction?**

The ensuing years will reveal the total impact of this disaster on society and the world of skyscrapers. Some changes will be determined by the findings of the World Trade Center
During the course of this study, the question of whether building codes should be changed in some way to make future buildings more resistant to such attacks was frequently explored. Depending on the size of the aircraft, it may not be technically feasible to develop design provisions that would enable all structures to be designed and constructed to resist the effects of impacts by rapidly moving aircraft, and the ensuing fires, without collapse. In addition, the cost of constructing such structures might be so large as to make this type of design intent practically infeasible.

Although the attacks on the World Trade Center are a reason to question design philosophies, the BPS Team believes there are insufficient data to determine whether there is a reasonable threat of attacks on specific buildings to recommend inclusion of such requirements in building codes. Some believe the likelihood of such attacks on any specific building is deemed sufficiently low to not be considered at all. However, individual building developers may wish to consider design provisions for improving redundancy and robustness for such unforeseen events, particularly for structures that, by nature of their design or occupancy, may be especially susceptible to such incidents. Although some conceptual changes to the building codes that could make buildings more resistant to fire or impact damage or more conducive to occupant egress were identified in the course of this study, the BPS Team felt that extensive technical, policy, and economic study of these concepts should be performed before any specific code change recommendations are developed. This report specifically recommends such additional studies. Future building code revisions may be considered after the technical details of the collapses and other building responses to damage are better understood.

The debris from the collapses of the WTC towers also initiated fires in surrounding buildings, including WTC 4, 5, 6, and 7; 90 West Street; and 130 Cedar Street. Many of the buildings suffered severe fire damage but remained standing. However, two steel-framed structures experienced fire-induced collapse. WTC 7 collapsed completely after burning unchecked for approximately 7 hours, and a partial collapse occurred in an interior section of WTC 5. Studies of WTC 7 indicate that the collapse began in the lower stories, either through failure of major load transfer members located above an electrical substation structure or in columns in the stories above the transfer structure. The collapse of WTC 7 caused damage to the Verizon building and 30 West Broadway. The partial collapse of WTC 5 was not initiated by debris and is possibly a result of fire-induced connection failures. The collapse of these structures is particularly significant in that, prior to these events, no protected steel-frame structure, the most common form of large commercial construction in the United States, had ever experienced a fire-induced collapse. Thus, these events may highlight new building vulnerabilities, not previously believed to exist.
Recommendations for Buildings Being Evaluated for Extreme Events

In the study of the WTC towers and the surrounding buildings that were subsequently damaged by falling debris and fire, several issues were found to be critical to the observed building performance in one or more buildings.

These issues fall into several broad topics that should be considered for buildings that are being evaluated or designed for extreme events. It may be that some of these issues should be considered for all buildings; however, additional studies are required before general recommendations, if any, can be made for all buildings. The issues identified from this study of damaged buildings in or near the WTC site have been summarized into the following points:

a. Structural framing systems need redundancy and/or robustness, so that alternative paths or additional capacity are available for transmitting loads when building damage occurs.
b. Fireproofing needs to adhere under impact and fire conditions that deform steel members, so that the coatings remain on the steel and provide the intended protection.
c. Connection performance under impact loads and during fire loads needs to be analytically understood and quantified for improved design capabilities and performance as critical components in structural frames.
d. Fire protection ratings that include the use of sprinklers in buildings require a reliable and redundant water supply. If the water supply is interrupted, the assumed fire protection is greatly reduced.
e. Egress systems currently in use should be evaluated for redundancy and robustness in providing egress when building damage occurs, including the issues of transfer floors, stair spacing and locations, and stairwell enclosure impact resistance.
f. Fire protection ratings and safety factors for structural transfer systems should be evaluated for their adequacy relative to the role of transfer systems in building stability.

The BPS Team has developed recommendations for specific issues, based on the study of the performance of the WTC towers and surrounding buildings in response to the impact and fire damage that occurred. These recommendations have a broader scope than the important issue of building concepts and design for mitigating damage from terrorist attacks, and also address the level at which resources should be expended for aircraft security, how the fire protection and structural engineering communities should increase their interaction in building design and construction,

---

possible considerations for improved egress in damaged structures, the public understanding of typical building design capacities, issues related to the study process and future activities, and issues for communities to consider when they are developing emergency response plans that include engineering response.

[Regarding one of these aspects,] building evacuation, the following topics were not explicitly examined during this study, but are recognized as important aspects of designing buildings for impact and fire events. Recommendations for further study are to:

Perform an analysis of occupant behavior during evacuation of the buildings at WTC to improve the design of fire alarm and egress systems in high-rise buildings.

Perform an analysis of the design basis of evacuation systems in high-rise buildings to assess the adequacy of the current design practice, which relies on phased evacuation.

Evaluate the use of elevators as part of the means of egress for mobility-impaired people as well as the general building population for the evacuation of high-rise buildings. In addition, the use of elevators for access by emergency personnel needs to be evaluated.

[Regarding another of these aspects,] education of stakeholders (e.g., owners, operators, tenants, authorities, designers), [they] should be further educated about building codes, the minimum design loads typically addressed for building design, and the extreme events that are not addressed by building codes. Should stakeholders desire to address events not included in the building codes, they should understand the process of developing and implementing strategies to mitigate damage from extreme events.

---

*For example, to facilitate counterflow by occupants moving downward and emergency responders (such as firefighters) moving upward, NFPA Life Safety Code requires that each stairwell that must accommodate a total cumulative occupant load of fewer than 2,000 persons have a stair width of 44 inches (1.12 meters), and those that must accommodate more than or equal to 2,000 persons have a stair width of 56 inches (1.42 meters) (Cote R, Harrington G. NFPA 101 Life Safety Code Handbook. Quincy, MA: National Fire Protection Association; 2006:158, 159).

**For some years this issue has been a major concern of fire protection individuals. Commenting on this subject, Charles Jennings, MS, MRP, John Jay College, stated that “The latest and most advanced thought is now devoted to developing pressurization requirements for elevator shafts and lobbies. The objective of these current efforts is to make elevators a useful component of the building evacuation system during a fire” (Jennings C. High-rise office building evacuation planning: human factors versus ‘Cutting edge’ technologies. [J Appl Fire Sci. 1994–95;4(4):289–302, Baywood Publishing Co., Inc.; 1995:291]). Since 9/11 there has been much discussion as to the feasibility of using elevators to evacuate occupants under emergency conditions. See Chapter 6 for additional information.

***Because of tragic 9/11 stories of doomed firefighters overburdened with gear and out of radio contact, Chicago and other cities are reviewing emergency communications and requiring or recommending that skyscrapers install lockers or closets with hoses, axes and oxygen tanks on upper floors so firefighters don’t have to carry them” (“High-rises remain vulnerable after 9/11.” O’Driscoll P. Los Angeles Times. September 25, 2005:3A). Since then some cities have installed interoperable radio communication systems.
Stakeholders should also be educated about the expected performance of their building when renovations, or changes in use or occupancy, occur and the building is subjected to different floor or fire loads. For instance, if the occupancy in a building changes to one with a higher fire hazard, stakeholders should have the fire protection systems reviewed to ensure there is adequate fire protection. Or, if the structural load is increased with a new occupancy, the structural support system should be reviewed to ensure it can carry the new load.

Final Report on the Collapse of the World Trade Center Towers

This report describes how the aircraft impacts and subsequent fires led to the collapse of the towers after terrorists flew jet fuel laden commercial airliners into the buildings; whether the fatalities were low or high, including an evaluation of the building evacuation and emergency response procedures; what procedures and practices were used in the design, construction, operation, and maintenance of the towers; and areas in current building and fire codes, standards, and practices that warrant revision.

Also in this report is a description of how NIST reached its conclusions. NIST complemented in-house expertise with private sector technical experts; accumulated copious documents, photographs, and videos of the disaster; established baseline performance\textsuperscript{*} of the WTC towers; performed computer simulations of the behavior of each tower on September 11, 2001; combined the knowledge gained into a probable collapse sequence for each tower; conducted nearly 1,200 first-person interviews of building occupants and emergency responders; and analyzed the evacuation and emergency response operations in the two high-rise buildings.

The report concludes with a list of 30 recommendations for action in the areas of increased structural integrity, enhanced fire endurance of structures, new methods for fire resistant design of structures, enhanced active fire protection, improved building evacuation, improved emergency response, improved procedures and practices, and education and training. [See details of these recommendations later in this chapter.]

The report’s complete “Summary of Findings” is Appendix 3–1 on the CD-ROM provided with this book.


Building Occupant Activity

The Federal Building and Fire Safety Investigation of the World Trade Center Disaster: Final Report on the Collapse of the World Trade Center Towers revealed that although almost 3,000 people lost their lives at the WTC site on September 11, five times that many people from the WTC towers successfully evacuated the site. The report stated that

Success in clearing a building in an emergency can be characterized by two quantities: the time people need to evacuate and the time available for them to do so. For the WTC Towers, the times available for escape were set by the collapse of the buildings. Neither the building occupants nor the emergency responders knew these times in advance. Moreover, the times were also three or four times shorter than the time needed to clear the tenant spaces of WTC 1 following the 1993 bombing.

The investigators examined the design of the buildings, the behavior of the people, and the evacuation process in detail to ascertain the factors that figured prominently in the time needed for evacuation. In analyzing these factors, NIST recognized that there were inherent uncertainties in constructing a valid portrayal of human behavior on that day. These included limitations in the recollections of the people, the need to derive findings from a statistical sampling of the building population, the lack of information from the decedents on the factors that prevented their escape, and the limited knowledge of the damage to the interior of the towers.

Occupant Population and Demographics

The Port Authority estimated that the population of the WTC complex on September 11, 2001, was 58,000 people, including those

---

*To document the egress from the two towers as completely as possible, NIST:

- Contracted with the National Fire Protection Association and the National Research Council of Canada to index a collection of over 700 previously published interviews with WTC survivors.
- Listened to and analyzed 9-1-1 emergency phone calls made during the morning of September 11.
- Analyzed transcripts of emergency communication among building personnel and emergency responders.
- Examined complaints filed with the Occupational Safety and Health Administration by surviving occupants and families of victims regarding emergency preparedness and evacuation system performance.

In addition NIST, in conjunction with NuStats, Partners, LLP as a NIST contractor, conducted an extensive set of interviews with survivors of the disaster and family members of occupants of the buildings. First, telephone interviews were conducted with 803 survivors, randomly selected from the list of approximately 100,000 people who had badges to enter the towers on that morning. The results enabled a scientific projection of the population and distribution of occupants in WTC 1 and WTC 2, as well as exploration of factors that affected evacuation. Second, 225 face-to-face interviews, averaging 2 hours each, gathered detailed, first-hand accounts and observations of the activities and events inside the buildings on the morning of September 11. These people included occupants near the floors of impact, witnesses to fireballs, mobility-impaired occupants, floor wardens, building personnel with emergency response responsibilities, family members who spoke to an occupant after 8:46 a.m., and occupants from regions of the building not addressed by other groups. Third, six complementary focus groups, a total of 28 people, were convened (NIST NCSTAR 1: Federal Building and Fire Safety Investigation of the World Trade Center Disaster: Final Report on the Collapse of the World Trade Center Towers. Washington, DC: National Institute of Standards and Technology, U.S. Department of Commerce; September 2005:157).

in the Port Authority Trans-Hudson (PATH) and Metropolitan Transit Authority (MTA) substations stations and the Concourse areas. Estimates from statistical analysis of the telephone interview data indicated that

There were 17,400 ± 1,180 occupants inside WTC 1 and WTC 2 at 8:46 a.m. Of these, 8,900 ± 750 were inside WTC 1 and 8,540 ± 920 were inside WTC 2. Estimates based on the layouts of the tenant spaces indicated that approximately 20,000 people worked in each tower. Relatively few visitors would have been present at 8:46 a.m. Thus, the towers were between one-third and one-half full at the time of the attack.

Of the estimated 17,400 people in the towers, 2749 people perished and thousands were injured. An undetermined number of people died entrapped in building elevators (there were 99 elevators in each tower).

Table 3–1 provides the likely locations of WTC decedents. Of the deceased, six were security managers, 13 were private security officers who worked at the WTC complex, and one was a security officer at a nearby building (their names are provided in the Dedication [p. v.] of this book).

In WTC 1, 1355 of the fatalities were people trapped on or above the 92nd floor (due to the fact that all three of the building stairwells were severely damaged and could not be used as a means of escape). “Of the roughly 7,545 building occupants who started that morning below the 92nd floor, all but 107 escaped the building. Those left

---


54On any given workday, up to 50,000 office workers occupied the towers, and 40,000 people passed through the complex” (The 9/11 Commission Report; 2004:278).

The lower than usual population on September 11 was attributed to the fact that some people were voting in New York City’s mayoral primary election; some were taking their children for the first day of school; due to Asia’s financial recession, many Asian investment firms had released employees or closed offices in the WTC; the 107th floor south tower observation deck was not scheduled to open until 9:30 a.m.; most retail stores under the complex were not yet open; and being 8:46 a.m., a lot of workers were yet to arrive (“For many on September 11, survival was no accident”; [USA Today]. December 20, 2001:5], authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix 1V” conducted in San Francisco by Mark Schofield and Douglas P. Forsman [March 6, 2002:4]).

“NIST estimated that if the towers had been fully occupied with 20,000 occupants each, it would have taken just over 3 hours to evacuate the buildings and about 14,000 people might have perished because the stairwell capacity would not have been sufficient to evacuate that many people in the available time” (NIST NCSTAR 1; 2005:xxxix).


54Eighty-three [elevator] mechanics from ACE Elevator of Palisades Park, N.J., left the buildings when the second jet hit. Dozens of people were trapped inside elevators at the time, according to the Port Authority. An elevator mechanic from another company rushed to the buildings from down the street and died trying to rescue people” (“For many on September 11, survival was no accident” [USA Today]. December 20, 2001:3], authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix 1V” conducted in San Francisco by Mark Schofield and Douglas P. Forsman [March 6, 2002:4]).

54These people “soon realized that they were unable to go downward to get away from the smoke and heat that [was] building up around them... Some of the people went toward the roof. However, there was no hope
behind were trapped by debris, awaiting assistance, helping others, or were just too late in starting their egress. For the most part, the evacuation was steady and orderly.56

Table 3–1 Likely Locations of WTC Decedents

<table>
<thead>
<tr>
<th>Location</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>WTC 1 occupants (total)</td>
<td>1,462</td>
</tr>
<tr>
<td>At or above the impact floors</td>
<td>1,355</td>
</tr>
<tr>
<td>Below the impact floors</td>
<td>107</td>
</tr>
<tr>
<td>WTC 2 occupants (total)</td>
<td>630</td>
</tr>
<tr>
<td>At or above the impact floors</td>
<td>619</td>
</tr>
<tr>
<td>Below the impact floors</td>
<td>11</td>
</tr>
<tr>
<td>Confirmed below impact zone in WTC 1 or WTC 2</td>
<td>302</td>
</tr>
<tr>
<td>Unknown location inside WTC 1 or WTC 2</td>
<td>243</td>
</tr>
<tr>
<td>Emergency responders (total)</td>
<td>421^4</td>
</tr>
<tr>
<td>FDNY</td>
<td>343</td>
</tr>
<tr>
<td>NYPD</td>
<td>23</td>
</tr>
<tr>
<td>PAPD</td>
<td>37</td>
</tr>
<tr>
<td>Hospital/paramedic</td>
<td>7</td>
</tr>
<tr>
<td>Federal</td>
<td>2</td>
</tr>
<tr>
<td>Volunteer responders</td>
<td>9</td>
</tr>
<tr>
<td>Bystander/nearby building occupant</td>
<td>18</td>
</tr>
<tr>
<td>American Airlines Flight 11</td>
<td>87^5</td>
</tr>
<tr>
<td>United Airlines Flight 175</td>
<td>60^5</td>
</tr>
<tr>
<td>No information</td>
<td>17</td>
</tr>
<tr>
<td>Total</td>
<td>2,749</td>
</tr>
</tbody>
</table>


1Where possible, NIST used eyewitness accounts to place individuals. Where no specific accounts existed, NIST used employer and floor information to place individuals.

2These individuals were typically security guards and fire safety staff who were observed performing activities below the floors of impact after the aircrafts struck.

3These 24 individuals were largely performing maintenance, janitorial, delivery, safety, or security functions.

4Emergency responders were defined to be people who arrived at the site from another location. Thus, security staff and Port Authority (PA) staff (different from PA police officers) were not defined as emergency responders.

5Does not include the five hijackers per aircraft.


In WTC 2, 619 of the fatalities were people trapped on or above the 77th floor due to the fact that of the three building stairwells only “one stairway• remained open above the crash, but few used it to escape. Stairway A, one of the three, was unobstructed from top to bottom…. Others went up these stairs in search of a helicopter rescue that wasn’t possible because of heavy smoke on the rooftop.” 57 • “Of the roughly 6,000 people who started the morning below the 77th floor, all but 11 evacuated the building, indicating sufficiently efficient movement within the three stairwells in the time available.” 58

Therefore, in both towers, a total of 118 occupants below the floors of impact perished. “Among the 118 decedents below the aircraft impact floors, investigators identified seven who were mobility impaired,••• but were unable to determine the mobility capability of the remaining 111.” 59

“Approximately 87 percent of the estimated 17,400 occupants of the towers, and 99 percent of those located below the impact floors, evacuated successfully.” 60

Evacuation of WTC 1


The number of survivors evacuated from WTC 1 was large, given the severity of the building damage and the unexpectedly short available time. Of those who were below the impact floors when the aircraft struck [7,545 people, as stated on p. 25 of the report], 99 percent survived. About 84 percent of all the occupants of the tower at the time survived. The aircraft impact damage left no exit path for those who were above the 91st floor. It is not known how many of those could have been saved had the building not

• An elevator machine room on the 81st floor, where the jet’s nose hit, helped protect one stairway in the south tower. … The elevator equipment room covered more than half the width of the 81st floor. Its size forced the tower’s designers to route Stairway A around the machines. The detour moved Stairway A from the center of the building … (on most floors, the stairways were about 30 feet [9.1 meters] apart in the core) … toward the northwest corner—away from the path the hijacked jet would take” (Cauchon D, Moore MT. Machinery saved people in WTC: Row of elevator hoists sheltered stairwell when jet hit tower. USA Today. May 17, 2002:1–3).

57 For many on September 11, survival was no accident” (USA Today. December 20, 2001:2), authored by Dennis Cauchon with contributors Barbara Hansen, Anthony DeBarros, and Paul Overberg. Article reprinted in the NFPA “Emergency Response Planning Workshop Participant Workbook, Appendix IV” conducted in San Francisco by Mark Schofield and Douglas P. Forsman (March 6, 2002:4).

••• Dennis Cauchon headed up an investigation published on December 20, 2001, “USA Today spent two months finding out precisely what happened in the 1 hour, 42 minutes and 5 seconds [55 seconds according to the NIST report] from the first jet crash to the last building collapse. The newspaper identified where 95% of the victims worked or were located at the time of the attacks. In addition, it matched floor plans, architectural drawings and photographs to the accounts of survivors and victims” (USA Today. December 20, 2001:2). The findings indicated that, “in each tower, 99% of the occupants below the crash site survived” (USA Today. December 20, 2001:1).


•••• People with physical disabilities rely on a variety of artificial means for mobility. Such devices range from canes and walkers to motorized wheelchairs” (Fire Risks for the Mobility Impaired. Emmitsburg, MD: U.S. Fire Administration. <www.usfa.fema.gov>; FA-204/December 1999:8).


60 ibid., pp. xxxviii.

61 ibid., pp. 138–160.
collapsed. While it is possible that a delayed or avoided collapse could have improved the outcome, it would have taken many hours for the FDNY [Fire Department of the city of New York] to reach the 92nd floor and higher and then to conduct rescue and fire suppression activity there.

The following are specific facts derived from the interviews:

The median time to initiate evacuation was 3 min for occupants from the ground floor to floor 76, and 5 min for occupants [on floors 77 through 91] near the impact region [between floors 93 and 91]. The factors that best explained the evacuation initiation delays were the floor the respondent was on when WTC was attacked, whether the occupant encountered smoke, damage or fire, and whether he or she sought additional information about what was happening.

Occupants throughout the building observed various types of impact indicators throughout the building, including wall, partition, and ceiling damage and fire and smoke conditions.

Damage to critical communications hardware likely prevented announcement transmission, and thus occupants did not hear announcements to evacuate, despite repeated attempts from the lobby fire command station.

Evacuation rates reached a maximum in approximately 5 minutes, and remained roughly constant until the collapse of WTC 2, when the rate in WTC 1 slowed to about 20 percent of the maximum.

The maximum downward travel rate was just over one floor per minute, slower than the slowest speed measured for non-emergency evacuation. This was in part because:

- Occupants encountered smoke and/or damage during evacuation.
- Occupants were often unprepared for the physical challenge of full building evacuation.
- Occupants were not prepared to encounter transfer hallways during the descent.
- Mobility-impaired occupants were not universally identified or prepared for full building evacuation.
- Occupants interrupted their evacuation.

The mobility-impaired occupants did not evacuate as evenly as the general population.

- Those who were ambulatory generally walked down the stairs with one hand on each handrail, taking one step at a time. They were typically accompanied by another occupant or an emergency responder. Combined, they blocked others behind them from moving more rapidly.
- On the 12th floor, FDNY personnel found 40 to 60 people, some of whom were mobility impaired. The emergency responders were assisting about 20 of these mobility-impaired people down the stairs just prior to the collapse of the building. It is unknown how many of this group survived.

*The general pattern of the evacuation is described in detail in Chapter 2 of the report and is available online at <http://wtc.nist.gov/NISTNCSTAR1CollapseofTowers.pdf>.
• Some mobility-impaired occupants requiring assistance to evacuate were left by coworkers, thereby imposing on strangers for assistance.

Evacuation of WTC 2

The evacuation from WTC 2 was markedly different from that from WTC 1. Over 90 percent of the occupants had started to self-evacuate before the second aircraft struck, and three-quarters of those from above the 78th floor had descended below the impact region prior to the second attack. (Nearly 3,000 occupants were able to survive due to self-evacuation and the use of the still-functioning elevators.) As a result, 91 percent of all the occupants survived. Eleven people from below the impact floors perished, about 0.1 percent. Eighteen people in or above the impact zone when the plane struck are known to have found the one passable stairway and escaped. It is not known how many others from the impact floors or above found their way to the passable stairway and did not make it out or how many could have been saved had the building not collapsed. A delayed or avoided collapse could have provided the additional time for more people to learn about and use the passable stairway.

The following are specific facts derived from the interviews:\(^{*}\)

The median time to initiate evacuation was 6 minutes, somewhat longer than in WTC 1.

As in WTC 1, occupants observed various types of impact indicators throughout the building, including wall, partition, and ceiling damage and fire and smoke conditions.

Building announcements were cited by many as a constraint to their evacuation, principally due to the 9:00 a.m. announcement instructing occupants to return to their work spaces. Crowdedness in the stairways, lack of instructions and information, as well as injured or disabled evacuees in the stairwells were the most frequently reported obstacles to evacuation.

Evacuation rates from WTC 2 showed three distinct phases:

1. Before WTC 2 was attacked, occupants used elevators, as well as stairs, to evacuate, resulting in approximately 40 percent of the eventual survivors leaving the building during that 16 minute window.
2. After WTC 2 was attacked and the elevators were no longer operational, the evacuation rate slowed down to a steady rate equivalent to the rate observed in WTC 1, which also had only stairs available to occupants.
3. About 20 minutes prior to building collapse, the rate in WTC 2 slowed to approximately 20 percent of the stairwell-only evacuation rate.


\[^{*}\] The general pattern of the evacuation is described in detail in Chapter 3 of the report and is available online at <http://wtc.nist.gov/NISTNCSTAR1CollapseofTowers.pdf>.
Information obtained by Fahy and Proulx from various media reports and a preliminary analysis of over 250 first-person accounts (National Fire Protection Association [NFPA] and National Research Council of Canada [NRCC] initiative) indicate that

In Tower 1, many reported leaving “immediately.” As many others reported “routine” activities, gathering belongings, or short delay. However, some delayed as long as 20 minutes or more before beginning evacuation.

People on floors 90 and 91 [of Tower 1] evacuated in times as short as 45 minutes on September 11th. (In 1993, the median evacuation time from the 90th floor was 2½ hours. No one evacuated in less than 2 hours.)

In Tower 2, most reported leaving right after Tower 1 was hit.... Once Tower 2 was hit, no one reported delaying their evacuation.

Building occupants [of Tower 2] had less than one hour [actually 56 minutes] to evacuate before the collapse.

There were a number of evacuees with disabilities that included two blind men with guide dogs, two deaf people and several wheelchair users.63

All indications are that the occupants who were able to evacuate did so in an orderly and competent manner. The World Trade Center had a comprehensive, well-executed fire life safety program and emergency plan that helped emergency staff and occupants to react appropriately to the catastrophic events that unfolded.

Of the estimated 17,400 occupants inside WTC 1 and WTC 2 at 8:46 a.m.,

- Two-thirds had participated in at least one fire drill in the 12 months prior to the 2001 disaster. Eighteen percent did not recall whether they had participated or not; 18 percent reported that they had not. New York City law prohibited requiring full evacuation using the stairs during fire drills.
- Six percent reported having a limitation that constrained their ability to escape. (This extrapolated to roughly 1,000 of the WTC 1 and WTC 2 survivors.) The most common of these limitations, in decreasing order, were recent injury, chronic illness, and use of medications.64

One clear message that applies to all high-rise buildings, whether they are evaluated to be at risk to a terrorist event or not, is that all occupants should be well trained in evacuation procedures.

What about Announcements and Instructions for Occupants to Return to or Remain in Their Offices? After the first plane hit the north tower, for surviving occupants in the south tower, “Building announcements were cited by many as a constraint to their evacuation, principally due to the 9:00 a.m. announcement instructing occupants to return to their work spaces.”65

---

65ibid., p. 160.
At 9:00 a.m. came the first building-wide public address system announce-
ment that there was a fire in WTC 1, that WTC 2 was secure, and that peo-
ple should return to their offices. This added confusion to an already tense
situation, a situation that became even more turbulent when at 9:02 a.m., a
contradictory announcement said that people may wish to start an orderly
evacuation if conditions on their floor warranted.66

“As a result of the announcement, many civilians remained on their floors. Others
reversed their evacuation and went back up.”67

“Similar advice was given in person by security officials in both the ground floor
lobby [of the south tower]—where a group of 20 that had descended by the elevators
was personally instructed to go back upstairs—and in the upper sky lobby, where many
waited for express elevators to take them down. Security officials who gave this advice
were not part of the fire safety staff.”68 “Nineteen of them returned upstairs, where 18
died; the 20th was told by her supervisor, who was in the group, to leave rather than
return upstairs. The supervisor also survived.”69

“Several South Tower occupants called the Port Authority police desk in 5 WTC.
Some were advised to standby for further instructions; others were strongly advised to
leave.”70

“It is not known whether the order by the FDNY to evacuate the South Tower
was received by the deputy fire safety director making announcements there. However,
at approximately 9:02—less than a minute before the building was hit—an instruction

66 Ibid., p. 37.
67 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon
the United States, investigation of “facts and circumstances relating to the terrorist attacks of September 11,
2001” by the National Commission on Terrorist Attacks upon the United States (also known as the 9/11
68 A note (No. 46) in The 9/11 Commission Report to this reference was “When a notable event occurred,
it was standard procedure for the on-duty deputy fire safety director to make an ‘advisory’ announcement
to tenants who were affected by or might be aware of the incident, in order to acknowledge the incident and
to direct tenants to stand by for further instruction. The purpose of advisory announcements, as opposed
to ‘emergency’ announcements (such as to evacuate), was to reduce panic” (The 9/11 Commission Report,
Chapter 9, Note 46, citing various civilian and FDNY interviews, and Port Authority of New York and New
69 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon
the United States, investigation of “facts and circumstances relating to the terrorist attacks of September 11,
2001” by the National Commission on Terrorist Attacks upon the United States (also known as the 9/11
70 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon
the United States, investigation of “facts and circumstances relating to the terrorist attacks of September 11,
2001” by the National Commission on Terrorist Attacks upon the United States (also known as the 9/11
over the South Tower’s public-address system advised civilians, generally, that they could begin an orderly evacuation if conditions warranted. Like the earlier advice to remain in place, it did not correspond to any prewritten emergency instruction.”  

It must be realized that at the time the first plane hit the north tower, no one explicitly knew that this was a terrorist act or that another aircraft was only 16 minutes and 29 seconds away from slamming into the south tower. After the first collision there were large amounts of material falling from the crash site to the ground outside of the north and south towers as well as a number of occupants who had started jumping from upper floors. The first priority of the WTC emergency personnel would have been to address the life safety of occupants in the north tower. Based on the information known at the time, it would not have been considered prudent to evacuate occupants from the south tower, since this may have involved placing those persons in danger from falling objects. It was only after the second plane hit that an indication of the diabolical nature of the disaster was revealed.

**Final Report Recommendations**


> The tragic consequences of the September 11, 2001, attacks were directly attributable to the fact that terrorists flew large jet-fuel laden commercial airliners into the WTC towers. Buildings for use by the general population are not designed to withstand attacks of such severity; building regulations do not require building designs to consider aircraft impact. In our cities, there has been no experience with a disaster of such magnitude, nor has there been any in which the total collapse of a high-rise building occurred so rapidly and with little warning.

> While there were unique aspects to the design of the WTC towers and the terrorist attacks of September 11, 2001, NIST has compiled a list of recommendations to improve the safety of tall buildings, occupants, and emergency responders based on its investigation of the procedures and practices that were used for the WTC towers; these procedures and practices are commonly used in the design, construction, operation, and maintenance of buildings under normal conditions. Public officials and building owners will need to determine appropriate performance requirements for those tall buildings, and selected other buildings, that are at higher risk due to their iconic status, critical function, or design.

> The eight major groups of recommendations are listed as follows in an order that does not reflect any priority:

- **Increased Structural Integrity**: The standards for estimating the load effects of potential hazards (e.g., progressive collapse, wind) and the design of structural

---

71 ibid.

systems to mitigate the effects of those hazards should be improved to enhance structural integrity.

Enhanced Fire Endurance of Structures: The procedures and practices used to ensure the fire endurance of structures should be enhanced by improving the technical basis for construction classifications and fire resistance ratings, improving the technical basis for standard fire resistance testing methods, use of the “structural frame” approach to fire resistance ratings, and developing in-service performance requirements and conformance criteria for sprayed [on] fire-resistance material.

New Methods for Fire Resistant Design of Structures: The procedures and practices used in the fire resistant design of structures should be enhanced by requiring an objective that uncontrolled fires result in burnout without local or global collapse. Performance-based methods are an alternative to prescriptive design methods. This effort should include the development and evaluation of new fire resistive coating materials and technologies and evaluation of the fire performance of conventional and high-performance structural materials.

Improved Active Fire Protection: Active fire protection systems (i.e., sprinklers, standpipes/hoses, fire alarms, and smoke management systems) should be enhanced through improvements to design, performance, reliability, and redundency of such systems.

Improved Building Evacuation: Building evacuation should be improved to include system designs that facilitate safe and rapid egress, methods for ensuring clear and timely communications to occupants, better occupant preparedness for evacuation during emergencies, and incorporation of appropriate egress technologies.

Improved Emergency Response: Technologies and procedures for emergency response should be improved to better enable better access to buildings, response operations, emergency communications, and command and control in large-scale emergencies.

Improved Procedures and Practices: The procedures and practices used in the design, construction, maintenance, and operation of buildings should be improved to include encouraging code compliance by nongovernmental and quasi-governmental entities, adoption and application of egress and sprinkler requirements in codes for existing buildings, and retention and availability of building documents over the life of a building.

Education and Training: The professional skills of building and fire safety professionals should be upgraded through a national education and training effort for fire protection engineers, structural engineers, architects, and building regulatory and fire service personnel.

---

*Performance-based design “applies a procedure to predict and estimate damage or behavior anticipated of a structure's design to design events, compared against preselected objectives. The design is revised until the predictive methodology indicates that acceptable performance can be obtained” (Manley BE. Fundamentals of structurally safe building design. In: Fire Protection Handbook. 20th ed. Quincy, MA: National Fire Protection Association; 2008:1–47).

**The prescriptive design approach “includes extensive detailed criteria for the design of systems that have been developed over many years of experience” (Cholin JM. Fire Protection Handbook. 20th ed. Woodworking facilities and processes. Quincy, MA: National Fire Protection Association; 2008:9–15).
The recommendations call for action by specific entities regarding standards, codes, and regulations, their adoption and enforcement, professional practices, education, and training; and research and development. Only when each of the entities carries out its role will the implementation of a recommendation be effective.

The recommendations do not prescribe specific systems, materials, or technologies. Instead, NIST encourages competition among alternatives that can meet performance requirements. The recommendations also do not prescribe specific threshold levels; NIST believes that this responsibility properly falls within the purview of the public policy setting process, in which the standards and codes development process plays a key role.

NIST believes the recommendations are realistic and achievable within a reasonable period of time. Only a few of the recommendations call for new requirements in standards and codes. Most of the recommendations deal with improving an existing standard or code requirement, establishing a standard for an existing practice without one, establishing the technical basis for an existing requirement, making a current requirement risk-consistent, adopting or enforcing a current requirement, or establishing a performance-based alternative to a current prescriptive requirement.

NIST strongly urges that immediate and serious consideration be given to these recommendations by the building and fire safety communities in order to achieve appropriate improvements in the way buildings are designed, constructed, maintained, and used in evacuation and emergency response procedures—with the goal of making buildings, occupants, and first responders safer in future emergencies.

NIST also strongly urges building owners and public officials to (1) evaluate the safety implications of these recommendations to their existing inventory of buildings and (2) take the steps necessary to mitigate any unwarranted risks without waiting for changes to occur in codes, standards, and practices.

NIST further urges state and local agencies to rigorously enforce building codes and standards since such enforcement is critical to ensure the expected level of safety. Unless they are complied with, the best codes and standards cannot protect occupants, emergency responders, or buildings.

Status of Recommendations
After publication of the NIST NCSTAR 1: Federal Building and Fire Safety Investigation of the World Trade Center Disaster: Final Report of the National Construction Team on the Collapses of the World Trade Center Towers, the National Construction Safety Team Act required NIST to do the following:

Conduct, or enable or encourage the conducting of, appropriate research recommended by the Team;
Promote (consistent with existing procedures for the establishment of building standards, codes, and practices) the appropriate adoption by the Federal Government, and encourage the appropriate adoption by other
agencies and organizations, of the recommendations of the Team with respect to—

- Technical aspects of evacuation and emergency response procedures;
- Specific improvements to building standards, codes, and practices; and
- Other actions needed to help prevent future building failures.

NIST is assigning top priority to work vigorously with the building and fire safety communities to assure that there is a complete understanding of the recommendations and to provide needed technical assistance in getting them implemented. NIST has identified specific codes, standards, and practices affected by each of the recommendations and begun to reach out to the responsible organizations to pave the way for a timely, expedited consideration of the recommendations.

In addition, NIST has implemented a web-based system so that the public can track progress on implementing the recommendations. This web site will list each of the recommendations, the specific organization or organizations (e.g., standards and code developers, professional groups, state and local authorities) responsible for its implementation, the status of its implementation by organization, and the plans or work in progress to implement the recommendations.

NIST has awarded a contract to the National Institute of Building Sciences (NIBS) to convene a panel of building code experts, representing the diverse technical areas covered by the WTC recommendations, to carry out the following tasks:

1. Develop a strategy for implementing relevant recommendations into model building codes.
2. Develop awareness of activities of other groups already focusing on implementing the recommendations (e.g., NFPA, ICC, ASCE 7, ASTM, AISC, ACI, AIA, and BOMA).**
3. Develop initial proposals for change to the model codes.
4. Shepherd proposed changes through the code-change processes.
5. Identify additional steps to be taken with respect to relevant standards.
6. Identify any needed training and educational tools.

The building code experts represent a broad spectrum of specific organizations (e.g., NFPA, ICC, ASCE, BOMA, and U.S. Accessibility Board) and areas of expertise (e.g., architecture, engineering, risk assessment, law enforcement, social science/egress, [security,] and insurance) that can address all of the recommendations. This core expertise will be augmented with the participation of other experts representing organizations and technical areas required to address one or more specific recommendations.

The timeline for this effort is governed by the established development cycle for the model codes.

The NIST WTC recommendations impact about 37 specific national standards, codes, and practice guidelines or regulations. In carrying out this

---

*For example, NFPA International formed a High-Rise Building Safety Advisory Committee (HRB-SAC) to initially review the NIST recommendations and forward each recommendation to the appropriate NFPA technical committee for consideration for its code establishment cycle.

**These acronyms are explained in the Acronym section at the back of this book.
work, NIST recognizes that not all of the recommendations will have an
impact on model building codes. Many will impact standards that are refer-
cenced in model codes. Others will impact stand alone standards used in prac-
tice but not referenced in model codes. A few will impact practices, including
education and training, that don’t have any impact on codes and standards.73•

A list of the recommendations and their implementation status can be viewed
online at the NIST website.74

Bombs and Bomb Threats

Bombs and bomb threats are very real possibilities in today’s world, and in some
countries, a frequent occurrence. They may be acts of terrorism used by a person or a group of
persons attempting to control others through coercive intimidation or by those who want

73 National Institute of Standards and Technology, NIST & The World Trade Center

74 National Institute of Standards and Technology, NIST & The World Trade Center
to promote their views by claiming direct responsibility or causing other targeted groups to be blamed for an incident. Terrorism may also include kidnappings, taking hostages, and other criminal acts such as bombings (although the September 11, 2001, destruction of the New York World Trade Center involved hijacked aircraft that were in effect turned into bombs, the incident was treated in the previous section “Aircraft Collisions”).

**Bombs**

Bombs involve either *explosives* or *incendiary devices*. *Webster’s College Dictionary* defines the former as “devices designed to explode or expand with force and noise through rapid chemical change or decomposition”; the latter are “devices used or adapted for setting property on fire” and can be activated by mechanical, electrical, or chemical means. Explosives may also be delivered in the form of a missile, such as a shoulder-launched, rocket-propelled grenade (RPG), or a mortar.

Conventional explosives may also be encased in radioactive waste material. Known as radiological or “dirty bombs,” if detonated these devices disperse radioactive material over an area determined by the size of the explosion, the kind and amount of material, weather conditions, and the types of facilities in the vicinity.\(^75\) After the detonation of a dirty bomb in a major urban area, as the level of radioactivity increased it could “spark panic,” overburdening the health-care system and perhaps forcing abandonment of many square blocks for decades.\(^76\) “Bombs can be constructed to look like almost anything and can be placed or delivered in any number of ways.\(^*\) The probability of finding a bomb that looks like a stereotypical bomb is almost nonexistent. The only common denominator that exists among bombs is that they are designed to explode.”\(^77\) Most bombs are improvised (hence the terms an improvised explosive device, an IED, and a vehicle-borne IED or a VBIED).

**Suicide Bombers**

Walk-in suicide bombers with explosives attached to their bodies or contained in a suitcase are extremely difficult to detect and can strike anywhere at any time. “A major

---


\(^{76}\) “A sudden terror often inspired by a trifling cause or a misapprehension of danger and accompanied by unreasoning or frantic efforts to secure safety” (*Webster’s Third New International Dictionary.* Springfield, MA: Merriam-Webster, Incorporated; 1993).


\(\ast\) An IED is a “device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components” (Definition from DOD, NATO as stated on *Answers.com* website. 2008. <www.answers.com/topic/improvised-explosive-device>; September 20, 2008).

\(\ast\ast\) A VBIED is a “military term for a car bomb or truck bomb. These are typically employed by suicide bombers and can carry a relatively large payload. They can also be detonated from a remote location. VBIEDs can create additional shrapnel through the destruction of the vehicle itself, as well as using vehicle fuel as an incendiary weapon” (Wikipedia. <https://en.wikipedia.org/wiki/Ied>; September 20, 2008).
reason for the concern, as the Israeli government has learned, is that no amount of preparedness can stop such bombers—not swarms of police patrols, stepped-up border enforcement or increased intelligence-gathering missions. In most cases, one person armed with less than a handful of plastic explosives can walk into a public gathering, flick a detonation switch and kill dozens of people.”  

Vehicle-Borne Improvised Explosive Devices (VBIEDs)

Bombs delivered by a vehicle (a car, a van, or a truck) are a grave reality. “A car bomb is an effective weapon because it is an easy way to transport a large amount of explosives and flammable material to the site where the explosion should take place. A car bomb also produces a large amount of shrapnel, or flying debris, that causes secondary damage to bystanders and buildings.”  

Car bombs and detonators function in a diverse manner of ways, and there are numerous variables in the operation and placement of the bomb within the vehicle. Earlier and less advanced car bombs were often wired to the car’s ignition system, but this practice is now considered more laborious and less effective than other more recent methods, as it required a greater amount of work for a system that could often be quite easily defused. While it is more common nowadays for car bombs to be fixed magnetically to the underside of the car, the underneath of passenger/driver’s seat, or inside of the mudguard, detonators triggered by the opening of the vehicle door or by pressure applied to the brakes or accelerating pedals are also used.

Bombs may also be detonated when a victim approaches the vehicle, when the vehicle is in motion, or when the vehicle passes by another vehicle that contains the explosives. “In recent years, car bombs have become widely used by suicide bombers who seek to ram the car into a building and simultaneously detonate it.” The destructive power of such a bomb depends on factors such as the type and amount of explosives, the location of the bomb in relation to a building, and the structural strength of the facility to withstand the explosion.

Table 3–2 summarizes significant bombing incidents** directed at American, Australian, British, French, Indian, Indonesian, Israeli, Kenyan, Pakistani, Saudi, Turkish, and Spanish peoples or their interests that have occurred from the 1993 New York World Trade Center attack to the present (the 2001 New York World Trade Center

---

**To obtain sources of information about vehicle bomb explosion hazards and evacuation distances, one can approach a structural engineer, a blast design consultant or expert, or the appropriate agencies.

**Dates and some details of incidents involving Al Qaeda versus United States and Allies, 1995–2003, were obtained from “The Chicago. Project on Suicide Terrorism,” Robert Pape, Professor of Political Science, the University of Chicago. <http://jtac.uchicago.edu/conferences/05/resources/pape_formatted%20for%20DTRA.pdf>. Others were obtained from various agencies and news sources, many of which are identified in the ensuing summaries of the incidents. At times, reports of casualties were conflicting. Therefore, the number of persons killed and injured could not always be definitively determined.
is addressed in the previous section). Although not all incidents involve high-rise buildings, they underline the seriousness of the threat that Western civilization faces today.

**1993 New York World Trade Center, New York**
The highly publicized 1993 international terrorist bombing of the New York World Trade Center Twin Towers, at the time the world’s second tallest buildings and a symbol...
of corporate America and technological achievement, sent shock waves throughout the world high-rise building community.

*February 26, 1993, New York City*—At 12:18 p.m. on a snowy Friday afternoon, a bomb containing approximately 545 kg TNT equivalent (1200 lb)\(^{82}\) of urea nitrate fertilizer, located in a parked van, detonated and tore a “five-story subgrade crater that measured 24 to 36 meters (80 to 120 feet) across on some levels”\(^{83}\) in the subterranean parking garage of the 110-story New York World Trade Center (WTC) located in lower Manhattan (Figure 3–6).

Of the estimated 100,000-plus occupants and visitors of this seven-high-rise building complex, the explosion left six dead and 1,042 injured (most suffered from smoke inhalation). It severely damaged many of the complex’s fire protection systems. For example, the fire alarm communication system for the Twin Towers of the Trade Center was incapacitated, and there was an interruption of primary and emergency power systems.

The bomb also resulted in a fire that rapidly disbursed thick, dark clouds of smoke to upper levels of the Twin Towers through horizontal openings—stairwell doors propped open while occupants were waiting to enter stairwells—and vertical openings—stairwells and elevator shafts. During this emergency, thousands of building occupants walked down darkened and smoke-filled stairwells to evacuate the building without the assistance of emergency lighting or of advisory emergency instructions delivered over the public address (PA) system. (Generators supplying emergency power to these systems started up, but after 12 minutes they overheated and shut down because of damage from

---

\(^{82}\) Hinman EE, Hammond DJ. *Lessons Learned from the Oklahoma City Bombing Defensive Design Techniques*. New York: ASCE Press, American Society of Civil Engineers; 1997:3.

\(^{83}\) ibid.
the explosion.) “Many persons were needlessly exposed to smoke inhalation and stress in premature evacuation from a structure in which upper floors were safer and more hospitable than the escape routes.”

According to the Bureau of Alcohol, Tobacco and Firearms (ATF), a vehicle identification number from the van, which had been rented but reported stolen the day prior to the explosion, was uncovered after the explosion. The ensuing investigation ultimately led to the identification and indictment of seven suspects, four of whom were convicted on conspiracy, assault, and various explosives charges. The evidence linked the defendants to the purchase of chemicals and hydrogen tanks used to manufacture the bomb, to the rental of the shed to warehouse the chemicals and later the bomb, and to the rental of the van that contained the bomb. Each of the four Muslim extremists directly responsible for this incident was sentenced to life in prison.

Considerable information relating to this bombing was obtained from the ATF and the NFPA. After the incident, two ATF National Response Teams assisted the New York City Police Department and the Federal Bureau of Investigation (FBI) in their inquiry. A thorough Fire Investigation Report on the World Trade Center Explosion and Fire can be obtained from the NFPA.

According to The World Trade Center Bombing: Report and Analysis, “It is estimated that approximately 50,000 people were evacuated from the WTC complex, including nearly 25,000 from each of the two towers. Fire alarm dispatchers received more than 1,000 phone calls, most reporting victims trapped on the upper floors of the towers. Search and evacuation of the towers were completed some 11 hours after the incident began.”

According to an evacuation study conducted by the NFPA and the NRCC (National Research Council of Canada) with funding provided by the National Institute of Standards and Technology (NIST), the evacuation of occupants from the Twin Towers ranged from minutes to hours, and less than 10 percent of the evacuees had previously participated in evacuation drills.

When an Emergency Overwhelms Security Staff
The 1993 WTC bombing vividly demonstrated that sometimes a building emergency may be of such magnitude that security personnel are unprepared to handle both the emergency itself and the heightened security demands created by the incident.

After the explosion, WTC security staff were involved in caring for the injured, assisting firefighters (at that time, the several hundred of which constituted the greatest single response to a fire in New York City Fire Department’s history) and other emergency services in occupant evacuation, and helping other agencies—the Port Authority Police and the New York Transit Police among others—to control access to the complex. Because of the enormity of the incident, the thousands of people affected, and the disastrous effects the explosion had on the towers’ fire life safety systems, building security personnel were

---


As can also be the case with serious fires (particularly if multiple ones simultaneously occur), explosions, workplace violence, civil disturbances, and some natural disasters.
inundated with demands for their services and were strained to the breaking point. Of course, the 2001 incident placed an almost indescribable burden on all involved, including those who lost their lives while helping others.

**Port Authority Liable in 1993 WTC Attack**

In 2008, a state appeals court unanimously upheld a jury’s verdict that the Port Authority (PA) of New York and New Jersey, which owned the WTC complex, because it was 68 percent liable for the bombing and the terrorists 32 percent liable, was liable for 100 percent of the recoverable damages caused by the 1993 bombing.\(^8^8\)

The ruling found “that the agency had not properly protected its underground public parking garage.... The appeals court noted the Port Authority did not argue that the bombing was unforeseeable, since the bombing method was not only foreseen but was brought to PA executives’ attention by the agency’s own internal study group. The group’s report said the trade center was vulnerable to terrorist attack through its parking garage. It detailed ‘with exact prescience’ how that vulnerability could be exploited, the appeals court said.”\(^8^9\) “In 1984, Peter Goldmark, then the Port Authority’s executive director, recognizing the trade center’s ‘iconic’ stature, asked Scotland Yard to assess the security of the complex and reported back to his colleagues that British officials were ‘appalled’ that there was public parking underneath the towers. In July 1985, an outside engineering consultant, Charles Schnabolk, issued a report saying that it was not only possible but ‘probable’ that there would be an attempt to bomb the trade center, and that it was ‘highly vulnerable through the parking lot.’”\(^9^0\)

**Changes after the 1993 WTC Attack**

According to Doug Karpiloff, the late security and life safety director for the World Trade Center, “Prior to the bombing, the WTC was an open building during the day, but closed at night. After the bombing, the Center was relegated to a closed facility, in which public parking was completely eliminated.”\(^9^1\) As reported by Security,\(^9^2\) security upgrades against the risk of vehicle bombs included the following measures:

> Forming a ring of 250 ten thousand-pound steel-reinforced planters surrounding the WTC complex, with a custom movable gate that permitted emergency vehicle access to the plaza. Then, according to Karpiloff, “If the gate is opened, the CCTV cameras lock onto the gate and can’t be moved until the gate is closed.” Once the gate was closed, the cameras unlocked and resumed regular surveillance. [According to Access Control & Security Systems,\(^9^3\) bomb-resistant trash containers were also provided as part of the perimeter protection system.]

---


Providing total closed-circuit television (CCTV) coverage of the plaza and perimeter of the WTC.

Restricting parking beneath the WTC to authorized tenants with special vehicle identification. [According to Access Control & Security Systems, the parking access control system utilized auto vehicle identification (AVI) tags on car windshields and driver’s proximity cards to make sure that both the vehicle and the driver were authorized to enter the garage.]

Equipping the underground parking garage with bullet-resistant guard booths, anti-ram barriers and explosives-detection trained (bomb-sniffing) dogs.

Stopping trucks one block from the buildings for inspection (after being cleared to proceed to the truck dock, the drivers were photographed along with their driver’s license, bill of lading, and registration information for storage on the WTC main server).

Installing a stopped vehicle detection system to sense cars stopping around the perimeter and within the WTC plaza. (When a stopped vehicle was sensed, the CCTV cameras locked onto that area, the WTC police were alerted and a video print of the vehicle could be taken. The cameras did not unlock until the vehicle was moved. This information was stored on the WTC server at the Security Command Center.)

After the 1993 WTC bombing, some high-rise office buildings installed CCTV systems at the entrance and exit points of under-building or subterranean parking garages. These cameras facilitated recording closeup images of the driver and license plate of every vehicle entering and the license plate of all vehicles exiting these areas. If there were an incident, this would help to identify vehicles that may have been involved.

1993 Bishopsgate Financial Area, London

The Bishopsgate bombing occurred on 24 April 1993, when the Provisional Irish Republican Army (IRA) detonated a truck bomb in London’s financial district in Bishopsgate, city of London, England. One person was killed in the explosion and 44 injured, causing £350 million in damage. As a result of the bombing, the ring of steel was introduced to protect the city, and many firms introduced disaster recovery plans in case of further attacks.95

94 ibid.
1995 Alfred P. Murrah Federal Building, Oklahoma City
April 19, 1995, Oklahoma City—At 9:02 a.m., when parents were dropping off their youngsters at the Alfred P. Murrah Federal Office Building’s day-care center, a homemade bomb containing an “estimated 2,177 kg (4,800 lb) of ammonium nitrate [fertilizer] and fuel oil (ANFO)” placed in a large rented truck parked in a no-parking, no-standing zone circular driveway outside the building detonated and blew away the facade and nearly half of this nine-story reinforced concrete frame building located in downtown Oklahoma City (Figure 3–7).

The blast left a 30-foot [9.1 meters]-wide, 8-foot [2.4 meters]-deep crater and shot a fireball and thick black smoke and debris high into the atmosphere. Shards of glass were propelled in every direction across several city blocks, office

---

windows were shattered, numerous nearby buildings suffered structural damage, and vehicles were damaged throughout the downtown business section.

Of the estimated 500-plus occupants and visitors of this structure, the explosion left 167 dead, including 19 children in the demolished day-care center. In addition, there were four fatalities at an adjacent building, one outside and one in a parked vehicle, while a nurse running to the scene was killed by a falling piece of concrete. 782 people were injured. The building was demolished as a result of the incident.97

Immediately following the explosion, the General Services Administration (GSA) placed over 1300 federal buildings throughout the United States on a security alert with building exterior patrols, inspection of packages, briefcases and vehicles, and heightened surveillance for persons and objects, including vehicles, which were suspicious or looked out of place. Parking was restricted around some buildings and some erected concrete barriers in front of the structures to protect against this type of threat.98

Timothy McVeigh was later executed for this incident, up until September 11, 2001, the worst terrorist attack in U.S. history.

Before this incident, there were no government-wide standards for security at federal facilities in the United States. After it, a study titled Vulnerability Assessment of Federal Facilities was conducted by the Standards Committee consisting of security specialists and representatives of the U.S. Department of Justice, including the Federal Bureau of Investigation (FBI), and of the U.S. Secret Service, General Services Administration (GSA), State Department, Social Security Administration, and Department of Defense. This committee developed “a set of [52] minimum security standards that can be applied to federal facilities. The standards cover the subjects of perimeter, entry, and interior security, and security planning”99 and embodied “new parking restrictions within buildings and in adjacent areas, use of X-rays and metal detectors at entrances for visitors and packages, erection of physical barriers, deployment of roving patrols outside the buildings, closed-circuit television monitoring, installation of shatterproof glass on lower floors, better alarm systems, locating new buildings farther from streets, grouping agencies with similar security needs, and tougher standards for visitor and employee identification.”100 “The Standards Committee divided federal holdings into five security levels to determine which security standards are appropriate for which security levels. These categories are based on such factors as size, number of employees, use, and required access to the public. The categories range from Level 1 [minimum security needs] to Level V [maximum security needs].”101 GSA has now developed The

97Information obtained from Hinman EE, Hammond DJ. Lessons Learned from the Oklahoma City Bombing Defensive Design Techniques. New York, NY: ASCE Press, American Society of Civil Engineers; 1997:1, 6, and various media reports.
Site Security Design Guide,* which “establishes the principles, explores the various elements, and lays out the process that security professionals, designers, and project and facility managers should follow in designing site security at any federal project, be it large or small, at an existing facility or one not yet built.”

1996 Khobar Towers Residential Military Complex, Dhahran, Saudi Arabia

“Khobar Towers was a complex of numerous apartment buildings in Al-Khobar near Dhahran, Saudi Arabia. On June 25, 1996, one of the apartment buildings [eight stories tall] was extensively damaged and others were seriously damaged when a massive [truck] bomb was detonated in the roadway that passed in front of the building.”

“Khobar Towers residential complex in Dhahran, Saudi Arabia, ... housed U.S. Air Force personnel. Nineteen Americans were killed, and 372 were wounded.”

“Most of the 19 U.S. servicemen who lost their lives were impacted by high-velocity projectiles created by the failed exterior cladding on the wall that faced the weapon. The building was an all-precast, reinforced concrete structure with robust connections between the slabs and walls. The numerous lines of vertical support along with the ample lateral stability provided by the ‘egg crate’ configuration of the structural system prevented collapse.”

Despite past allegations as to the identity of the attackers, the perpetrators are still unknown.

1998 U.S. Embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania

On the morning of August 7, the bomb-laden trucks drove into the embassies roughly five minutes apart—about 10:35 A.M. in Nairobi and 10:39 A.M. in Dar es Salaam.... The attack on the U.S. Embassy in Nairobi destroyed the...
embassy and killed 12 Americans and 201 others, almost all Kenyans. About 5,000 people were injured. The attack on the U.S. Embassy in Dar es Salaam killed 11 more people, none of them Americans. Interviewed later about the deaths of the Africans, Bin Ladin answered that “when it becomes apparent that it would be impossible to repel these Americans without assaulting them, even if this involved the killing of Muslims, this is permissible under Islam.” Asked if he had indeed masterminded these bombings, Bin Ladin said that the World Islamic Front for jihad against “Jews and Crusaders” had issued a “crystal clear” fatwa. If the instigation for jihad against the Jews and the Americans to liberate the holy places “is considered a crime,” he said, “let history be a witness that I am a criminal.”

2002 Sheraton Hotel, Karachi, Pakistan

On the morning of May 8, 2002, a suicide bomber killed 14 people, including 11 French engineers, outside of the Karachi Sheraton Hotel in Pakistan. The bomber driving a sedan pulled up close to a bus where the engineers were waiting to board. “The driver immediately detonated the explosives, reducing the 45-seat bus to a smoking wreck and shattering windows in the hotel and nearby buildings. In the front seat of the Toyota lay the charred remains of the bomber.”

2002 Nightclub, Bali, Indonesia

On October 12, 2002, three bombs, including a large vehicle bomb and a possible suicide bomber, devastated a nightclub area at Kuta Beach on the Indonesian island of Bali. The blasts killed 202 people, including seven Americans, and injured as many as 350. Most of those killed and injured were foreign tourists. This bombing has been attributed to members of the Jemaah Islamiya (JI) terrorist organization, a Southeast Asian–based terrorist network with links to al-Qa’ida, which allegedly helped finance the attack. The Bali bombing may have been carried out in response to audiotaped appeals from Al Qaeda leader Osama bin Ladin and his senior deputy Ayman al-Zawahiri broadcast on the al-Jazeera network beginning on October 6, 2002, that urged renewed attacks on U.S. and Western interests.

The FBI joined several other international antiterror agencies to assist Indonesia in the investigation of the attack. The investigation has yielded approximately 30 convictions overseas; including three suspects sentenced to death after being convicted of planning and carrying out the bombing. Notable among the convictions is Muslim cleric Abu Bakar Bashir, who is suspected of being the spiritual leader of JI. Bashir was sentenced in March

---


2003 to 30 months in prison for his part in the criminal conspiracy leading to the attack, although he was cleared of charges of planning a terrorist attack.

Investigators believe JI militants Noordin Mohammad Top and bomb-maker Azabari Husin were the masterminds behind the Bali nightclub attacks and several other Southeast Asian terrorist attacks. Husin was killed by Indonesian police during a shootout on November 9, 2005, in East Java, Indonesia. Top remained a fugitive at the end of 2005.109

2002 Hotel Mombassa, Kenya

November 28, 2002 in Mombasa, Kenya. Three suicide bombers crashed an SUV [sports utility vehicle] through a guard gate and onto the lobby steps of the Paradise Hotel, a seaside resort. Also, a surface-to-air missile was fired at an Israeli charter plane [carrying vacationers back to Israel] but it missed. The detonation of the vehicle killed 13 and injured 80.110

2003 Residential Compounds, Riyadh, Saudi Arabia

On the evening of May 12, 2003, al-Qa’ida operatives assaulted three residential compounds in Riyadh, Saudi Arabia, that house Western guest workers. At least fifteen assailants in six vehicles, two vehicles at each location, participated in the attacks against the Al-Hamra Oasis Village, Jedawal compound, and Vinnell Company compound located in suburban Riyadh. After breaching manned security barriers at two of the three sites, the attackers detonated vehicle-borne improvised explosive devices (VBIEDs) in the compounds, killing 35 people, including nine Americans, and injuring nearly 200 others. This assault followed a string of al-Qa’ida operations, including the August 7, 1998, East African embassy bombings; the October 12, 2000, bombing of the USS Cole in Aden, Yemen; the September 11, 2001, attack in the United States; and attacks on November 28, 2002, carried out against primarily Israeli targets in Mombasa, Kenya, involving simultaneous attacks against multiple targets.

The May 12 attack reflected a high degree of planning, pre-operational surveillance, and coordination among teams—traditional hallmarks of al-Qa’ida operations. It also reflected a highly refined approach to suicide bombings that may have incorporated lessons learned from the 1998 U.S. embassy bombings and other attacks. Preliminary investigation indicates that operatives traveling in lead vehicles attacked guards at each of the sites with small arms fire and hand grenades to quickly breach gates and other security measures to gain access to the compounds. Once inside the compounds, assailants may also have fired weapons to draw the attention of residents to window areas to maximize casualties.

---

The FBI and foreign partners have identified approximately 30 individuals thought to be involved in the planning and execution of the attack. Nearly all of these individuals have been killed or arrested by Saudi security forces.  

2003 JW Marriott Hotel, Jakarta, Indonesia

On the afternoon of August 5, 2003, a vehicle-borne improvised explosive device (VBIED) exploded in front of the JW Marriott Hotel located in Mega Kuningan, South Jakarta, Indonesia. The blast killed 11 people, not including the suicide bomber, and injured 144 others, including two U.S. citizens. The blast caused extensive damage to the hotel and an adjacent office building.

Investigation by the Indonesian National Police, the Australian Federal Police, and the FBI traced responsibility for the bombing to Jemaah Islamiyah (JI), a transnational Southeast Asian terrorist organization based in Indonesia with close links to al-Qa’ida, which helped to finance the bombing.

The international investigation has identified over 30 individuals involved in the conspiracy to bomb the JW Marriott Hotel in Jakarta. Witness testimony has identified Noordin Mohammed Top as the leader of the operation and Dr. Azahari Husin as the bombmaker. Approximately 30 of the conspirators have been arrested, tried, and convicted in Indonesian courts and have received prison sentences ranging from three to 14 years. Husin was killed by Indonesian police during a shootout on November 9, 2005, in East Java, Indonesia. Top remained a fugitive at the end of 2005.

The investigation into the bombing of the JW Marriott Hotel in Jakarta is ongoing.

2003 HSBC Bank and British Consulate, Istanbul, Turkey

On November 20, as US President George W. Bush was in the United Kingdom meeting with Prime Minister Tony Blair, two truck bombs exploded. Suicide bombers detonated the vehicles at the HSBC Bank AS and the British Consulate, killing thirty people [various news sources quote numbers of fatalities varying from 27 to 30] and wounding 400 others. The bombers appeared to have waited for the traffic lights in front of the HSBC headquarters to turn red to maximize the effects. Several Britons were killed in the two attacks, including the top British official in Istanbul, consul general Roger Short, but most of the victims were Turkish Muslims.... Police say that the bombers may have timed the attacks to coincide with Bush’s visit to the UK. Bin Laden allegedly planned [this] attack in Turkey.
2004 Train System, Madrid, Spain

On March 11, 2004, deadly bombings [of Madrid’s train system during rush hour involved explosives contained in backpacks left on four commuter trains. The incidents] that left 191 dead and 1,824 injured in Madrid were one of the worst worldwide terror attacks since the September 11, 2001 strikes on New York and Washington. In addition to the carnage, the March 11, 2004 blasts targeting the Spanish city’s train network caused major psychological and political fall-out. The country swiftly re-evaluated its contribution to U.S.-led global anti-terror operations. Three days after the attacks, blamed on Islamic militant groups including al-Qaeda, the then government was voted out of office. Its successors ended Spain’s military involvement in Iraq. Meanwhile, Spain launched a massive manhunt for the perpetrators, eventually bringing 29 suspects to trial in February 2007.115 A Spanish court Wednesday convicted 21 in the 2004 bombing of Madrid’s train system, the deadliest terrorist attack in continental Europe.116

2004 Offices and Residences, Al Khobar, Saudi Arabia

On the morning of May 29, 2004, terrorist attacks were carried out against at least three Western targets in the city of Al Khobar. Foreign Nationals, including Westerners, and Saudi citizens were killed in the attacks. Terrorists held around 50 people hostage in the offices and residences of foreign oil company employees in Al-Khobar. The attack began at 7.30 in the morning, when four attackers in army uniform attacked the APICORP compound, site of the headquarters of the Arab Petroleum Investment Corporation as well as its housing facilities. The perpetrators seemed to spare Muslims but not without advising them towards their ill-guided version of piety. The hostage crisis, which lasted for almost 25 hours, came to an end on 30 May 2004 when Saudi commandos rescued fifty people. Twenty-two people were killed by the terrorists which included eight Indians.117

2005 London Transportation System

On July 7, 2005, a series of coordinated suicide bomb blasts struck London’s transport system during morning rush hour. Beginning at 8:50 a.m. three bombs exploded within 50 seconds of each other on three London Underground trains, and a fourth bomb exploded on a bus nearly an hour later at 9:47 a.m. in London’s Tavistock Square. Fifty-two people were killed [including the four suicide bombers] and approximately 700 injured in the bombing. Among the casualties were one American killed and four wounded. The four suicide bombers were British citizens; three had been born in the United Kingdom, and the fourth had been born in Jamaica. The British

*Although this incident did not reportedly involve explosives, it is mentioned here as it bears some similarities to the 2008 Taj Mahal Palace and Tower Hotel and Oberoi Hotel incidents in Mumbai, India (see later description of these incidents), which also targeted Westerners.
citizenship of the bombers and the lack of strong ties between them and an international terrorist group illustrate the potential threat of “homegrown” terrorists as perpetrators of future attacks.\(^\text{118}\)

2005 London Transportation System Attempted Bombings

“On 21 July 2005, four attempted bomb attacks disrupted part of London’s public transport system two weeks after the 7 July 2005 London bombings. The explosions occurred around midday at Shepherd’s Bush, Warren Street and Oval stations on London Underground, and on a bus in Shoreditch. A fifth bomber dumped his device without attempting to set it off.”\(^\text{119}\)

Four men were found guilty for the attacks. “The failed bombers targeted three Tube trains and a bus—as happened on 7/7—but the devices [“only the detonators exploded”\(^\text{120}\)] failed to explode. The men are Muktar Ibrahim, 29, Yassin Omar, 26, Ramzi Mohammed, 25, and Hussain Osman, 28.”\(^\text{121}\) The four attempted bombers were each sentenced to life imprisonment with a minimum of 40 years.\(^\text{122}\)

2006 Commuter Trains, Mumbai, India

On July 11, 2006, seven bomb blasts, within 15 minutes of each other, ripped through trains in the evening rush hour on commuter trains in Mumbai (formerly Bombay),\(^\text{123}\) the nation’s financial capital.

The Indian government accused Pakistan’s military spy agency, the Inter Services Intelligence, of planning the July 11 Mumbai train bombings that killed 209 people…. The bombs consisted of pressure cookers filled with ammonium nitrate and RDX, a base commonly used in military explosives…. Roy [Indian police commissioner, A. N. Roy] said the Lashkar-e-Tayyaba, a banned terrorist group from Pakistan, and the Students Islamic Movement of India were part of the planning and carried out the attacks.\(^\text{124}\)

2007 London Incidents

June 29, 2007, London

Two car bombs were discovered and disabled before they could be detonated. The first device was left near the Tiger Tiger nightclub in Haymarket at around 01:30, and the second was in Cockspur Street, in the same area of the city.\(^\text{125}\)


\(^{120}\) ibid.


“Deputy Assistant Commissioner Peter Clarke, head of the counter-terrorism command, gave the following statement: ‘At around 1am this morning a London Ambulance Service crew was called to the Tiger Tiger nightclub in Haymarket in Piccadilly, London, to treat a person who had been taken ill. While they were there they noticed a Mercedes car parked outside the Tiger Tiger Club and noticed that there appeared to be smoke inside the vehicle. The police were called and the Metropolitan Police explosives officers went to the scene and examined the car. Inside they found significant quantities of petrol, gas cylinders, and I cannot at this stage tell you how much petrol because we have not yet have a chance to measure it precisely but what I can tell you is that it was in several large containers. There was also a large number of nails in the vehicle.’”

“It is thought the second car was found parked illegally in the West End by traffic wardens in the early hours of this morning. It was then towed to the pound—located in the car park—but left outside in the public area when staff reported that it smelt of fuel”.

“The cars and their devices were recovered intact for forensic examination and both were found to contain petrol cans, gas canisters and a quantity of nails, with a mobile phone-based trigger.”

June 30, 2007, Glasgow International Airport

“A Jeep Cherokee trailing a cascade of flames rammed into Glasgow airport on Saturday, shattering glass doors just yards from passengers at the check-in counters. Police said they believed the attack was linked to two car bombs found in London the day before.” Both of the car’s occupants were arrested. “Police identified the two men as Bilal Abdullah, a British-born, Muslim doctor of Iraqi descent working at the Royal Alexandra Hospital, and Kafeel Ahmed, also known as Khalid Ahmed, the driver, who was treated for severe burns at the same hospital.” Ahmed later died.

“A jury found the doctor, Bilal Abdulla, a passenger in the Jeep Cherokee, guilty of two charges of conspiracy to commit murder and conspiracy to cause explosions in three bungled car bombing attempts in Glasgow and London over 24 hours.... The day before that attack, Dr. Abdulla and Mr. Ahmed drove to London’s West End theater district in two Mercedes-Benz sedans, primed with bombs similarly constructed from gasoline canisters and propane cylinders, along with 2,000 nails for shrapnel. The cars were parked

outside a nightclub and beside a busy bus stop. The two attackers waited nearby with mobile phones linked to other phones wired to the bombs used as triggers. But evidence at the trial showed that the two vehicles had failed to explode despite repeated signals from the mobile phones because of faulty assembly of the so-called fuel air bombs involved."

2008 JW Marriott Hotel, Islamabad, Pakistan

September 20, 2008, at approximately 8:00 p.m., a dump truck containing an estimated 1,300 pounds (600 kilograms) of military-grade explosives rammed a metal barrier and came to a halt about 60 feet (18 meters) from the Marriott Hotel, which is surrounded by government buildings and is located in Pakistan’s capital. Detonated by the driver, the resulting explosion killed 53 people, injured more than 250 people, severely damaged the hotel, and left a crater 60 feet (18 meters) wide and 24 feet (7.3 meters) deep in front of the main building."

“The government released surveillance camera footage showing the attack. A suicide bomber at the wheel of a dump truck opened fire at Marriott security guards who refused to let him into the parking lot. He then detonated himself and started a small fire. The guards spent four minutes trying to extinguish the blaze when another, much bigger explosion went off.”

“The massive blast ripped through the Marriott Hotel’s walls, blew out ceilings, scorched trees, reduced nearby cars to charred husks of twisted metal and shattered windows hundreds of yards away. Flames began shooting out of the windows of many of the hotel’s 290 rooms.”

The explosion was during the Muslim holy month of Ramadan and so the hotel’s restaurants would have contained many Muslims breaking their daily fast.

“No group immediately claimed responsibility for the blast, though suspicion fell on al-Qaeda and the Pakistani Taliban. Analysts said the attack served as a warning from Islamic militants to Pakistan’s new civilian leadership to stop cooperating with the U.S.-led war on terror.”

2008 Taj Mahal Palace and Tower Hotel and Oberoi Hotel, Mumbai, India

On November 26, 2008, “Hooded gunmen, firing automatic weapons and throwing hand grenades, attacked at least two luxury hotels, the city’s largest train station, a Jewish center, a movie theater, even a hospital…. Even by the standards of terrorism in India, which has suffered a rising number of attacks this year, the assaults were particularly brazen in scale, coordination and execution.”

---


136 Some hostages free after Indian attacks. Somini Sengupta reported from Mumbai and Mark McDonald from Hong Kong. Reporting was contributed by Michael Rubenstein and Prashanth Vishwanathan from Mumbai; Jeremy Kahn and Hari Kumar from New Delhi; Souad Mekhennet from Frankfurt, Germany; Sharon Otterman and Michael Moss from New York; and Mark Mazzetti from Washington (The New York Times. <www.nytimes.com/2008/11/28/world/asia/28mumbai.html?_r=1&hp>; November 27, 2008).
The death toll from the series of coordinated attacks was at 101 [later estimated at 171], including at least six foreigners, by Thursday afternoon authorities said. The Italian Foreign Ministry confirmed one of its citizens had been killed. The nationalities of the others was still being checked. Another 314 people were wounded in the attacks, including seven British and two Australian citizens. In addition, at least nine gunmen were killed in fighting with police. Also among the dead was Hemant Karkare, the chief of the Mumbai police’s anti-terror squad, and as many as 11 police officers.\textsuperscript{137}

Ashok Pawar, a local police constable who arrived at the Taj Mahal Palace & Hotel [Figure 3–8] shortly after the gunmen lay siege to it, said he could see their carefully scripted tableau in the closed-circuit TV cameras in the hotel’s second floor security room. In two teams of two, the gunmen kicked down hotel room doors, forced guests to come out into the hallway, tied the men’s hands behind their backs, usually with a bed-sheet, and herded their captives into one room…. The gunmen soon realized they were being watched, and so they smashed the cameras, lobbed a grenade and started firing at Mr. Pawar and his colleagues in the security room.\textsuperscript{138}

The leader of a commando unit involved in a gun battle Thursday morning inside the Taj said during a news conference on Friday that he had seen a dozen dead bodies in one of the rooms. His team also discovered a gunman’s backpack, which contained dried fruit, 400 rounds of AK-47 ammunition, four grenades, Indian and American money, and seven credit cards from some of the world’s leading banks. They pack also had a national identity card from the island of Mauritius, off Africa’s


southeastern coast. The attackers were ‘very, very familiar with the layout of the hotel,’ said the commander.\(^{139}\)

“It is possible the Mumbai attackers chose the Taj and Oberoi because security at the two facilities was not as prominent or visible as in other hotels. In any case, that the Mumbai attackers pre-positioned explosives and other weapons for their use inside the hotel indicates they conducted extensive preoperational surveillance of the targets and likely understood the security countermeasures present in each location."\(^{140}\)

“India has accused a senior leader of the Pakistani militant group Lashkar-e-Taiba of orchestrating last week’s terror attacks that killed at least 172 people here, and demanded the Pakistani government turn him over and take action against the group. Just two days before hitting the city, the group of 10 terrorists who ravaged India’s financial capital communicated with Yusuf Muzammil and four other Lashkar leaders via a satellite phone that they left behind on a fishing trawler they hijacked to get to Mumbai, a senior Mumbai police official told The Wall Street Journal. The entire group also underwent rigorous training in a Lashkar-e-Taiba camp in Pakistan-controlled Kashmir, the official said.”\(^{141}\) Subsequently, two senior leaders of Lashkar-e-Taiba and 20 other alleged militants were arrested by Pakistan and the death toll was amended to 171.\(^{142}\)

Commenting on the incident, “What happened in Mumbai on November 26 will always remain etched in the minds of every Indian. The terrorists’ attack on iconic buildings and elsewhere has definitely raised the issue of security of high-rise buildings, both commercial and residential, in our country.”\(^{143}\)

“While the Taj and Oberoi hotels probably were attacked in part because of their status as Mumbai landmarks, the direct targeting of foreigners indicates the hotels also were chosen in a bid to strike Westerners.... The Mumbai attacks showed that attacking locations where Westerners are known to congregate, rather than attacks against marketplaces or cinemas that will primarily kill Indian nationals, could well be a more efficient and effective way for militants to use their limited resources. And as hotels and other traditional soft targets harden their facilities and implement new security countermeasures to prevent further Mumbai-style attacks, militants will seek less-secure venues that will achieve the same result. Such targets could include apartment complexes or neighborhoods that primarily house Westerners—similar to the 2004 attacks on the Saudi Arabian Oil Co. residential facilities in Al Khobar, Saudi Arabia—or other soft targets such as Western-style marketplaces or restaurants.”\(^{144}\)


\(^{142}\) Khalid Tanveer with contributions from Nahal Toosi and Zara Khan. Pakistan confirms Mumbai arrests. The Associated Press. <www.google.com/hostednews/ap/article/ALeqM5hkiMxbHNH0BqgpWA22ZG6VD6wVTmAD94VRHIC80>; December 15, 2008.


This incident bears close similarities to a previously planned attack known as the 1993 New York Landmarks Plot. According to Stratfor,

In July 1993, U.S. counterterrorism agents arrested eight individuals later convicted of plotting an elaborate, multistage attack on key sites in Manhattan. The militants, who were linked to Osama bin Laden’s then-relatively new group, al Qaeda, planned to storm the island armed with automatic rifles, grenades and improvised explosive devices (IEDs). In multiple raids on key targets combined with diversionary attacks, they aimed to kill as many people as possible.

The planned attack, which came to be known as the “Landmarks” plot, called for several tactical teams to raid sites such as the Waldorf-Astoria, St. Regis and U.N. Plaza hotels, the Lincoln and Holland tunnels, and a midtown Manhattan waterfront heliport servicing business executives and VIPs traveling from lower Manhattan to various New York-area airports. The militants carried out extensive surveillance both inside and outside the target hotels using human probes, hand-drawn maps and video surveillance. Detailed notes were taken on the layout and design of the buildings, with stairwells, ballrooms, security cameras and personnel all reconnoitered.

The attackers intended to infiltrate the hotels and disguise themselves as kitchen employees. On the day of the attack, one attack team planned to use stolen delivery vans to get close to the hotels, at which point heavily armed, small-cell commando teams would deploy from the rear of the van. Stationary operatives would use hand grenades to create diversions while attack teams would rake hotel guests with automatic weapons. The attackers planned to carry gas masks and use tear gas in hotel ballrooms to gain an advantage over any security they might come up against. They planned to attack at night, when the level of protection would be lower.

A little more than fifteen years later, the Nov. 26 attacks in Mumbai closely followed the script of the New York plot. Militants armed with AK-47s, grenades and military-grade explosives carried out a very logistically sophisticated and coordinated attack on the financial capital of India.

Bomb Threats

Bomb threats are delivered in a variety of ways. Sometimes a threat is communicated in writing, via e-mail, or by an audio recording. There is more than one reason for making or reporting a bomb threat. For instance, a caller who has definite knowledge or believes an explosive or incendiary device has been or will be placed may want to minimize personal injury or property damage. This caller could be the person who placed the device or someone who has become aware of such information. On the other hand, a caller may simply want to create an atmosphere of anxiety and panic, which will, in turn, disrupt the normal

---

145 Stratfor website (www.stratfor.com) December 3, 2008. From the New York Landmarks Plot to the Mumbai attack, Fred Burton and Ben West. <www.stratfor.com/weekly/20081203_new_york_landmarks_plot_mumbai_attack>; December 13, 2008. According to its website, “Stratfor is the world’s leading online publisher of geopolitical intelligence. Our global team of intelligence professionals provides our members with insights into political, economic, and military developments to reduce risks, to identify opportunities, and to stay aware of happenings around the globe…. Stratfor provides published intelligence and customized intelligence service for private individuals, global corporations, and divisions of the US and foreign governments around the world” (About Stratfor. <www.stratfor.com/about_stratfor>; December 13, 2008).
activities at the facility where the device is purportedly located. Whatever the reason for
the report, there will certainly be a reaction to it. Through proper planning, the wide vari-
ety of potentially uncontrollable reactions can be greatly reduced.

Daredevils, Protestors, and Suicides

The height of high-rise buildings may attract people who want to gain notoriety, publi-
cize a cause, or quickly end their own life.

Daredevils

In the 1970s, the newly constructed Twin Towers of the New York World Trade Center
were the scenes of three daring acts by a tightrope walker, a parachutist, and a climber.
The following details of these incidents were obtained from Twin Towers by Angus
Kress Gillespie.146

April 7, 1974, New York City—Starting at 7:15 AM, 24-year old French tight-
rope walker, Philippe Petit, walked back and forth seven or eight times on a
tightrope cable stretched between the roofs of the 1,350-foot high Twin Towers.
Three days before this heart-stopping display, Petit and three companions, all
disguised as construction workers, used a freight elevator to transport cables
and other equipment to the roof. On the night before the walk, they positioned
themselves on each roof and used a five-foot crossbow to shoot an arrow, with
a nylon fishing line attached, across from the north to the south Tower. Using
the line, they then strung across a 131-foot cable and secured it in place.

   The next morning, Petit nonchalantly walked back and forth between
   the towers for nearly 75 minutes, stopping at times to sit down, lie down,
   and even hang from his feet. So many spectators gathered to watch that it
   caused a giant traffic jam on the streets below. Eventually, Petit was per-
   suaded by a Port Authority police sergeant to come to the safety of the roof.

July 22, 1975, New York City—A skydiver parachuted from the north
tower roof to the plaza 1350 feet below. A New York Times reporter, Lee
Dembart, described how it was accomplished: “With his white parachute
concealed in a green bag, 34-year old Owen J. Quinn, of 30–42 23rd Street,
Astoria, eluded security guards on the 78th floor of the north tower, walked
to the roof above the 110th floor, jumped off at 4:45 PM, and landed less than
two minutes later on the raised ceremonial plaza between the buildings.”147
Apart from some cuts and bruises on his leg, caused by the wind blowing him
into the side of the building, he landed safely. Quinn, who said that he was
trying to draw attention to the plight of the poor, was booked on charges of
criminal trespass and reckless endangerment.

May 27, 1977, New York City—Starting at 6:30 AM, George W.
Willig, a 27-year old amateur mountain climber, using special equipment

147 Dembart L. Queens Skydiver Leaps Safely from Roof of the Trade Center. New York Times. July 23,
1975, as reported in Gillespie AK. Twin Towers: The Life of New York’s World Trade Center. Piscataway, NJ:
Rutgers University Press; 1999:142, 143.
that he designed to fit the window-washing equipment tracks, in three and a half hours climbed the outside of one of the Twin Towers. The spectacle was watched by thousands of onlookers on the ground and millions of viewers on television. When he safely reached the roof he was greeted by two police officers. Later, the city of New York sued him for a quarter of a million dollars to cover the costs of police overtime and the police helicopters that were dispatched to the scene to stop news helicopters from flying too close to the towers. The lawsuit was later dropped and Willig paid a $1.10 fine, which equated to a penny a floor.

An essential element in preventing the first two types of these acts is controlling access to building roofs. In the last type, it is important for a building’s perimeter to be controlled using security personnel, video surveillance, or a combination of both.

**BASE Jumping**

BASE is an acronym for Building, Antenna, Span (bridges), and Earth (cliffs). BASE jumping is a practice by which parachutists leap off high fixed objects.

Sometimes, high-rise building owners permit these jumps, particularly where a special film permit or sporting competition is being staged. For example, the *Los Angeles Times* reported that Petronas Towers, at the time the world’s tallest two buildings, was the site of the 2001 Malaysia International Extreme Skydiving Championships in Kuala Lumpur. However, in many jurisdictions these jumps violate trespassing and reckless endangerment laws. “In private, some veterans tell of concocting elaborate ruses involving forged employee passes, paying off security guards and removing air-conditioning grates, all to pull off a stealth building jump. In 2001, BASE jumpers were arrested or cited for parachuting off buildings in cities including Minneapolis, New York and Paris.”

“In a bid for credibility—and more legal jump sites—veteran jumpers are offering training sessions and camps that stress safety, and selling gear made especially for their sport.” According to Jean Potvin, a skydiver and physics professor, “The new BASE-specific gear is reliable, and the sport can be practiced safely by experienced jumpers if all goes well. But the ante is upped for those who want to jump off buildings, he said. Odd winds that swirl around high-rises could slam a parachutist into a window. Vision becomes tricky on a nighttime jump from a high-rise, when the backdrop is darkness and not sky blue. Jumpers must be able to steer their chutes away from power lines, telephone poles and other obstacles. All in a matter of seconds.”

Strictly controlling access to the roof is the way to stop BASE jumpers.

**Protestors**

Protestors have attempted to drape large banners promoting their raison d’être over the front of a building, and daredevils have used high-rises as their own personal stages to perform outlandish feats to gain attention, achieve notoriety, or simply to prove that they can do it.

---

149 ibid., p. E1.
150 ibid., p. E3.
Suicides
Numerous people have gone to a building’s roof and, tragically, committed suicide by jumping over the side. Some have scaled an upper floor wall facing a building atrium; climbed over an office, apartment, or hotel guestroom balcony wall or wrought-iron railing; climbed out of windows that can be opened; and even broken out a window on a floor and subsequently jumped to their deaths. Undoubtedly, in older high-rise buildings equipped with exterior fire escapes, some have used this means of escape as a means of death.

Daredevils, protestors, and suicides can also be a serious problem when a building is being constructed. Strict access control to the construction site is the key to preventing such incidents.

Elevator and Escalator Incidents

Elevators
Since the late 1970s, elevators have been developed with fully integrated, state-of-the-art microcomputer-based systems that analyze calls, set priorities, and dispatch cars on demand, enabling operators to control every aspect of elevator function. However, not all elevator systems located in high-rise buildings are this modern and sophisticated. Sometimes, despite rigid continuing-maintenance schedules, they may malfunction or break down.

Common elevator malfunctions include elevator cars that do not correctly align with the floor when they arrive there, elevator doors that do not close, and elevator cars that “slip” while in motion (possibly caused by stretching of the elevator cables used in traction elevators) or stall between floors, thereby entrapping occupants. If any of these conditions occurs, it must be reported promptly to management, engineering, or security staff, who in turn will notify the elevator company responsible for maintaining the equipment. The first three problems may result in temporary shutdown of the elevator for maintenance. Passenger entrapment, however, is a problem that requires immediate attention.

An elevator may momentarily stop and then immediately self-release the occupants, or it may stop completely and require an elevator technician to release the occupants (or, if a medical emergency occurs with a trapped occupant(s), the situation may necessitate calling the fire department or emergency services to deal with the situation). Attempts by a passenger to self-exit stalled elevators can have tragic consequences.

Sometimes crimes against persons—such as an assault (including that of a sexual nature) or a robbery—can occur within an elevator car, where, unless viewed by a video camera inside the car, often no one (apart from the victim of the assault or robbery) is present to witness the incident (because the perpetrator will usually not commit such a crime if anyone other than the intended victim is present).

A word of caution here is that with today’s telecommunications capabilities, one must be particularly careful when granting access to elevator programming functions. The following incident of using an elevator to commit theft illustrates this point:

For months there were thefts of desktop computers from various tenants distributed throughout a 39-floor office building. The modus operandi

*Information written with technical assistance from How to Operate Elevators under Emergency Situations. Otis Elevator Company, 5811.*
was always the same. The computers would disappear from locked tenant spaces after normal business hours. There were never any visible signs of unauthorized entry. Every conceivable pathway, the thief might have taken to remove the items from the building was examined. It was determined that the only possible means for removal of the items was using the single service/freight elevator. However, after normal business hours this elevator was always programmed to be “on security.” It was finally ascertained that the elevator was being taken “off security” for a time period that coincided with the thefts. Further investigation revealed that a building engineer had accessed the elevator system remotely from his home computer and changed the elevator’s security status. The engineer then had gone to the building and to the tenant floor using the freight elevator. The thefts were carried out using a building master key to gain access to the tenant suite. The stolen items were then loaded into the elevator car and transported down to the loading dock, where there were no CCTV cameras to view the incident. Later the elevator was then remotely placed back “on security.”

Also, acts of vandalism can occur inside elevator cars. A possible solution is to install vandal-resistant interiors. (“In general all lift [elevator] surfaces should be robust and resistant to damage from cleaning materials and body fluids. There should be no visible fixings[,] and gaps between moving parts should be restricted to avoid attack. Stainless steel is often specified in [a] hostile environment.”) Another mitigating measure is the use of elevator cars with transparent sidewalls in a transparent elevator shaft. However, the problem of elevator vandalism may be related to the operation of the elevator itself. As noted, “clearly, installing vandal-resistant interiors and control panels in the elevator cabs will reduce the number of incidents and costs to repair damage. But if you are having repeated incidents, look beyond the surface. Is the elevator system control system working properly? Long wait times and long travel times will increase frustration. And more frustration is going to spur more elevator vandalism.”

Despite the fact that elevators are a very safe form of transportation in modern high-rise buildings, elevator technicians and workers may sustain injuries or death while


working on or near elevator systems. Also, the passengers who use them are potentially at risk.

**Escalators**

Escalator riders can be the victims of petty theft by pickpockets and more serious crimes such as physical assaults. Escalators can also be the scene of injuries and deaths caused by loose shoelaces, heels of women’s shoes, unsuitable shoes, and loose clothing being caught in the moving stairs or handrails; riders (particularly young children and possibly older persons) slipping and falling, particularly when exiting the escalator; and escalator installers and repair persons being injured or killed while working on an escalator.**

Also accidents can occur when people try to travel in the opposite direction of the

---


Elevators and escalators are potential sources of serious injuries and deaths to the general public and to workers installing, repairing, and maintaining them (Staal J, Quackenbush J. Elevators, escalators and hoists. In: Stellman JM, ed. Encyclopaedia of Occupational Health and Safety. 4th ed., Vol III. Geneva: International Labour Office; 1998:40–44 [chapter 93]). Workers are at risk also, for instance, when cleaning elevator shafts, conducting emergency evacuations of stalled elevators, or doing construction near open shafts. The Bureau of Labor Statistics reported 68 elevator-related deaths from 1992-2003 among people using elevators while at work, an average of six passenger deaths per year. These included supervisors/managers, clerks/stock handlers, janitors/cleaners and their supervisors, plus a wide variety of other occupations. Almost all the fall deaths involved falls into elevator shafts, including 18 deaths where an elevator door opened and there was no elevator car. The “caught in/between” and “struck by” deaths often involved getting caught in the elevator door or between the elevator and door or shaft.


**According to “Deaths and Injuries Involving Elevators and Escalators: A Report of CPWR–Center for Construction Research and Training” (Revised July 2006), by Michael McCann and Norman Zaleski,

During this same period [1992–2003], the CPSC reported 24 non-work related deaths of elevator passengers in 12 states and the District of Columbia—about two per year. The states were Alabama (1 death), California (2), District of Columbia (3), Florida (1), Illinois (1), Maryland (1), Minnesota (3), Nevada (1), New York (3), Ohio (1), Virginia (1), Washington (2), and Wisconsin (2). The eight “caught in/between” deaths usually resulted after clothing became trapped at the bottom or top of an escalator or between a stair and escalator sidewall; seven of the 16 fall deaths were from head injury. Four of the fall deaths occurred due to falling off the escalator while riding the escalator sidewalls.

In 1994, the Consumer Product Safety Commission [CPSC] estimated that there were 7,300 escalator and 9,800 elevator injuries requiring hospitalization (CPSC. 1998. Escalator Safety. CPSC Document #5111. ,www.cpsc.gov/cpscpub/pubs/5111.html; Cooper David. 1997. Escalator Side-of-Step Entrapment. Presented at International Association of Electrical Engineers Elevcon '96, Barcelona, Spain. ,www.elevator-expert.com/escalator.htm.). The data were based on a nationwide survey of 90 hospitals. Based on the number of elevators and escalators in the United States, the CPSC estimated that there were 0.221 accidents per escalator and 0.015 accidents per elevator annually. The CPSC estimated that 75% of the escalator injuries resulted from falls, 20% from entrapment at the bottom or top of an escalator or between a moving stair and escalator sidewall, and 5% “other.” The “caught-in” incidents generally resulted in more serious injuries than did falls. Of particular concern is the fact that half of the approximately 1,000 sidewall-entrapment injuries involved children under age five (Armstrong D. US Urges Upgrade in Elevator Safety. Boston Globe; 1996b: July 21). The children’s injuries were mostly caused when a child’s hands or footwear (including dangling shoelaces) became caught in an escalator comb plate at the top or bottom of an escalator or in the space between moving stairs and an escalator sidewall

moving walkway (sometimes this happens when a person who has just boarded an escalator changes his or her mind and turns 180 degrees in the opposite direction and tries to walk back to the point where he or she boarded the escalator), when riders kneel or sit on the escalator steps, or when people do not hold onto the handrails.

**Fires**

As long as buildings have existed, the risk of fire occurring in them has been of special concern. “In terms of reported [high-rise building] fires, there are actually four property classes that dominate the statistics. Office buildings and hotels and motels are among them, but so are apartment buildings and hospitals (and other facilities that care for the sick).”

The threat of fire is always present in high-rise buildings. High-rise fires can be particularly dangerous to building occupants. “The most critical threats in high-rise structures include fire, explosion, and contamination of life-support systems such as air and potable water supplies. These threats can be actuated accidentally or intentionally, and because they propagate rapidly, they can quickly develop to catastrophic levels.”

Before proceeding, it is helpful to understand the makeup of fire and the behavior of building occupants when it occurs.

**Basics of Fire Science**

Fire is the combustion of fuels (whether solids, liquids, or gases) in which heat and light are produced. Combustion is a chemical reaction between a substance and oxygen that needs three factors to occur—fuel, oxygen, and heat—to occur. Removal of any one of these factors usually results in the fire being extinguished.

Within a high-rise building, there is an abundance of fuel, much equipment and furnishings being made from highly combustible synthetic materials. The centralized heating, ventilation, and air-conditioning (HVAC) systems ensure that there is a plentiful supply of oxygen within interior spaces. An accidental or deliberate application of heat to this scenario may have dire consequences to the life safety of occupants. When combustion occurs, heat can travel by moving from areas of high temperature to areas of lower temperature. This transfer is accomplished by means of conduction, convection, radiation, or direct contact with a flame (Figure 3–9).

Conduction is the movement of heat by direct contact of one piece of matter (whether solid, liquid, or gas, but most often a solid) with another. This heat transfer is crucial to the spread of a fire in a high-rise. For example, in a steel-framed building, when heat is conducted from one end along a steel beam that passes through a fireproof barrier, its other end can ignite materials.

Convection involves the movement of heat when a liquid or gas is heated, expands, becomes less dense, rises, and is displaced by lower temperature and, hence, denser liquid or gas. This denser liquid or gas is then heated and the process continues. The danger

---

*Some of this information was obtained from the Escalator Safety Guide. <www.safetyinfo.ca/pdf/ttc_escalator_safety_brochure.pdf>; December 20, 2008. More escalator safety information can be obtained from the Escalator, Elevator Safety Foundation (www.eesf.org, www.safetrider.org, www.asaferide.org).*  

of heat transfer by circulating air is heightened in high-rise buildings because when a fire occurs, convection currents can carry hot gases produced by combustion upward through floor-to-floor air-conditioning systems, elevator shafts, open stairshafts, dumbwaiters, mail chutes, laundry and linen chutes, unsealed poke-throughs,* and, in some high-rises, the exterior skin of a building—thereby spreading the fire to upper floors. This phenomenon is known as stack effect (Figure 3–10). Stack effect, as described by Quiter, “results from the temperature differences between two areas, usually the inside and outside temperatures, which create a pressure difference that results in natural air movements within a building. In a high-rise building, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke through the building.”155

Radiation is the movement of heat across a space or through a material as waves. Direct contact is self-explanatory.

*Poke-throughs are holes are cut through floors to allow the passage of conduits or ducts, primarily for the passage of electrical wiring, plumbing, heating, air-conditioning, communications wiring, or other utilities. Problems arise when the space between the conduit or the duct and the surrounding floor is not completely sealed with fire-resistant material, thereby negating the fire-resistance rating of the floor and potentially providing a passageway for deadly fire gases (Brannigan FL, Corbett GP. Brannigan’s Building Construction for the Fire Service. 4th ed. Ont. Canada: Jones and Bartlett Publishers; 2008:242).

Principal Threat to Life Safety

Smoke is usually the principal threat to building occupants’ life safety, and is the “total airborne effluent from heating or burning a material.” It may spread not only vertically between floors but also horizontally through a floor’s corridors, open spaces, conduits and ducts, and HVAC systems. Smoke may also spread rapidly through the concealed space that extends throughout the entire floor area of many steel-framed high-rises, especially if this space is used as a return plenum for the HVAC systems. Gann and Nelson stated,

>Along with heat, the burning of every combustible material or product produces smoke—gases and aerosols that, in sufficiently high concentration, present hazards to people in the vicinity. Products near those already burning may also contribute to the smoke as they decompose from exposure to the

---


*Product refers to a finished commercial item, and material refers to a single substance. Thus, for example, a chair (the product) is composed of several materials (e.g., a wooden frame, polyurethane padding, cotton batting, an aramid fire barrier, and a polyester/cotton cover fabric)” (Gann RG, Bryner NP. Combustion products and their effects on life safety. In: Fire Protection Handbook. 20th ed. Quincy, MA: National Fire Protection Association; 2008:6–11).
heat from the fire. Predominant among the hazards, which generally occur simultaneously, are the following:

- Sensory irritation of the upper and/or lower respiratory tract, which can affect speed of movement and the ability to negotiate escape and, at higher exposures, can lead to incapacitation or death
- Central nervous system depression resulting from inhalation of asphyxiant fire gases, which can, in ascending exposures, lead to impaired judgment, disorientation, loss of motor coordination, unconsciousness, and, ultimately, death
- Thermal effects, including hyperthermia and thermal burns of the skin and respiratory tract

Exposure to these hazards is often prolonged by eye irritation and diminished visibility due to smoke obscuration, which can affect the ability of occupants to see and negotiate escape routes efficiently. Survivors from a fire may also experience postexposure complications that can lead to delayed health effects or even death.157

Building Fires

For centuries, fires have been a threat to buildings. Some have led to the devastation of all or major portions of cities (for example, the burning of Rome in 64 AD; the great fire of London in 1666; the fire of Moscow in 1571 and 1812; the Hamburg, Germany, fire in 1842; the great fire in Quebec, Canada, in 1845; the Rangoon, Burma, fire of 1850; the great fire in Shanghai in 1894; the Great Chicago fire in 1871; the great fire of 1886 in Vancouver, Canada;158 the Ottawa-Hull fire of 1900 in Ontario, Canada;159 and the great earthquake and fire of San Francisco in 1906).160 From the early 1900s, the most deadly high-rise building fires have been as follows:

- Worst high-rise factory building fire. Asch Building Triangle Shirtwaist Company, New York City, New York, 1911: 146 killed
- Worst high-rise hotel building fire. Tae Yon Kak Hotel, Seoul, South Korea, 1971: 163 killed
- Worst high-rise office building fire. Joelma Building, São Paulo, Brazil, 1974: 179 killed
- Worst high-rise residential and apartment building fire. John Sevier Center, Johnson City, Tennessee, 1989: 16 killed

Table 3–3 lists significant fires\footnote{Although not a major event, the following incident highlights the fact that many times a fire is the result of one apparently innocuous but unsafe action. As reported in “5 injured in explosion at Westwood high-rise,”} in high-rise office buildings, hotel buildings, residential and apartment buildings, and mixed-use buildings. Included in the list is the

\begin{itemize}
  \item Worst high-rise factory building fire. Asch Building Triangle Shirtwaist Company, New York City, New York, 1911: 146 killed
  \item Worst high-rise hotel building fire. Tae Yon Kak Hotel, Seoul, South Korea, 1971: 163 killed
  \item Worst high-rise office building fire. Joelma Building, São Paulo, Brazil, 1974: 179 killed
  \item Worst high-rise residential and apartment building fire. John Sevier Center, Johnson City, Tennessee, 1989: 16 killed
\end{itemize}

160 Names and dates of these events were obtained from “Large Building Fires and Subsequent Code Changes,” by Jim Arnold, Clark County Department of Development Services, Building Division: Las Vegas, NV, p. 3, April 7, 2005.
Asch Building Triangle Shirtwaist Company fire because locked exits contributed to its high number of fatalities and underscored the need to move occupants to a safe area during fire incidents.\footnote{161}

Some of these incidents are addressed in more detail as follows.

**Table 3–3 Significant High-Rise Building Fires\footnote{162}**

<table>
<thead>
<tr>
<th>Date</th>
<th>Type of Building</th>
<th>Incident</th>
<th>Persons Killed/Injured</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 25, 1911</td>
<td>Factory</td>
<td>Asch Building Triangle Shirtwaist Factory Fire, New York City, New York</td>
<td>146 workers killed</td>
</tr>
<tr>
<td>June 5, 1946</td>
<td>Hotel</td>
<td>Hotel LaSalle, Chicago, Illinois</td>
<td>61 killed</td>
</tr>
<tr>
<td>December 7, 1946</td>
<td>Hotel</td>
<td>Hotel Winecoff, Atlanta, Georgia</td>
<td>119 killed, 90 injured</td>
</tr>
<tr>
<td>January 26, 1969</td>
<td>Hotel</td>
<td>Victoria Hotel, Dunnville, Ontario, Canada</td>
<td>13 killed\footnote{163}</td>
</tr>
<tr>
<td>December 25, 1971</td>
<td>Hotel</td>
<td>Tae Yon Kak Hotel, Seoul, South Korea</td>
<td>163 killed (greatest loss of life in a hotel building fire)</td>
</tr>
<tr>
<td>September 1973</td>
<td>Hotel</td>
<td>Copenhagen Hotel, Denmark</td>
<td>35 killed\footnote{164}</td>
</tr>
<tr>
<td>February 1, 1974</td>
<td>Office (bank)</td>
<td>Joelma Building, São Paulo, Brazil</td>
<td>179 killed, 300 injured (greatest loss of life in an office building fire)</td>
</tr>
<tr>
<td>July 12, 1979</td>
<td>Hotel</td>
<td>Zaragoza, Spain</td>
<td>76 killed\footnote{165}</td>
</tr>
<tr>
<td>November 21, 1980</td>
<td>Hotel</td>
<td>Prince Hotel, Kawaji, Japan</td>
<td>44 killed\footnote{166}</td>
</tr>
<tr>
<td>November 21, 1980</td>
<td>Hotel</td>
<td>MGM Grand Hotel, Las Vegas, Nevada</td>
<td>85 guests and hotel employees killed, approx. 600 injured</td>
</tr>
<tr>
<td>February 10, 1981</td>
<td>Hotel</td>
<td>Las Vegas Hilton Hotel, Las Vegas, Nevada</td>
<td>8 killed, 350 injured</td>
</tr>
<tr>
<td>March 6, 1982</td>
<td>Hotel</td>
<td>Westchase Hilton Hotel</td>
<td>12 killed (all guests on one floor)\footnote{167}</td>
</tr>
<tr>
<td>October 18, 1984</td>
<td>Hotel</td>
<td>Alexander Hamilton Hotel, Paterson, New Jersey</td>
<td>15 killed, more than 50 injured</td>
</tr>
<tr>
<td>December 31, 1986</td>
<td>Hotel</td>
<td>Dupont Plaza Hotel &amp; Casino, Puerto Rico</td>
<td>97 killed and more than 140 injured</td>
</tr>
</tbody>
</table>

(Continued)
Table 3–3 (Continued)

<table>
<thead>
<tr>
<th>Date</th>
<th>Type of Building</th>
<th>Incident</th>
<th>Persons Killed/Injured</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 29, 1987</td>
<td>Hotel</td>
<td>Hotel Concorde, Margarita, Venezuela</td>
<td>11 killed(^{168})</td>
</tr>
<tr>
<td>January 1, 1988</td>
<td>Hotel</td>
<td>First Hotel, Bangkok, Thailand</td>
<td>13 killed(^{169})</td>
</tr>
<tr>
<td>January 11, 1988</td>
<td>Mixed use</td>
<td>East 50th Street Apartment Building, Manhattan, New York</td>
<td>4 killed, 9 residents and 16 firefighters injured(^{170})</td>
</tr>
<tr>
<td>May 4, 1988</td>
<td>Office</td>
<td>First Interstate Bank Building, Los Angeles, California</td>
<td>1 building engineer killed, 40 injured</td>
</tr>
<tr>
<td>June 30, 1989</td>
<td>Office</td>
<td>Peachtree 25th Building, Atlanta, Georgia</td>
<td>5 killed, 26 injured (incl. 6 firefighters)</td>
</tr>
<tr>
<td>December 24, 1989</td>
<td>Residential</td>
<td>John Sevier Center, Johnson City, Tennessee</td>
<td>14 residents and 2 visitors killed, 50 (incl. 15 firefighters) injured (greatest loss of life in a residential building fire)</td>
</tr>
<tr>
<td>March 1, 1990</td>
<td>Hotel</td>
<td>Sheraton Hotel, Cairo, Egypt</td>
<td>18 people died and 70 were injured(^{171})</td>
</tr>
<tr>
<td>February 23, 1991</td>
<td>Office</td>
<td>One Meridian Plaza, Philadelphia, Pennsylvania</td>
<td>3 firefighters killed</td>
</tr>
<tr>
<td>January 6, 1995</td>
<td>Residential</td>
<td>Residential High-Rise, North York, Ontario, Canada</td>
<td>6 residents killed</td>
</tr>
<tr>
<td>November 20, 1996</td>
<td>Office</td>
<td>Garley Office Building, Hong Kong</td>
<td>40 killed (incl. 1 firefighter), 81 injured</td>
</tr>
<tr>
<td>July 11, 1997</td>
<td>Hotel</td>
<td>Royal Jomtien Resort, Pattaya, Thailand</td>
<td>91 hotel guests and staff killed, 51 injured</td>
</tr>
<tr>
<td>September 11, 2001</td>
<td>Office and hotel</td>
<td>New York World Trade Center, New York</td>
<td>2,749 killed and thousands injured</td>
</tr>
<tr>
<td>March 5, 2003</td>
<td>Hotel</td>
<td>Rand Inn International Hotel, Johannesburg, South Africa</td>
<td>6 people killed and 67 injured(^{172})</td>
</tr>
<tr>
<td>October 17, 2003</td>
<td>Office (government)</td>
<td>69 West Washington, Chicago, Illinois</td>
<td>6 killed and several injured</td>
</tr>
<tr>
<td>October 15, 2004</td>
<td>Office (government)</td>
<td>Parque Central, Caracas, Venezuela</td>
<td>Building unoccupied apart from several security staff who evacuated safely</td>
</tr>
<tr>
<td>February 12, 2005</td>
<td>Office</td>
<td>Windsor Building, Madrid, Spain</td>
<td>Building that was unoccupied apart from several security staff was demolished because of extensive fire damage</td>
</tr>
</tbody>
</table>

1911 Asch Building (Triangle Shirtwaist Company), New York City

According to the NFPA Centennial Edition,

_The Triangle Shirtwaist Company fire [the worst high-rise factory fire] [Figure 3–11] began on Saturday, March 25, 1911, at the Triangle Shirtwaist_


\(^{169}\)Ibid.


\(^{171}\)Hotel fires. Emergency & Disaster Management Inc. <www.emergency-management.net/hotel_fire.htm>; October 2, 2008.

\(^{172}\)Ibid.
Company's sweatshop for 625 workers on the eight, ninth, and tenth floors of the Asch Building.... Its cause has never been established, but investigators suspect that ash from a garment cutter's cigar or cigarette ignited a piece of material in a scrap bin on the eighth floor (Figure 3–11).

The 10-story building had only one exterior fire escape and just two staircases when it should have had three. In addition, one of its two freight
elevators was out of service. To prevent what some supervisors thought was an increase in pilferage, they’d further reduced the odds of escape by locking many of the exit doors.

As the fire spread unchecked, workers grabbed the standpipe hose line and tried to extinguish it, but they quickly found that the hose had rotted and the valves were frozen shut. In a panic, the workers surged towards the most familiar exits, where they were met with a wall of flame racing up the stairs. Those who could scrambled to another exit and discovered that the door was locked. When they tried to force it open, they found that the door swung inward, and the press of people jammed it shut.

Faced with a horrible death by fire, many of the workers, most of whom were young women, leapt to their deaths from the windows.

The fire, which killed 146 people, marked a turning point in the way U.S. fire protection codes address such occupancies.  

1946 Hotel LaSalle, Chicago, Illinois

On the night of June 5, a raging fire swept though much of the [Hotel LaSalle] and claimed the lives of sixty-one persons, including many children. Most of the dead succumbed not to the flames, but rather to asphyxiation when they opened their hotel room doors and their rooms filled with thick, black smoke....

The fire, though not particularly unusual in the context of early-twentieth-century hotel history, was devastating enough to prompt the city of Chicago to enact several new hotel-related building codes and fire-fighting procedures. These included the installation of automatic alarm systems, the posting of instructions in all hotel rooms of what to do in case of a fire, and increased use by the fire department of two-way radio devices.

1946 Hotel Winecoff, Atlanta, Georgia

According to an article in The Quarterly,

The Hotel Winecoff fire in the early morning hours of December 7, 1946, resulted in the death of 119 people and injuries to 90 others in this unsprinklered 15-story hotel.

“It is reported that the night manager attempted to warn the occupants of the guest rooms of the danger by house telephones, though the cramped halls and corridors on each floor were rapidly untenable and there was but the SINGLE STAIRWAY FOR EGRESS from the upper floors the position was hopeless for the occupants except for the possibility of rescue through the exterior windows.”

“Many persons lost their lives by jumping who might have been rescued had they remained in the building a few minutes longer.”

---

176ibid., p. 148.
Some contributing factors were as follows:

- “Delayed discovery and delayed alarm to the fire department.”\(^{177}\)
- “The fire spread from floor to floor through the unenclosed [unprotected] stairway by ignition of the combustible interior finish in the corridors and halls, aided by the draft produced through the open wood transoms over the wood doors to the guest rooms in which the exterior windows had been thrown open to await rescue or to obtain air to maintain life.”\(^{178}\)
- “More than half of the 195 transoms over the doors to guest rooms in the Wincoff were found in open position following the fire.”\(^{179}\) Closing the transoms would have “thus delayed the fire in the corridors from spreading rapidly into the rooms.”\(^{180}\)

“Automatic fire detection equipment, properly maintained, installed in the corridors (in rooms if the hotel management wished to protect the fool who smokes in bed) could have avoided the tragic delayed discovery altogether. Properly maintained automatic sprinkler protection for the corridors alone would have not only detected the fire but extinguished the fire in its incipient stage.”\(^{181}\)

As a result of the fire “important changes resulted in the codes and standards process: most notably, the recognition of the flammability of interior finish and the development of fire test standards.”\(^{182}\)

1974 Joelma Building, São Paulo, Brazil

February 1, 1974, São Paulo, Brazil—The Joelma Building, a 25-floor reinforced concrete, office building in São Paulo, Brazil, was the scene of the worst high-rise office building fire in history.

“An air conditioning unit on the twelfth floor overheated, starting a fire.\(^*\) Due to the fact that highly flammable materials had been used to construct it, the entire building was engulfed in flames within 20 minutes. By the time the fire was extinguished at 1:30 pm, of the 756 people in the building, 179 had been killed and 300 more were left injured.”\(^{183}\)

“The fire was discovered at around 8:50 am, and was reported to the São Paulo Fire Department approximately 15 minutes later, by an occupant of an adjacent building.”\(^{184}\) “Inside, the fire reached the building’s only

\(^{177}\) ibid., p. 149.
\(^{178}\) ibid., p. 148.
\(^{179}\) ibid., p. 154.
\(^{180}\) ibid.
\(^*\) Incendio a video produced by the National Fire Protection Association indicated that when the air-conditioning unit was installed, an electrical circuit breaker for it was not available. It had been installed in a manner that bypassed the floor’s electrical control panel (NFPA Media Productions, Technical Advisor, John Sharry, 1974). The video was based on information from a joint investigation of the National Fire Protection Association and the National Bureau of Standards, U.S. Department of Commerce.
\(^{183}\) ibid.
stairwell and climbed as high as the 15th floor. It did not reach any higher because of a lack of flammables in the stairwell, however it filled the well with smoke and heat, making it impassable.”

“Approximately 170 people went to the roof during the fire, in hopes of being rescued by helicopter. There was, however, no place clear enough or big enough for helicopters to land. Even if such had been put in, the strong heat and dense smoke made approaching the building by helicopter extremely hazardous. Some “people hid under the tiles on the roof of the building. They alone were found alive.” [Forty people jumped to their deaths trying to escape.]

“At the time, no emergency lights, fire alarms, fire sprinkler systems, or emergency exits were fitted to the building. There was only one stairwell, which ran the full height of the building. No evacuation plans had been posted in case of a fire.”

1980 MGM Grand Hotel, Las Vegas, Nevada

November 21, 1980, Las Vegas, Nevada—The MGM Grand Hotel fire resulted in the death of 85 persons, injury to about 600, and more than $30 million in property damage. The fire started at approximately 7:10 a.m. in a restaurant in the Main Casino and resulted in considerable smoke spread throughout the 23-story hotel building. There were approximately 3,400 registered hotel guests. Of the 79 body locations identified, 61 were in the high-rise tower and 18 on the casino level. The most probable cause of the fire was heat caused by an electrical fault in the restaurant.

According to the NFPA’s investigation study, the major contributing factors in this fire, and significant additional findings included the following:

- Rapid fire and smoke development on the Casino level due to available fuels, building arrangement, and the lack of adequate fire barriers.
- Lack of fire extinguishment in the incipient stage of the fire.
- Unprotected vertical openings contributed to smoke spread to the high-rise tower.

Substandard enclosure of interior stairs, smokeproof towers and exit passageways contributed to heat and smoke spread and impaired the means of egress from the high-rise tower.

---

185 ibid.
186 ibid.
187 Information from Incendio, a 10-minute video produced by the National Fire Protection Association (NFPA Media Productions: Quincy, MA; 1974).
189 Details of the MGM Grand Hotel fire were obtained from an NFPA investigation report (Richard Best and David P. Demers conducted the investigation) contained in “Special Data Information Package High-Rise Fires-Hotel and Motel Buildings” (Quincy, MA: National Fire Protection Association, One-Stop Data Shop; August 1999). Information obtained from article “Fire at the MGM Grand.” Fire Journal. NFPA International: Quincy, MA; 1982: 20–37.
190 Details of the MGM Grand Hotel fire were obtained from an NFPA investigation report (Richard Best and David P. Demers conducted the investigation) contained in “Special Data Information Package High-Rise Fires-Hotel and Motel Buildings” (Quincy, MA: National Fire Protection Association, One-Stop Data Shop; August 1999). Information obtained from article “Fire at the MGM Grand.” Fire Journal. NFPA International: Quincy, MA; 1982: 20–37.
Distribution of smoke throughout the high-rise tower through heating, ventilating and air conditioning equipment....

Smoke spread through elevator hoistways* to the high-rise tower....

The performance of automatic sprinkler protection in protected areas on the Casino level was excellent and halted the spread of fire into those areas. This performance is contrasted with extensive fire development and spread in non-sprinklered areas....

There was no evidence of the execution of a fire emergency plan, and there was some delay in notifying occupants and the fire department....

The number of exits and capacity of exits from the Casino at the time of the fire were deficient based on the 1981 Edition of NFPA 101, the Life Safety Code....

There was no evidence of manual fire alarm pull stations located in the natural path of escape on the Casino level....

There was no automatic means of returning elevators to the main floor in the event of fire thereby avoiding the boarding of elevators by occupants during the fire. Ten victims were found in elevators at the MGM Hotel....

An estimated 300 persons were evacuated from the roof of the high-rise tower.... Favorable factors in the MGM helicopter evacuation operation included clear weather, daylight hours, and the unusual availability of the participating Air Force helicopters.191

1981 Las Vegas Hilton Hotel, Las Vegas, Nevada

February 10, 1981, Las Vegas, Nevada—The fire [that started about 8:00 pm and resulted in eight deaths and 350 being injured] at the Las Vegas Hilton was incendiary in origin. The fire quickly developed in an elevator lobby on the eighth floor that had carpeting as its wall and ceiling finish. A flame front

*The hoistway is the “the structural component in which the elevators move in a building” (Emergency Evacuation Elevator Systems Guideline. Council on Tall Buildings and Urban Habitat: Chicago, IL; 2004:45).
**According to Hall and Cote,

The 1980 MGM Grand Hotel fire, in Las Vegas, Nevada, inspired an industry response that combined unprecedented widespread code compliance with fire safety provisions that often ran ahead of code requirements. The result has been a dramatic change both in the fire death toll in hotels and motels and in the use of proven fire protection systems in that industry,...

Led by strong industry associations and fire safety–conscious professionals at the major chains, the industry began to respond. In 1980, the year of the MGM Grand Hotel fire, sprinklers were reported present in only one of nine hotel or motel fires reported to U.S. fire departments. Detectors were reported present in just over one-fourth of reported hotel or motel fires.

An industry-sponsored study of sprinkler usage in 1988 found sprinklers present in roughly half of all properties, suggesting the percentage today is much higher still. The latest data show smoke detectors in more than 80 percent of hotel and motel fires and automatic sprinklers in 40 percent of hotel and motel fires and more than three-fourths of high-rise hotels. It is reasonable to assume that the new level of built-in fire protection had much to do with the dramatic drop in the number of hotel and motel fires since 1980. NFPA statistics from 1988 through 1997 indicated that sprinklers cut the chances of dying in a given fire by 91 percent and also reduced the average property loss per fire by 56 percent.

In terms of the deadliest fires, beginning in 1983, only two hotel or motel fires have killed 10 or more people, and each of them was on the outer fringes of the industry

that formed on the exterior of the building exposed each elevator lobby on the floors above primarily by radiation. The fire progressed vertically from floor to floor to the top of the building via the building’s exterior.192

Occupants who were trapped or who remained in their rooms and telephoned the hotel operators were told to put wet towels and sheets around the doors and wait for the fire department. Most of the smoke inhalation injuries occurred when guests opened their room doors or tried to evacuate the building.193

Four victims were found in guest rooms.... All the rooms had open doors to the corridor or evidence that corridor doors had been opened.... There were no fatalities in rooms in which occupants kept the doors closed and waited out the fire or waited for rescue.194

According to the NFPA’s fire investigation,

[T]he most significant factors that contributed to the fire spread and subsequent fatalities, injuries and damage in the fire incident were:

failure to extinguish the fire in its incipient stage and the presence of highly combustible carpeting on the walls and ceilings of the involved elevator lobbies contributing to the exterior fire spread. The resulting fire spread exposed a large number of the building’s occupants on multiple floors.195

“The person who initially called in the fire alarm to the security dispatcher was arrested, charged, and indicted for eight counts of homicide and arson. The individual was a hotel room service bus boy, and had been employed there only a few weeks.”196

1986 Dupont Plaza Hotel & Casino, Puerto Rico

December 31, 1986, San Juan, Puerto Rico—The Dupont Plaza Hotel and Casino fire [Figure 3–12] resulted in the death of 97 persons and over 140 injuries. The mid-afternoon fire resulted in smoke that spread to the 17-level hotel tower guest room floors.

Eighty four of the 97 fatalities were located in the casino.... Five fatalities occurred in the lobby area, three were found in a passenger elevator stopped between the basement and the first floor level, one fatality was in a guest room on the west side of the fourth floor, and two victims were found on the exterior of the building at the poolside bar ... like the five occupants trapped in the lobby, the 84 victims in the casino were caught by the violent extension of the fire through the casino/lobby level.197

Local authorities and the Bureau of Alcohol, Tobacco and Firearms (ATF) determined that the fire was deliberately lit amongst guest room

193ibid, p. 14.
194ibid., p. 15.
195ibid., p. ii.
196ibid., p. 17.
furniture temporally stored in a ballroom. Three persons were convicted of arson and imprisoned for sentences between 75 and 99 years.\textsuperscript{198}  

[According to the NFPA’s fire investigation,] four major factors contributed to the loss of life in the Dupont Plaza Hotel:

Lack of automatic sprinklers in the south ballroom (room of fire origin).
Rapid fire growth and spread.

\textsuperscript{198}ibid., p. 25.
Lack of automatic fire detection systems/inadequate exit for the casino.
Vertical opening between the ballroom and casino levels.

Additional findings:
Smoke movement to the high-rise tower by way of vertical penetrations.
Hotel tower occupants were not aware of a severe fire

Even though significant amounts of smoke, heat, and toxic gases penetrated the high-rise tower, especially on its lower levels, there was only one fatality in the tower. It is felt that exterior balconies provided occupants trapped for hours with a safe refuge area until the fire could be suppressed or they could be assisted by rescuers.

1988 First Interstate Bank Building, Los Angeles, California
May 4, 1988, Los Angeles, California—The First Interstate Bank Building fire (Figure 3–13), at 707 Wilshire Boulevard, resulted in the tragic death of a building engineer trapped in a service elevator that he used to travel to the initial fire floor to investigate the source of automatic fire alarms, smoke inhalation suffered by many of the 40 people located inside the office building at the time of the fire, and a loss estimated by the National Fire Protection Association Fire Analysis and Research Division at $50 million.

The fire started after normal business hours on the 12th floor of this 62-floor high-rise building. The Los Angeles Fire Department was first notified of it at 10:37 P.M. by a telephone call from a security officer at a neighboring building. Using 64 fire companies and 383 fire department personnel it was extinguished 3 hours and 42 minutes later on the 16th floor. The cause of the fire was never positively determined.

According to the NFPA's analysis of the fire,
the major factors that contributed to the loss of life and fire severity include:
the lack of automatic fire sprinklers on the floor of fire origin;
the delay in fire department notification following the internal automatic fire alarm;

---

199 ibid., p. v.
200 ibid.
••Severe fires in occupied office buildings during business hours are very rare, in large part due to the awareness of people in the building to unusual conditions. Occupants of high-rise office buildings are mobile, awake, and alert, and they are effective early detectors if they are adequately trained to summon help. When such alerting occurs, fires usually are in their initial phase of growth, when they can be controlled more easily. This illustrates the importance of occupant training that includes emergency fire notification procedures” (Klem TJ. “3 major high-rise fires reveal protection needs” [NFPA Journal. National Fire Protection Association: Quincy, MA; September/October 1992:61]).

201 Details of the First Interstate Bank Building fire were largely obtained from a video of the fire (Los Angeles Fire Department, Los Angeles, 1988).

••This delay was confirmed by the extent of the fire development when the fire department arrived at the building. “The first responding chief fire officer reported that a significant portion of the 12th floor was involved in flames” (Klem TJ. “3 major high-rise fires reveal protection needs” [NFPA Journal. National Fire Protection Association: Quincy, MA; September/October 1992:61]).
the absence of compartmentation[,] typical of an open office floor plan,* 
leading to rapid fire growth, development, and spread by means of combustible office furnishings; 
significant floor-to-floor fire extension by internal and external means; and

*Floor plan is defined as “architectural drawings showing the floor layout of a building and including precise room sizes and their relationships. The arrangement of the rooms on a single floor of a building, including walls, windows, and doors” (Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:66).
significant floor-to-floor smoke spread by way of stairways, elevators, utility shafts and penetrations, and HVAC ducts.  

Unsafe Investigation of the Fire Alarm

The death of the building engineer investigating the fire alarms was attributed to the fact that he took an elevator that directly penetrated the fire floor. To do so, he bypassed the building’s fire life safety system and rode a service elevator to the fire floor. On arrival at the 12th floor, the engineer began to open the metal elevator car doors, but they buckled because of the intense heat of a fire that had intruded into the elevator vestibule. As a result, the doors could not be closed and he died crying out for help on his portable radio.

Taking an elevator that can directly access the floor where a fire or fire alarm is occurring is extremely dangerous, particularly by nonfire department personnel who lack firefighter training, are not wearing protective clothing, and are not equipped with the breathing apparatus and forcible entry tools that firefighters have when they respond to fire incidents.

1989 Peachtree 25th Building, Atlanta, Georgia

June 30, 1989, Atlanta, Georgia—The Peachtree 25th Building fire resulted in the death of five occupants, including an electrician who apparently caused the fire, the injury of 20 building occupants and six firefighters, and direct property damage estimated at over $2 million. The fire began on the sixth floor of this 10-story office building at 10:30 a.m. on a Friday. “Caused by improper repairs to an electrical distribution system, this fire was an extreme, sudden, and intense fire.” The Atlanta City Fire Department extinguished the fire only after it had caused heavy damage to the sixth floor and to electrical rooms on the fourth and fifth floors.

According to the NFPA’s investigation of the fire, factors contributing to the loss of life and severity of the fire included the following:

- Unsafe actions by an electrician replacing a fuse in the sixth-floor electrical room while the electrical power was on.
- “The rapid development of a severe fire as a result of arcing in the electrical room.”
- The ignition of wall- and floor-finish materials in the exit-access corridor directly outside the electrical room, the door of which was open.
- “The absence of automatic sprinkler protection to control fire growth and spread in the exit-access corridor.”
- “The immediate blockage of the egress path due to both the location of the room of fire origin and the rapid spread of fire in the corridor”, and
- “Smoke apparently spread throughout the sixth floor in two ways. First, smoke from the fire in the room of origin quickly began to fill the corridor and advanced ahead of the flame front. The smoke entered the office spaces through doors that were left open, through cracks and openings around closed doors, and through

---

203 ibid., p. 62.
205 ibid.
206 ibid.
other natural cracks and voids such as small openings between the top of interior partitions and the suspended ceiling assemblies. Second, the ceiling collapsed outside the room of fire origin, and pressurized smoke quickly filled the plenum space that extended all over the office areas. This smoke then entered the offices through the ceiling vents used to collect return air and seeped through cracks and crevices in the ceiling assembly.”

1991 One Meridian Plaza, Philadelphia, Pennsylvania

February 23, 1991, Philadelphia, Pennsylvania—The One Meridian Plaza fire resulted in the tragic death of three firefighters because of smoke inhalation and destroyed eight floors of this 38-story high-rise office building. The fire started on the 22nd floor at 8:23 p.m. It was caused by “spontaneous ignition of improperly stored linseed-soaked rags that were being used to restore and clean.” Eighteen and one-half hours later, the Philadelphia City Fire Department declared it under control on the 30th floor (the first floor above the fire floor that had an automatic sprinkler system).

According to the NFPA,

The following significant factors affected the outcome of the fire:
- the lack of automatic sprinklers on the floor of fire origin;
- the effectiveness of automatic sprinklers on the 30th floor which, supplied by fire department pumpers, halted the fire’s vertical spread;
- the lack of early detection of the incipient fire by automatic means;
- inadequate pressures for fire hoses because settings of pressure-reducing valves were too low for the specific application in this building;
- the improper storage and handling of hazardous materials, producing both the initial ignition and rapid early fire growth; and
- the early loss of the building’s main electrical service and emergency power.

Unsafe Investigation of the Fire Alarm

In this fire, when the first automatic fire alarm was received from the 22nd floor, a maintenance worker almost lost his life when he took an elevator to investigate the source of the alarm, leaving a security guard at the first-floor desk. “When he reached that floor and the elevator doors opened, he encountered heat and dense smoke. The man dropped to the floor, notified the security guard of the fire by portable radio, and told the guard that he could not close the elevator doors. However, he was able to tell the guard how to override the elevator controls so the guard could return the elevator to the first floor. The guard gained control of the elevator, and the maintenance man returned safely to the ground level.”

---

207 ibid, p. 55.
211 ibid., p. 58.
1995 Residential Building, North York, Ontario, Canada
January 6, 1995, North York, Ontario, Canada—At approximately 5:00 a.m., a fire in a residential high-rise building led to the deaths of six residents. “All were found on upper stories in exit stairways. The fire appeared to have been ignited by the improper disposal of smoking materials and initially involved a couch in a fifth-floor apartment. The fire caused severe damage to the apartment and to an exit access corridor.”

“After unsuccessfully attempting to extinguish the fire, the occupant in the apartment of fire origin left without closing the dwelling unit door to the corridor. Fire and smoke passed through the open door into the exit access corridor and made that corridor untenable for many fifth-floor residents. The residents who did not escape early in the incident stayed in their apartments until they were rescued by firefighters. The combination of closed doors and noncombustible walls prevented untenable conditions and deaths from occurring in other fifth-floor apartments.... In many instances, the people who remained in their apartments or moved to the balconies were exposed to less risk to their safety than those who attempted to escape.”

Based on the NFPA’s investigation of this fire,

The following significant factors were considered as having contributed to the loss of life and property in this incident:

- Lack of automatic sprinkler protection
- Lack of door self-closing devices on apartment entrance doors
- Vertical smoke movement due to stack effect
- Staff who were not trained with respect to managing fire emergencies in the building for which they were responsible
- Lack of fire safety training for building residents
- Voice communication equipment that could not transmit messages that were understood by residents.

“The events in this incident point directly to the importance of being able to reliably communicate information to residents and the need for resident training so that residents are able to make an educated decision on whether to evacuate or to stay in place during a fire emergency.”

1996 Garley Office Building, Hong Kong

November 20, 1996—Fire ripped through the 16-story Garley commercial building. Flames funnelled up the elevator shaft like a giant Bunsen burner, killing 40 people, including a firefighter, and injuring 81 others, many of whom were unable to escape from the buildings upper floors. Investigators later determined that the blaze started when sparks and molten metal fell onto combustible materials stacked in an elevator shaft during a welding operation.

---

213 ibid., pp. 1, 2.
214 ibid., p. 2.
215 ibid.
As a result of the fire, authorities learned how disastrous poor housekeeping and a lack of fire safety education can be in old high-rises. Smoke doors on the top floors had been wedged open, allowing rapid fire spread, and no safety precautions had been taken while the elevators were being repaired. Many of the building’s residents and occupants used the elevators exclusively and didn’t even know the location of the stairwells.\(^{216}\)

1997 Royal Jomtien Resort, Jomtien Beach, Thailand, Hotel

According to the NFPA Fire Journal,

At approximately 10:20 a.m. on July 11, 1997, a fire began in a ground-floor coffee shop at the [17-story] Royal Jomtien Resort. The fire killed 91 hotel guests and staff and seriously injured 51. The fire, which started when LP-Gas leaking from a portable cylinder ignited, did substantial damage to the resort.

Staff members smelled what they thought was gas emanating from the buffet area of the coffee shop. Investigating its source, a staff member noticed that gas was leaking from the valve assembly of a 9-kilogram (20-pound) liquid propane gas cylinder. The man tried to shut down the cylinder’s main control valve. However, he inadvertently turned the valve the wrong way and, instead of shutting off the flow of gas, actually increased it. The vapor, expanding as it was released, quickly ignited.

A combination of combustible wood-and-vinyl-covered furnishings in the area of fire origin, the combustible decor of the coffee shop, the wooden decor of the complex, and the lack of any active fire suppression systems allowed the fire to develop rapidly.

Combustible interiors, the westerly breeze, and the lack of fire separation, compartmentation, and active suppression systems allowed the fire to spread rapidly through the lower levels of the complex. As the fire grew, the lack of pressurization in the stairwell, the lack of self-closers on many of the upper-level doors, and the lack of firestopping in the service shafts allowed smoke to penetrate the upper levels, causing the hotel to fill with smoke.

According to the local police officers responsible for the initial investigation, the sister of one of the hotel’s senior managers had fled the area of the fire before she realized that no one had begun to evacuate the resort’s guests. When she re-entered the complex to do so, she was overcome by the fire.\(^{217}\)

2001 New York World Trade Center, New York

This incident is addressed earlier in this chapter as an aircraft collision.

2003 69 West Washington, Chicago, Illinois

October 17, 2003 Chicago, Illinois—The 37-story Cook County Administration Building fire resulted in six deaths and several injuries. The victims were found in a stairwell,

\(^{216}\) Anderson C. “Hong Kong’s high-rise fire safety campaign” (NFPA Journal. National Fire Protection Association: Quincy, MA; May/June 2001:1).

several floors above the fire floor. The fire originated in a storage room on the 12th floor of this unsprinklered office building.

Compartmentalization contained the fire damage to a single office suite. Closed solid core doors and ... gypsum board partition walls limited the fire damage in rooms, on both the north end and south end of Suite 1240. However, the partition walls did not extend above the drop ceiling. The lack of partitions above the drop ceiling allowed for the rapid spread of smoke and fire gases throughout the 12th floor and then throughout the building, through penetrations, HVAC ducts, and open doors.\(^{218}\)

At approximately 5:00 pm, on October 17, 2003, an occupant of suite 1240 smelled smoke, alerted the other occupants in the suite and began to evacuate the suite. Another occupant of Suite 1240 found a small fire on top of a set of wall shelves in the storage room, under a ceiling mounted light fixture.... The remaining occupants left the suite, after notifying security via telephone.\(^{219}\)

Chicago Fire Department (CFD) logged in a call to 911 by a security officer at 5:02:29 p.m. and arrived at the building at 5:06:30 p.m.\(^{220}\)

The fire was reported as “knocked down” at 6:07:45 p.m.\(^{221}\)

According to the Report of the Cook County Commission Investigating the 69 West Washington Building Fire of October 17, 2003,

Victims were found in the southeast stairwell of the 37-story office building after that stairwell filled with smoke. All of the fatalities were attributed to smoke inhalation. The southeast stairwell filled with smoke at approximately 5:15 P.M. to 5:20 P.M. after members of the Chicago Fire Department opened the stairwell door on the 12th floor, which was the floor where the fire was located. The opening of the door irretrievably compromised the stairwell as a safe escape route. Approximately 80 minutes after opening the door, the Fire Department searched the stairwell above the 14th floor for the first time. The Fire Department discovered the victims within a few minutes after beginning that search.\(^{222}\)

Based on its investigation, the Commission has concluded that the six deaths and the serious injuries that occurred in the fire would not have


\(^{219}\)Ibid, p.3.

\(^{220}\)Ibid.

\(^{221}\)Ibid., p. 4.

occurred if the building had been equipped with fire sprinklers and/or had stairwell doors that automatically unlocked in the event of a fire.\textsuperscript{223}

“Therefore, the fatalities (and much of the damage) could have been avoided by the presence of sprinklers. What was learned from this fire? Perhaps only that the knowledge that is already known should be applied. Sprinklers greatly increase the safety of buildings, and locked stairwells, even from the stair side, create a hazard.”\textsuperscript{224}

2004 Parque Central, Caracas, Venezuela

According to the NFPA Fire Journal,

Sometime before midnight on October 15, 2004, a fire began on the 34th floor of the East Tower of the Parque Central, a 56-story government [reinforced concrete] office building in Caracas, Venezuela, and South America’s tallest high-rise. Fortunately, the building was unoccupied at the time, except for a handful of security personnel who evacuated safely.

Despite the fact that a sprinkler system had been installed in the Parque Central the fire did more than U.S. $250 million in damage, burning the structure’s contents from the 34th floor to the 50th. Why? Because, as previous inspections revealed, the sprinkler system had not been properly tested or maintained, thus it wasn’t in a working condition; the building designers said local fire alarm panels weren’t connected to a building-wide panel; and the standpipe system was inoperable at the time of the fire.\textsuperscript{225}

Past history and performance shows that this fire could probably have been controlled quickly by a standard wet-pipe sprinkler system and that the fire department’s chances of controlling the fire at, or a few floors above, the floor of fire origin would have increased if the standpipe system had been working. This fire highlights the importance of periodic inspection, testing, and maintenance of fire protection systems, as well as the importance of strictly following manufacturers’ installation instructions.\textsuperscript{226}

2005 Windsor Building, Madrid, Spain

“On the night of February 12, 2005, a fire started in the Windsor building [Edificio Windsor] in Madrid, Spain, a 32-story tower framed in steel-reinforced concrete. At its peak, the fire, which burned for almost a day, completely engulfed the upper ten stories of the building. More than 100 firefighters battled to prevent the uncontrollable blaze from spreading to other buildings.”\textsuperscript{227}

\textsuperscript{223} ibid., p. 2. The report contains detailed conclusions and recommendations, “For more information on this report or to received the full version of the report and supporting documentation, contact the Fire Commission attorney” (Cook County Info Center. <www.co.cook.il.us/fire_reportreport.htm>; March 26, 2008).


\textsuperscript{226} ibid., p. 52.

“The fire apparently caused the collapse of the top floor spans surrounding the still-standing core structure of the ten uppermost floors.”

According to Arup,*

The long delay** between detection and fire brigade*** intervention played an important role in allowing the unsprinklered fire to grow out of control. In addition the rapid spread of the fire above the 21st Floor appears to be due to failure of the compartmentation measures between the facade detail and the floor which is intended to prevent vertical fire spread.

Fire safety design in many countries relies heavily on sprinkler protection to prevent fire growth and thereby limit possibilities for fire spread via the facade. The lack of sprinklers, along with the failure of compartmentation, appears to be an important factor in this case.

Although there is a requirement to fire stop**** the gap between the slab edge and the inside of the curtain wall, most codes do not address the tie-back connection of the curtain wall to the structure. Therefore a light facade structural element can heat up quickly and the resulting expansion can produce an outward bulging away from the slab edge, which can create internal flues if it happens before the facade glazing breaks. In other words by not considering the thermo-mechanical response of the system, there are no provisions to prevent such damage in Building Codes worldwide.

An added complication in the case of Edificio Windsor was that the curtain wall facade had recently been replaced and it appears that a new support structure had been fixed onto the outside of the original mullion and transom arrangement. This means that there would have been a double-layered gap that needed to be fire stopped, complicating this detail still further....

Lessons to be learned

Procedures to ensure early call out to the Fire Brigade
Provisions for speedy access to the fire floor via protected fire fighting lifts and use of wet risers

---

* As stated on its website Arup is “a global firm of designers, engineers, planners and business consultants.” The article by Arup states that “The following is an Arup view based upon what is known about the fire event in conjunction with our structural fire design and analysis experience. It has been prepared based upon information in the public domain only and will be updated as further information becomes available” (Madrid Windsor fire: the Arup view. <www.arup.com/fire/feature.cfm?pageid=6150>; October 11, 2008).


*** A group of people organized to engage in rescue, fire suppression, and related activities” (NFPA Glossary of Terms. National Fire Code. Quincy, MA: National Fire Protection Association; 2005). Fire brigades are usually public agencies. However, if a facility is large enough it may have a proprietary or an in-house fire brigade.


Effective compartmentation measures, including sprinkler protection for high-rise buildings

Good coordination of fire safety measures with refurbishment works and programme, especially in an occupied building

Structural fire full frame analysis, rather than single element small-scale fire tests, as a basis for design.\textsuperscript{230}

Fire Alarms

Fire alarms are significant events in high-rise buildings. A fire alarm is “a signal initiated by a fire alarm-initiating device such as a manual fire alarm box, automatic fire detector, watering switch, or other device in which activation is indicative of the presence of a fire or fire signature.”\textsuperscript{231} As Bryan explained, “The primary purpose of a fire detection system is to respond to a fire, and to transform this response into a visual-audible signal which should alert the building’s occupants and the fire department that a fire has been initiated. The fire detection system is intended to respond to the initial signs, signals, or stimuli which indicates that a fire has begun.”\textsuperscript{232} (See the section titled “Manual Fire Alarm Stations” in Chapter 6 for the sequence of events caused by fire alarms in modern high-rise buildings.)

 Whenever a fire or a fire alarm occurs, all building occupants need to be alerted to the existence (or possible existence) of fire and to initiate emergency procedures. All occupants should be evacuated in a prompt, safe, and orderly fashion according to procedures established in the building emergency management plan.

When a Fire Emergency Is Faked

“Some of the life-safety requirements [for a high-rise structure] actually pose unique security difficulties. The code provision which insists upon unimpeded exit during a building emergency means that if such an emergency can be faked, egress may be possible under little or no surveillance. Even if the emergency is genuine, it may occur at a time when the security forces are unprepared for the joint demands of emergency response and heightened security attention.”\textsuperscript{233} For example, in a high-rise office building, an individual could set off a fire alarm by activating a manual fire alarm station. This should result in the evacuation of occupants from that floor, and floors above and below the incident (the actual number of floors will depend on the emergency plan for the building concerned). After all occupants have left, the person could then quickly roam unchallenged through offices and steal items (including possibly from handbags and billfolds in coats left behind in the hurry to evacuate). The thief could then enter a stairwell, descend to the ground level, and freely walk out of the building.

Two individuals could similarly stage such an event to gain unauthorized entry to a floor that is normally secured (i.e., the elevators only proceed to the floor if authorized

\textsuperscript{230}ibid.


access cards are used). One person could activate a manual fire alarm station on one floor, thereby causing the stairwell doors to unlock automatically (if this feature is provided) throughout the building. An accomplice waiting in a stairwell on the targeted floor could then proceed into the tenant space (sometimes stairwells lead directly into tenant areas rather than into common corridors) and gain access to commit a crime. Afterward, the thief could then board a passenger elevator—because during fire alarm situations in many modern high-rise buildings, the elevators remain in service unless a smoke detector in the elevator lobby, elevator shaft, or elevator machine room has been activated or the elevators have been manually recalled from the Fire Command Center—or reenter the stairwell and proceed down to the ground level to exit the building. Some buildings require security staff to manually recall all elevators serving floors in alarm to prevent occupants from using them during fire and fire alarm situations. This practice has the added advantage of securing the floor from unauthorized access using elevators.

The following measures can be considered to maintain security during a fire or fire alarm:

1. If stairwells lead directly into tenant areas, consider redesigning the space to remove this security hazard.
2. Train building occupants to always take personal valuables with them during evacuation and, if such actions do not place them in danger, to quickly secure other valuable assets.
3. Position video cameras with alarm-activated recording capability in tenant high-risk areas (particularly where valuables such as cash and high-value assets are located) and in building stairwells close to the ground-level exits to at least obtain a record of an incident.

Hazardous Materials, Chemical and Biological Weapons, and Nuclear Attack

A hazardous material is “a substance (solid, liquid, or gas) capable of creating harm to people, property, and the environment.” Such a substance may be corrosive, explosive, flammable, irritating, oxidizing, poisonous, radioactive, or toxic in effect. Hazardous materials may be chemical, biological, or nuclear in nature.

In the high-rise setting, hazardous materials may be in a building for legitimate operational purposes or be maliciously introduced into the building in order to harm people.

Hazardous Materials

Hazardous materials in a high-rise building may include a variety of substances that will vary according to the type of occupancy. Such materials may include diesel fuel for the building’s emergency generator, cleaning materials for use by janitorial staff, construction materials, and chemicals such as chlorine for swimming pools and hot tubs.

---

*The automatic recall of elevators may vary from country to country, city to city, depending on the requirements of the authority having jurisdiction.

The following hazardous materials, as mentioned in *Hazardous Materials in an Office Environment*, may be present within a high-rise office building, some of which may be present in other high-rise occupancies:

- Photographic materials such as fixer solutions
- Printing/reproduction/art materials such as inks, thinners, solvents, ammonia, and paint
- Liquid office materials such as cleaners and pesticides
- Maintenance supplies and materials such as oils, engine fluids, transformer dielectrics [insulators\(^{235}\)], lead acid batteries, paints, thinners, solvents, and fluorescent light tubes
- Janitorial and cleaning materials such as cleaners containing solvents, acids, caustics, chlorine compounds, pesticides, and polishes
- Renovation and construction materials (such as varnishes, paints, coatings, glues, sealant, asbestos, and compressed gas)\(^{236}\)

All hazardous materials should be identified, their characteristics documented, and instructions provided for their safe handling.*

The presence of hazardous materials in a building can cause serious problems, particularly when an explosion occurs. The following example illustrates this point.

**April 25, 2002, New York, New York**—A late-morning explosion caused by volatile chemicals severely damaged the façade, hailing sheets of glass and debris onto the street, of a 10-story Manhattan commercial building. The blast that originated in the basement was possibly linked to shipments of 50-gallon drums of acetone used by a sign company. “The explosion, which rocked the busy commercial neighborhood, triggered mass evacuations of surrounding buildings and caused widespread alarm in the area, witnesses said.”\(^{237}\) In all, 42 people were injured in the incident.\(^{238}\)

---


*For example, in the United States, businesses, by law, must identify known hazardous materials and provide a Material Safety Data Sheet (MSDS) for each such chemical located onsite. As Fischer and Green (Fischer RJ, Green G. *Introduction to Security*. 6th ed. Stoneham, MA: Butterworth-Heinemann; 1998:284) explain,

Each MSDS contains seven sections:
1. Product identification and emergency notification instructions
2. Hazardous ingredients list and exposure limits
3. Physical and chemical characteristics
4. Physical hazards and how to handle them (that is, fire, explosion)
5. Reactivity—what the product may react with and whether it is stable
6. Health hazards—how the product can enter the body, signs and symptoms of problems, and emergency first-aid steps
7. Safe handling procedures

Also, all polychlorinated biphenyl (PCB) transformers used in or near a commercial building are required by law to be registered with the building owner, who is responsible for maintaining records and adhering to reporting provisions. (Note: After the World Trade Center’s destruction on September 11, 2001, trace amounts of PCBs were found at the site of 7 WTC, the building that housed two electrical substations [Collapsed 7 WTC contained toxic chemicals. *Pasadena Star News*. Pasadena, CA: January 20, 2002]).


\(^{238}\)Ibid.
The types of hazardous materials outside a high-rise building may include PCBs (as already mentioned), radioactive substances in a nearby nuclear facility, potentially dangerous materials transported along an adjacent or under-building railway line or roadway, or flammable and potentially harmful chemicals contained in a nearby chemical manufacturing plant or oil refinery.

As previously stated, “the most critical threats in high-rise structures include fire, explosion, and contamination of life-support systems such as air and potable water supplies. These threats can be actuated accidentally or intentionally, and because they propagate rapidly, they can quickly develop to catastrophic levels.” Therefore, to minimize or eliminate the hazards to people, property or the environment, every hazardous material incident should be handled by building emergency staff according to standard operating procedures (described later in the sample Building Emergency Procedures Manual in Chapter 9).

Chemical and Biological Weapons

The threat of chemical and biological weapons (CBW) has existed for some time in the modern world. However, since the mid-1990s, the potential for the use of CBW against civilians has dramatically increased. “As early as 1995, European intelligence officials learned that chemical and biological warfare instructions disseminated from Al Qaeda sources in Pakistan and Afghanistan were circulating among Islamic terrorist cells. That year, Belgium police seized what turned out to be an 8,000-page guerilla manual for jihad. One chapter, titled ‘How to Kill,’ described how to prepare ‘toxins, toxic gas and toxic drugs.’”

According to the U.S. Centers for Disease Control and Prevention,

[A] *bioterrorism attack is the deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death in people, animals, or plants. These agents are typically found in nature, but it is possible that they can be changed to increase their ability to cause disease, be resistant to current medicines, or spread into the environment. Biological agents can be spread through the air, through water, or in food. Terrorists may use biological agents because they can be extremely difficult to detect and do not cause illness for several hours to several days. Some bioterrorism agents, like the

---


smallpox virus, can be spread from person to person, and some, like anthrax, cannot.\textsuperscript{241}

The potential for deliberate contamination of buildings with toxic chemical substances, such as sarin gas or hydrogen cyanide, and dangerous biological material, such as anthrax (\textit{Bacillus anthracis}) and ricin, is a concern, particularly due to several high-profile incidents involving sarin gas and anthrax.

\textit{March 1995, Tokyo, Japan}—A Japanese cult terrorist group deliberately released sarin gas on a Tokyo subway. It killed 13 people and caused 5,000 more to seek medical attention. “First responders had difficulty in identifying the odorless, colorless chemical and in knowing how to simultaneously protect themselves, handle mass casualties and stop the toxin from spreading in the subway system. Some of the deaths included subway maintenance workers who rushed to the scene and unknowingly touched, breathed in and further agitated the lethal nerve agent.”\textsuperscript{242}

\textit{September 2001, East Coast United States}—Five anthrax-contaminated letters were mailed to two Democratic senators and news media (CBS, NBC, and the New York Post). These letters were received soon after the September 11, 2001, terrorist attacks on the New York World Trade Center and the Pentagon and led to the deaths of five people and 17 others being infected. According to Barbara Rosenberg, a molecular biologist, “The anthrax discovered in the letters mailed to the two U.S. senators was so refined that it contained 1 trillion spores per gram, characteristic of the ‘weaponized’ anthrax made by U.S. defense labs.”\textsuperscript{243}

On July 29, 2008, the suspected perpetrator of these attacks, U.S. government microbiologist Bruce Ivins, died of an apparent suicide while under investigation for these crimes.\textsuperscript{244}

The difference between a chemical and biological attack is that “a biological [and radiological] agent will almost never cause immediate symptoms; a chemical agent almost always will.”\textsuperscript{245}

\textbf{Nuclear Attack}

As unlikely as a nuclear attack may be, the events of September 11, 2001, have brought the widespread realization that certain individuals in this world will stop at nothing to achieve their objectives. Therefore, a nuclear attack needs to be addressed as a possible threat to high-rise buildings situated in major urban centers.

\textsuperscript{241}Dealing with Today’s Asymmetric Threat to U.S. and Global Security, summary of the personal remarks at the May 2008 symposium co-sponsored by CACI International (CACI) and the National Defense University (NDU) (CACI International; 2008:31).

\textsuperscript{242}“Sensors of chemical warfare agents make a mass-transit debut” (\textit{Corporate Security}, Corporate Security Publishing, ssbrooks@gateway.net, July 14, 2000, p. 2).

\textsuperscript{243}Neuman J. Scientists weigh in with deductions on anthrax killer. \textit{Los Angeles Times}. April 21, 2002: A20.


\textsuperscript{245}Berkeley Lab. Berkeley Lab researchers develop concise website on handling chemical-biological attacks against buildings (U.S. Department of Energy’s Lawrence Berkeley National Laboratory. <http://securebuildings.lbl.gov>); April 3, 2002. Site development was led by Phillip Price).
“Nuclear Terrorism denotes the use, or threat of the use, of nuclear or radiological weapons in acts of terrorism, including attacks against facilities where radioactive materials are present. In legal terms, nuclear terrorism is an offense committed if a person unlawfully and intentionally ‘uses in any way radioactive material … with the intent to cause death or serious bodily injury,’ according to international conventions.”

The Institute of Real Estate Management states,

>The immediate effects of a nuclear attack are unmistakable: a flash of intense light followed by a blast of heat and radiation. Likewise, the secondary effect is [well] known … radioactive fallout. The degree of immediate and secondary effects will depend on the size and type of weapon, the terrain (hilly versus flat), the height of the explosion (e.g., near or far from the ground), the distance from the explosion, and weather conditions.

People near the explosion most likely would be killed or seriously injured by the initial blast, heat, or radiation. Those several miles away from the explosion would be endangered by the initial blast, heat, and subsequent fires. Others probably would survive but would be affected by radioactive fallout. It is for these people that an emergency plan must be provided.

The only precaution that a property manager can take to prevent loss due to a nuclear attack is to provide an emergency shelter for occupants, employees, and others at the property at the time of such an attack. Such a shelter could be a special building, underground bunker, or any space with walls and roof thick enough to absorb radioactive waves given off by fallout.

“... There is also growing concern about so-called dirty bombs, [or a radiological dispersal device (RDD)] laced with radioactive material from a hospital, nuclear plant or manufacturing facility, for instance, that can contaminate the environment.”

A dirty bomb uses conventional explosives to spread radioactive material.

>Depending on the type and quantity of radioactive material used in a device and variables such as weather conditions and the size of particles released, the impact of an RDD attack could vary greatly.

---

246 Dealing with Today’s Asymmetric Threat to U.S. and Global Security, summary of the personal remarks at the May 2008 symposium co-sponsored by CACI International (CACI) and the National Defense University (NDU) (CACI International; 2008:31).


248 Term “radiological dispersal device (RDD)” stated in “Cleanup after a radiological attack,” by Elizabeth Parker (The Nonproliferation Review, Fall-Winter 2004:167).


experts generally agree that an RDD is most appropriately characterized as a weapon of mass disruption, rather than mass destruction. A typical attack would result in few, if any, immediate casualties from radiation exposure, but the ensuing contamination would likely prompt widespread panic, causing significant economic and psychosocial damage.\textsuperscript{251} Long-term economic consequences, moreover, could be very significant if affected areas included major commercial or industrial sites and could not be readily restored to public use.\textsuperscript{252}

Such a weapon could be hand-carried into a building concealed in a suitcase.

Kidnappings and Hostage Situations

Kidnapping is “the forcible abduction or stealing and carrying away of a person.... A person is guilty of kidnapping if he unlawfully removes another from his place of residence or business, or a substantial distance from the vicinity where he is found, or if he unlawfully confines another for a substantial period in a place of isolation, with any of the following purposes: (a) to hold for ransom or reward, or as a shield or hostage; or (b) to facilitate commission of any felony or flight thereafter; or (c) to inflict bodily injury on or to terrorize the victim or another; or (d) to interfere with the performance of any governmental or political function.”\textsuperscript{253} High-rise buildings may be the site of kidnappings of business executives, wealthy citizens, children involved in custody battles, political hostages, diplomats, politicians, and other individuals.

A hostage is “an innocent person held captive by one who threatens to kill or harm him if his demands are not met.”\textsuperscript{254}

High-rise buildings have been the site of hostage-taking situations, examples of which follow:

1982, First Interstate Bank Building, Los Angeles, California—A man entered this 62-story high-rise office building, accosted the building’s chief engineer in the main lobby, and demanded to be taken to the roof. On reaching it, he then tried to obtain publicity for a cause he was promoting—in this case, that smoking is bad for your health. Building management immediately called the police department, and after a tense standoff, the individual eventually surrendered without anyone being injured.

March 11, 2002, Rembrandt Tower, Amsterdam, Holland—On a Monday morning, shortly after most businesses in the tallest building in the Dutch capital opened, a man armed with explosives and two guns took control of the 35-story office building.


\textsuperscript{252}Parker E. Cleanup after a radiological attack. The Nonproliferation Review. Fall-Winter 2004:168, 169.


The gunman held as many as 18 people hostage in the building’s main lobby, and more than 200 people were trapped in their offices. After seven hours, the gunman shot himself. All hostages were freed unharmed. Reportedly, the gunman was protesting the advertising practices of a major electronics firm that was previously headquartered in the high-rise.255

December 8, 2006, Citigroup Center, Chicago, Illinois—“Joe Jackson forced a security guard at gunpoint to take him up to the 38th floor offices of Wood, Phillips, Katz, Clark & Mortimer, which specialized in intellectual property and patents. He carried a revolver, knife and hammer in a large manila envelope and chained the office doors behind him, the police said.

“Jackson, 59, told the police before he was shot that he had been cheated over a toilet he had invented for use in trucks, Superintendent Phil Cline of the Police Department said Saturday…. The gunman who fatally shot three people in a law firm’s high-rise office before he was killed by police felt cheated over an invention.”256

“The building was locked down during the siege. Occupants of the other offices were instructed to lock themselves into their offices and not to venture out into the halls. The lockdown took place for 45 minutes. All Metra Train services [a train station is located at the building] were shut down until 5:00 pm, while the crime scene was considered active.”257

Labor Disputes, Demonstrations, and Civil Disorder

Events such as labor disputes, demonstrations, and civil disorder can have a significant impact on the day-to-day operation of a high-rise building. Their effects will be influenced by the nature of the incident, the number of persons participating in it, the conduct of the participants, the response of building management and involved outside agencies, and the location of the incident in relation to the building.

Labor Disputes

Labor disputes may be peaceful affairs where orderly groups of persons assemble outside the building; quietly display placards, signs, and banners to passing motorists; pass out leaflets explaining their cause; and present petitions to the parties involved. They can, however, be violent events, where large groups of angry persons protesting a labor issue pertaining to the building, or one of its tenants, throw rocks and various other objects in an attempt to forcibly enter the building or surround the building to prevent occupants and visitors from entering or leaving.

Demonstrations

A demonstration is a gathering of people for the purposes of publicly displaying their attitude toward a particular cause, issue, or other matter. Such an activity, if carried out

peacefully on public property, is permissible. However, the activity must not obstruct, block, or in any way interfere with the ingress to and egress from private property such as a high-rise building. As with a labor dispute, a demonstration may vary from a peaceful affair to a violent one.

Civil Disorder

Civil disorder is “any public disturbance involving acts of violence by assemblages of three or more persons, which causes an immediate danger of or results in damage or injury to the property or person of any other individual.”

Civil disorder is known as a civil disturbance. A riot is “a form of civil disorder characterized by disorganized groups lashing out in a sudden and intense rash of violence, vandalism or other crime. While individuals may attempt to lead or control a riot, riots are typically chaotic and exhibit herd behavior.... Riots typically involve vandalism and the destruction of private and public property. The specific property to be targeted varies depending on the cause of the riot and the inclinations of those involved. Targets can include shops, cars, restaurants, state-owned institutions, and religious buildings.”

Medical Emergencies

Medical emergencies that can occur in high-rise buildings range from people choking to drug overdoses, from respiratory emergencies to seizures, from food poisoning to dental emergencies, and from serious injury to suicide. Because building populations are made up of people often working under pressure and stress, there is always the possibility of heart attacks or strokes.

Natural Disasters

Natural disasters may be earthquakes, tsunamis, volcanoes, heat waves, storms (non cyclone, tornadoes, and tropical cyclones [cyclones, hurricanes, and typhoons]), and floods and landslides.

Earthquakes

\[\text{The foundations of the earth shake.}\]
\[\text{The earth is broken asunder,}\]
\[\text{The earth is split through,}\]
\[\text{The earth is shaken violently.}\]

—Isaiah 24:18–19

Earthquake is “a term used to describe both sudden slip on a fault, and the resulting ground shaking and radiated seismic energy caused by the slip, or by volcanic or magmatic

---


activity, or other sudden stress changes in the earth.” Earthquakes range from an almost indiscernible tremble of the ground to the violent shaking of a major quake. This shaking is sometimes side-to-side and other times up-and-down; it can last for a few seconds or for several minutes.

When earthquakes occur, the strength and duration of the shaking largely determines the potential for damage. Some earthquakes are preceded by smaller quakes called foreshocks, some occur suddenly with no forewarning, some occur in groups of approximately the same magnitude (called swarms or clusters), and some are followed by smaller quakes called aftershocks.

According to McNally,

> Probably the best-known gauge of earthquake intensity is the local Richter magnitude scale, developed in 1935 by United States seismologist Charles F. Richter. This scale, commonly known as the Richter scale, measures the ground motion caused by an earthquake. Every increase of one number in magnitude means the energy release of the quake is about 32 times greater. For example, an earthquake of magnitude 7.0 releases about 32 times as much energy as an earthquake measuring 6.0. An earthquake with a magnitude of less than 2.0 is so slight that usually only a seismometer can detect it. A quake greater than 7.0 may destroy many buildings. The number of earthquakes increases sharply with every decrease in Richter magnitude by one unit. For example, there are 8 times as many quakes with magnitude 4.0 as there are with magnitude 5.0.

Although large earthquakes are customarily reported on the Richter scale, scientists prefer to describe earthquakes greater than 7.0 on the moment magnitude scale. The moment magnitude scale measures more of the ground movements produced by an earthquake. Thus, it describes large earthquakes more accurately than does the Richter scale.

### Earthquake History

Table 3–4 details major known earthquakes that have occurred in the world.

The U.S. Geological Survey states that

> Although it may seem that we are having more earthquakes, earthquakes of magnitude 7.0 or greater have remained fairly constant throughout this century and, according to our records, have actually seemed to decrease in recent years. There are several reasons for the perception that the number of earthquakes, in general, and particularly destructive earthquakes is increasing.

1. A partial explanation may lie in the fact that in the last twenty years, we have definitely had an increase in the number of earthquakes we have been able to locate each year. This is because of the tremendous increase in the number of seismograph stations in the world and the many improvements in global communications.

---


Table 3–4 Earthquakes with 50,000 or More Deaths

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Deaths</th>
<th>Magnitude</th>
<th>Comments</th>
</tr>
</thead>
</table>
| January 23, 1556 | Shensi (Shaanxi or Shanxi), China | 830,000 | ~8        | Deadliest earthquake on record. “In the winter of 1556, an earthquake catastrophe occurred in the Shaanxi and Shanxi Provinces. In our Hua County, various misfortunes took place. Mountains and rivers changed places and roads were destroyed. In some places, the ground suddenly rose up and formed new hills, or it sank in abruptly and became new valleys. In other areas, a stream burst out in an instant, or the ground broke and new gullies appeared. Huts, official houses, temples, and city walls collapsed all of a sudden.”

| July 27, 1976    | Tangshan, China               | 255,000 (official) | 7.5      | Official casualty figure is 255,000 deaths. Estimated death toll as high as 655,000. This is probably the greatest death toll from an earthquake in the last four centuries and the second greatest in recorded history. |

| August 9, 1138   | Aleppo, Syria                 | 230,000 | Not available | The third largest earthquake in the world since 1900 and the largest since the 1964 Prince William Sound, Alaska, earthquake. In total, 227,898 people were killed or were missing and presumed dead, and about 1.7 million people were displaced by the earthquake and subsequent tsunami in 14 countries in South Asia and East Africa. The tsunami caused more casualties than any other in recorded history and was recorded nearly worldwide on tide gauges in the Indian, Pacific, and Atlantic oceans. |

| December 26, 2004 | Sumatra                       | 227,898 | 9.1       |                                                                 |

| December 22, 856 | Damghan, Iran                 | 200,000 | Not available | It was felt from the Yellow Sea to Qinghai (Tsinhai) Province and from Nei Mongol (Inner Mongolia) south to central Sichuan (Szechwan) Province. There were large numbers of landslides and ground cracks throughout the epicentral area. Some rivers were dammed, others changed course. |

| December 16, 1920 | Haiyuan, Ningxia (Ning-hsia), China | 200,000 | 7.8       |                                                                 |

(Continued)

---


<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Deaths</th>
<th>Magnitude</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 23, 893</td>
<td>Ardabil, Iran</td>
<td>150,000</td>
<td>Not available</td>
<td>Extreme destruction in the Tokyo-Yokohama area from the earthquake and subsequent firestorms. Although often known as the Great Tokyo Earthquake (or the Great Tokyo Fire), the damage was apparently most severe at Yokohama. A tsunami was generated in Sagami Bay with wave heights as high as 12 m (39 ft) on O-shima and 6 m (20 ft) on the Izu and Boso Peninsulas.</td>
</tr>
<tr>
<td>September 1, 1923</td>
<td>Kanto (Kwanto), Japan</td>
<td>142,800</td>
<td>7.9</td>
<td>Extreme damage in Ashgabat (Ashkhabad) and nearby villages, where almost all brick buildings collapsed, concrete structures were heavily damaged, and freight trains were derailed.</td>
</tr>
<tr>
<td>October 5, 1948</td>
<td>Ashgabat (Ashkhabad), Turkmenistan (Turkmeniya, USSR)</td>
<td>110,000</td>
<td>7.3</td>
<td>At least 86,000 people killed, more than 69,000 injured, and extensive damage in northern Pakistan. At least 82,000 people killed and severe damage in the Dujiangyan-Mianzhu-Mianyang area. Landslides blocked roads and buried buildings in the Beichuan-Wenchuan area.</td>
</tr>
<tr>
<td>October 8, 2005</td>
<td>Pakistan</td>
<td>86,000</td>
<td>7.6</td>
<td>Over 40% of the population of Messina and more than 25% of Reggio di Calabria killed by the earthquake and tsunami, as well as by fires in some parts of Messina. Casualty toll is based on census data 1901–1911, some estimates are as high as 110,000. Tsunami heights of 6–12 m (20–39 ft) observed on the coast of Sicily south of Messina and heights of 6–10 m (20–33 ft) observed along the coast of Calabria. Aftershocks continued into 1913.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Deaths</th>
<th>Magnitude</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 31, 1970</td>
<td>Chimbote, Peru</td>
<td>70,000</td>
<td>7.9</td>
<td>About 50,000 people were killed—20,000 missing and presumed dead—and 150,000 injured in Ancash and La Libertad Departments from the earthquake and a catastrophic debris avalanche of rock, ice, and mud which buried the town of Yungay, which had a population of about 20,000.</td>
</tr>
<tr>
<td>November 1, 1755</td>
<td>Lisbon, Portugal</td>
<td>70,000</td>
<td>8.7</td>
<td>This earthquake occurred on All Saint's Day while many of the 250,000 inhabitants of Lisbon were in church. Stone buildings swayed violently and then collapsed on the population. Many who sought safety on the river front were drowned by a large tsunami. Fire ravaged the city.</td>
</tr>
<tr>
<td>January 11, 1693</td>
<td>Sicily, Italy</td>
<td>60,000</td>
<td>7.5</td>
<td>“The 1693 earthquake was a disastrous event affecting eastern Sicily, southern Italy, where it caused over 60,000 victims and total destruction of several villages and towns in the districts of Siracusa, Ragusa, and Catania. The earthquake was followed by a tsunami that struck the Ionian coasts of Sicily and the Messina Strait and was probably observed even in the Aeolian Islands.”</td>
</tr>
<tr>
<td>1268</td>
<td>Silicia, Asia Minor</td>
<td>60,000</td>
<td>Not available</td>
<td></td>
</tr>
<tr>
<td>June 20, 1990</td>
<td>Western Iran</td>
<td>40,000 to 50,000</td>
<td>7.4</td>
<td>Estimated 40,000 to 50,000 people killed, more than 60,000 injured, 400,000 or more homeless and extensive damage and landslides in the Rasht-Qazvin-Zanjan area, Iran. Nearly all buildings were destroyed in the Rudbar-Manjil area.</td>
</tr>
<tr>
<td>February 4, 1783</td>
<td>Calabria, Italy</td>
<td>50,000</td>
<td>Not available</td>
<td></td>
</tr>
</tbody>
</table>


Note: Some sources list an earthquake that killed 300,000 people in Calcutta, India, on October 11, 1737. Recent studies indicate that these casualties were most likely due to a cyclone, not an earthquake. (Source: The 1737 Calcutta Earthquake and Cyclone Evaluated by Roger Bilham, BSSA, Vol. 84, No. 5, 1650–1657, October 1994.)

Names in paraentheses () indicate what the town/region was called at the time of the earthquake.

---

In 1931, there were about 350 stations operating in the world; today, there are more than 4,000 stations and the data now comes in rapidly from these stations by telex, computer and satellite. This increase in the number of stations and the more timely receipt of data has allowed us and other seismological centers to locate many small earthquakes which were undetected in earlier years, and we are able to locate earthquakes more rapidly.

The NEIC now locates about 12,000 to 14,000 earthquakes each year or approximately 35 per day. Also, because of the improvements in communications and the increased interest in natural disasters, the public now learns about more earthquakes. According to long-term records (since about 1900), we expect about 18 major earthquakes (7.0–7.9) and one great earthquake (8.0 or above) in any given year. However, let’s take a look at what has happened in the past 32 years, from 1969 through 2001, so far. Our records show that 1992, and 1995–1997 were the only years that we have reached or exceeded the long-term average number of major earthquakes since 1971. In 1970 and in 1971 we had 20 and 19 major earthquakes, respectively, but in other years the total was in many cases well below the 18 per year which we may expect based on the long-term average.

2. The population at risk is increasing. While the number of large earthquakes is fairly constant, population density in earthquake-prone areas is constantly increasing. In some countries, the new construction that comes with population growth has better earthquake resistance; but in many it does not. So we are now seeing increasing casualties from the same sized earthquakes.

3. Better global communication. Just a few decades ago, if several hundred people were killed by an earthquake in Indonesia or eastern China, for example, the media in the rest of the world would not know about it until several days, to weeks, later, long after such an event would be deemed “newsworthy.” So by the time this information was available, it would probably be relegated to the back pages of the newspaper, if at all. And the public Internet didn’t even exist. We are now getting this information almost immediately.

4. Earthquake clustering and human psychology. While the average number of large earthquakes per year is fairly constant, earthquakes occur in clusters. This is predicted by various statistical models, and does not imply that earthquakes that are distant in location, but close in time, are causally related. But when such clusters occur, especially when they are widely reported in the media, they are noticed. However, during the equally anomalous periods during which no destructive earthquakes occur, no one deems this as remarkable.

A temporal increase in earthquake activity does not mean that a large earthquake is about to happen. Similarly, quiescence, or the lack of seismicity, does not mean a large earthquake is going to happen. A temporary increase or decrease in the seismicity rate is usually just part of the natural variation in the seismicity. There is no way for us to know whether or not this time it will lead to a larger earthquake. Swarms of small events, especially in
geothermal areas, are common, and moderate-large magnitude earthquakes will typically have an aftershock sequence that follows. All that is normal and expected earthquake activity.\textsuperscript{270}

In many parts of the world, modern high-rise buildings in areas subject to earthquake activity are constructed in accordance with strict building codes. Older buildings erected before seismic design considerations may need structural retrofits to bring them up to code. The effect of earthquakes on a high-rise building depends on factors such as the building’s location in relation to the quake’s epicenter, type of soil or rock beneath the structure, magnitude of the quake, duration of the shaking, type of motion the structure is subjected to, and the building’s design and construction. The shaking of an earthquake may cause no structural damage, or it may cause damage so severe that the building collapses. Modern high-rise buildings can be seismically designed to withstand certain magnitude earthquakes. “The idea of earthquake-proof construction is unrealistic, unless exceptionally expensive measures are taken. Any building will collapse if the ground under it shakes hard enough or becomes permanently deformed. But structures can be designed and constructed to incorporate a high degree of earthquake resistance.”\textsuperscript{271}

As Dames and Moore/URS Corporation explained, “To resist seismic forces, steel buildings are either constructed with braced frames (such as X-bracing) or moment frames (rigid beam-column assembly).”\textsuperscript{272} Many structures, particularly seismically designed steel-framed buildings, have been constructed to flex and move without breaking. Lower floors may shake more rapidly, but movement of the building from side to side is greatest on uppermost floors. “To dissipate the force of the ground shaking through a tall structure, the building is designed to sway\textsuperscript{273} as a unit in a side-to-side motion.”

Case Study: 1994, Northridge Earthquake
January 17, 1994, Northridge, California—At 4:31 a.m. an earthquake of magnitude 6.7 rocked the heavily populated San Fernando Valley. It severely impaired the public transportation network and residential community; 72 people were killed and 11,846 people were treated for earthquake-related injuries. “30 of the 72 Northridge deaths


\textsuperscript{271}Kimball V. Earthquake Ready, 2nd ed. Santa Monica, CA: Roundtable Publishing, Inc., 1988:42. (Kate Hutton, Technical Advisor, is a staff seismologist at the California Institute of Technology.)


\textsuperscript{273}Kimball V. Earthquake Ready, 2nd ed. Santa Monica, CA: Roundtable Publishing, Inc.; 1988:106. (Kate Hutton, Technical Advisor, is a staff seismologist at the California Institute of Technology.)
were attributed to heart attacks.” Thousands were left homeless in the wake of this disaster that had an insured loss of $12,500,000,000.

The January 17, 1994, Northridge earthquake raised some serious safety concerns about the degree of earthquake resistance that high-rise buildings, in particular steel moment frame structures, afford. Unlike braced frames, these moment frames feature larger beams and columns, with additional welding or bolting of the connections. Before this earthquake, this structural system was thought to be among the safest seismically. As John Hall, an associate professor of civil engineering at the California Institute of Technology, pointed out,

During the 1994 Northridge earthquake, many modern steel buildings suffered unexpected fractures in welded beam-to-column connections. Although none of these buildings collapsed, fractured connections are a serious matter since they reduce the lateral strength of the structure, and, thereby, increase the risk of collapse. The problem is apparently widespread and, at this point, one must assume that any welded steel moment-frame is susceptible to this type of connection failure.

The following comments regarding this situation were written shortly after the quake in *The Northridge Earthquake, January 17, 1994, A Special Report* by Dames and Moore/URS Corporation:

Steel moment frame buildings have generally been considered very effective in resisting seismic forces. However, the high intensity of the Northridge earthquake pushed even steel moment frame buildings to their seismic limits, causing damage not experienced before. More than 50 relatively new 2- to 10-story structures that sustained brittle structural damage have been identified at the time of writing this report. Such damage raises troubling questions about the seismic resistance of this type of construction. Damage took the form of cracks in welds and rupture of steel sections at connections of beams to columns and columns to the base plate—both areas are critical for stability of the structure. Steel-framed buildings are designed to absorb energy by bending without breaking. However, the failure of welded connections would not allow the level of bending assumed in design and can cause brittle failures. Steel members in existing buildings are covered with fireproofing and are not readily available for inspection. Thus, damage caused by the quake may go unnoticed unless a detailed and costly inspection program is undertaken. The damage to steel moment frame buildings has potentially the highest structural significance of the Northridge earthquake and will probably result in substantial research and associated design code changes.

---

274 Reich K. “Study raises Northridge quake toll to 72,” results of a study by Michael E. Durkin, a Woodland Hills public health researcher as reported in the *Los Angeles Times* (December 20, 1995:A1).


After this disaster, the city of Los Angeles by ordinance required that owners of steel moment frame buildings inspect for damage, and the Federal Emergency Management Agency (FEMA) subsequently prepared guidelines to address this potential hazard.

Even though issues about weld cracks in steel-framed construction were the most startling results of the quake, the failures of concrete-framed parking structures were among the most dramatic (Figure 3–14). As the *Engineering News Record* reported, “In response to such collapses, federal officials anticipate a new treatment of parking structures in the National Earthquake Hazard Reduction Program’s 1997 provisions, to serve as a basis for model codes.”

During a severe earthquake, occupants and building contents will be shaken. Items not properly secured may fall; desks and furniture may slide; filing cabinets and bookcases may topple; ceiling tiles may be dislodged; windows may crack or shatter; sprinkler heads may shear off and result in water discharge; seismic devices may cause building elevators to go to the nearest floor in the direction of travel, stop, automatically open elevator car doors, and then cease operation; automatic fire detection and reporting equipment may produce multiple false alarms; electrical power may be disrupted; lights may go off; the telephone system may be damaged or, shortly after the shaking has stopped, be deluged with calls. Falling objects will often cause injuries.

Soil liquefaction, landslides, and fires are common results of major earthquakes. Liquefaction occurs in areas where loose soils with a high water table are present. “As the earthquake causes water to percolate up through the loose soil, it creates quicksand. Heavy objects such as buildings and other structures may sink or tilt into the liquefied soil.”\(^{279}\) Fires can result from fuel spillage, rupturing of gas lines, and the many ignition

---


sources available in urban areas. If the earthquake is a major one, public fire fighting capabilities will be severely strained because of extraordinary demands for service, difficulties in transporting equipment along damaged or blocked roadways and freeways, and possible disruption of the public water supply.

**Tsunamis**

A tsunami is “a large wave caused by earthquakes, submarine landslides, and, infrequently, by eruptions of island volcanoes. During a major earthquake, an enormous amount of water can be set in motion as the seafloor moves up and down. The result is a series of potentially destructive waves that can move at more than 500 miles [805 kilometers] per hour.”

“Tsunamis travel at high speed through deep water (350 [563 kilometers] to 500 miles [805 kilometers] per hour) with modest wave heights (inches or feet) that have wavelengths that are hundreds of kilometers long. These open ocean tsunamis are imperceptible to humans, but can be detected by water pressure sensors on the ocean floor. When it reaches shallower coastal waters, the tsunami slows down, causing its wave height to build rapidly. Tsunamis are common in the Pacific Ocean and less frequent in the Indian and Atlantic Oceans.”

(See Table 3–5 for a listing of major tsunamis that have occurred in the world.)

**Table 3–5** Major Tsunamis Worldwide

<table>
<thead>
<tr>
<th>Date</th>
<th>Origin</th>
<th>Effects</th>
<th>Death Toll</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 7, 1692</td>
<td>Puerto Rico Trench,</td>
<td>Port Royal, Jamaica, permanently submerged. “Generated by earthquake.”</td>
<td>2,000</td>
</tr>
<tr>
<td></td>
<td>Caribbean</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1707</td>
<td>Japan</td>
<td>“Generated by earthquake.”</td>
<td>30,000</td>
</tr>
<tr>
<td>November 1, 1755</td>
<td>Atlantic Ocean</td>
<td>Lisbon, Portugal destroyed. “Generated by earthquake.”</td>
<td>60,000</td>
</tr>
<tr>
<td>February 20, 1835</td>
<td>Peru-Chile Trench</td>
<td>Concepción, Chile destroyed.</td>
<td>Not known</td>
</tr>
<tr>
<td>August 8, 1868</td>
<td>Peru-Chile Trench</td>
<td>Ships washed ashore several miles inland; Town of Arica destroyed. “Generated by earthquake.”</td>
<td></td>
</tr>
<tr>
<td>August 27, 1883</td>
<td>Krakatau (Krakatoa)</td>
<td>Devastation in East Indies. “Generated by eruption of volcano.”</td>
<td>36,000</td>
</tr>
<tr>
<td>June 15, 1896</td>
<td>Japan Trench</td>
<td>Swept the east coast of Japan, with waves of 100 feet (30.5 meters) at Yoshihimama. “Generated by earthquake.”</td>
<td>27,122</td>
</tr>
<tr>
<td>December 28, 1908</td>
<td>Sicily, Italy</td>
<td>East coast of Sicily, including Messina, and toe of Italy badly damaged. “Earthquake and 8 m [26 feet] wave.”</td>
<td>58,000</td>
</tr>
</tbody>
</table>

(Continued)
### Table 3-5 (Continued)

<table>
<thead>
<tr>
<th>Date</th>
<th>Origin</th>
<th>Effects</th>
<th>Death Toll</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 1, 1923</td>
<td>Kanto (Kwanto), Japan</td>
<td>Although often known as the Great Tokyo Earthquake (or the Great Tokyo Fire), the damage was apparently most severe at Yokohama. A tsunami was generated in Sagami Bay with wave heights as high as 12 m (39 ft) on O-shima and 6 m (20 ft) on the Izu and Boso Peninsulas.</td>
<td>142,800²⁹¹</td>
</tr>
<tr>
<td>March 3, 1933</td>
<td>Japan Trench</td>
<td>9,000 houses and 8,000 ships destroyed in Sanriku district, Honshu.</td>
<td>3,000</td>
</tr>
<tr>
<td>April 1, 1946</td>
<td>Aleutian Trench</td>
<td>Damage to Alaska and Hawaii. &quot;Generated by earthquake.&quot;²⁹³</td>
<td>159</td>
</tr>
<tr>
<td>May 22, 1960</td>
<td>South-central Chile</td>
<td>Coinciding with a week of earthquakes. &quot;The largest earthquake (magnitude 9.5) of the 20th century.&quot;²⁹⁴ Damage to Chile and Hawaii.</td>
<td>1,500 (61 in Hawaii)</td>
</tr>
<tr>
<td>March 27, 1964</td>
<td>Anchorage, Alaska</td>
<td>Severe damage to south coast of Alaska. &quot;An earthquake and subsequent landslides generated a series of tsunamis.&quot;²⁹⁵</td>
<td>115</td>
</tr>
<tr>
<td>August 23, 1976</td>
<td>Celebes Sea</td>
<td>Southwest Philippines struck, devastating Alicia, Pagadian, Cotabato, and Davao. &quot;Generated by earthquake.&quot;²⁹⁶</td>
<td>8,000</td>
</tr>
<tr>
<td>December 26, 2004</td>
<td>Sumatra, Indian Ocean</td>
<td>&quot;1.7 million people were displaced by the earthquake and subsequent tsunamis in 14 countries in South Asia and East Africa. The tsunami caused more casualties than any other in recorded history and was recorded nearly worldwide on tide gauges in the Indian, Pacific and Atlantic Oceans.&quot;²⁹⁸</td>
<td>227,898 (including quake victims)</td>
</tr>
</tbody>
</table>


²⁹⁴ibid.

²⁹⁵ibid.

²⁹⁶ibid.

²⁹⁷ibid.

According to the *Journal of Reinsurance*,

Tsunami damage to land, structures and infrastructure depends not only upon the wave height at the coastline, but the way the wave travels inland, and the design and construction of the impacted structures. Tsunami damage does not result simply from inundation or the force of waves. Tsunamis transport debris fields that act as battering rams. Spontaneous dams form between obstructions and burst when water pressures build up behind them. The landscape they leave behind may be scoured of almost all evidence of human activity. Utilities like water, sewer, power, telephone, roads and bridges, ports and harbors are often destroyed, along with buildings. Damage is widespread, with long-term economic impacts on low-lying communities and coastal regions.²⁹⁹

Japan has a history of tsunamis following major earthquakes; its government has developed a tsunami early warning system similar to the U.S. Emergency Broadcast System, which broadcasts warnings over television and radio networks. “The Tsunami Warning System (TWS) in the Pacific, comprised of 26 participating international Member States, has the functions of monitoring seismological and tidal stations throughout the Pacific Basin to evaluate potentially tsunamigenic earthquakes and disseminating tsunami warning information. The Pacific Tsunami Warning Center (PTWC) is the operational center of the Pacific TWS. Located near Honolulu, Hawaii, PTWC provides tsunami warning information to national authorities in the Pacific Basin.”³⁰⁰

**Volcanoes**

According to CBC News Online,

A volcano is a geological formation, usually a conical mountain, that forms when molten rock, called magma, flows up from the interior of the Earth to the surface. Magma finds its way upwards along fissures or cracks in the planet’s crust and bursts out onto the surface, resulting in a volcano.

The Earth’s crust is composed of 15 plates that float on the molten layer beneath them. Most volcanoes line the boundaries of these plates. One of these boundaries is referred to as “the circle of fire” and extends from the west coast of the Americas to the east coast of Asia. Seventy-five per cent of the world’s active volcanoes are found along this “circle of fire.”

A volcano erupts in one of two ways: either the magma is forced up to the surface or the rising magma heats water trapped within the surface, causing an explosion of steam. In either case, the eruption can eject rocks, volcanic ash, cinders and hot gases into the air. The rapidly cooling lava can form volcanic glass.³⁰¹

See Table 3–6 for a listing of the world’s deadliest volcanoes.

“The best warning of a volcanic eruption is one that specifies when and where an eruption is most likely to occur and what type and size eruption should be expected.


Chapter 3 • Security and Fire Life Safety Threats  

Such accurate predictions are sometimes possible but still rare in volcanology. The most accurate warnings are those in which scientists indicate an eruption is probably only hours to days away based on significant changes in a volcano’s earthquake activity, ground deformation, and gas emissions. Experience from around the world has shown that most eruptions are preceded by such changes over a period of days to weeks.  

Heat Waves  

A heat wave is “a period of abnormally and uncomfortably hot and usually humid weather. To be a heat wave such a period should last at least one day, but conventionally it lasts from several days to several weeks.”

Deadly heat waves have struck areas such as Europe in 2003 and 2006; India in 1998, 2002, and 2003; Shanghai in 1998 and 2003; Chicago in 1995; Japan in 1994; and Athens in 1987. “In Australia during the 20th century, heatwaves caused

Table 3–6  World’s 10 Deadliest Volcanoes

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Death Toll</th>
<th>Major Cause of Death</th>
</tr>
</thead>
<tbody>
<tr>
<td>79 AD</td>
<td>Vesuvius, Italy</td>
<td>3,360</td>
<td>Ash flows and falls</td>
</tr>
<tr>
<td>1631</td>
<td>Vesuvius, Italy</td>
<td>3,500</td>
<td>Mudflows, lava flows</td>
</tr>
<tr>
<td>1783</td>
<td>Laki, Iceland</td>
<td>9,350</td>
<td>Starvation</td>
</tr>
<tr>
<td>1792</td>
<td>Unzen, Japan</td>
<td>14,300</td>
<td>Volcano collapse, tsunami</td>
</tr>
<tr>
<td>1815</td>
<td>Mount Tambora, Indonesia</td>
<td>92,000</td>
<td>Starvation</td>
</tr>
<tr>
<td>1882</td>
<td>Galunggung, Indonesia</td>
<td>4,011</td>
<td>Mudflows</td>
</tr>
<tr>
<td>1883</td>
<td>Krakatau, Indonesia</td>
<td>36,417</td>
<td>Tsunami</td>
</tr>
<tr>
<td>1902</td>
<td>Mount Pelee, Martinique</td>
<td>29,025</td>
<td>Ash flows</td>
</tr>
<tr>
<td>1919</td>
<td>Kelut, Indonesia</td>
<td>5,110</td>
<td>Mudflows</td>
</tr>
<tr>
<td>1985</td>
<td>Ruiz, Colombia</td>
<td>25,000</td>
<td>Mudflows</td>
</tr>
</tbody>
</table>


104Estimated deaths for 2003 were as high as 35,000, including 14,802 in France alone, as reported in the New Scientist article, “European heatwave caused 35,000 deaths,” October 10, 2003, information supplied by the Earth Policy Institute based in Washington, DC, using data available from eight western European countries, <www.newscientist.com/article/dn4259-european-heatwave-caused-35000-deaths.html>; May 28, 2008.
more deaths than any other natural hazard. In 1939 alone, a heatwave in southern Australia caused 438 deaths.”

If a building is not air conditioned, a heat wave can be a threat to the life safety of its occupants. In a widespread heat wave impacting a city or region, there will greater pressure on public utilities to meet increased demands for electrical power to operate cooling fans and air conditioners. As a result, electrical power outages may occur at buildings, and as a consequence HVAC systems will shut down.

**Storms (Noncyclone, Tornadoes, and Tropical Cyclones)**

A storm is “any disturbed state of the atmosphere, especially as affecting the earth’s surface, implying inclement and possibly destructive weather…. Storms range in scale from tornadoes and thunderstorms, through tropical cyclones, to widespread extratropical cyclones … rainstorms, windstorms, hailstorms, snowstorms, etc. Notable special cases are blizzards, ice storms, sandstorms, and duststorms.”

**Noncyclone**

Noncyclone storms may include torrential rains, windstorms, hailstorms, snowstorms, blizzards, ice storms, sandstorms, and dust storms.

**Tornadoes**

A tornado is defined by the *Glossary of Meteorology* as “a violently rotating column of air, in contact with the ground, either pendant from a cumuliform cloud or underneath a cumuliform cloud, and often (but not always) visible as a funnel cloud.”

“Tornadoes are generally spawned by thunderstorms, though they have been known to occur without the presence of lightning. The stronger tornadoes attain an awe-inspiring intensity, with wind speeds that exceed 200 mph [322 kilometers per hour] and in extreme cases may approach 300 mph [483 kilometers per hour]…. Tornadoes can come one at a time, or in clusters, and they can vary greatly in length, width, direction of travel, and speed. They can leave a path 50 yards [46 meters] wide or over a mile [1.61 kilometers] wide. They may touch down for only a matter of seconds, or remain in contact with the ground for over an hour.”

“Wind speeds are sometimes estimated on the basis of wind damage using the Fujita scale …. [This six-point scale] (also known as the F-scale) relates tornado intensity indirectly to structural and/or vegetative damage.”

---


“Tornadoes occur on all continents but are most common in the United States, where the average number of reported tornadoes is roughly 1000 per year, with the majority of them on the central plains and in the southeastern states (see Tornado Alley). They can occur throughout the year at any time of the day. In the central plains of the United States they are most frequent in spring during the late afternoon.”

In the United States, if a threat of tornadoes is reported, tornado watch or tornado warning advisories may be issued by the National Weather Service (NWS). A tornado watch means that tornadoes are possible; a tornado warning means that tornadoes actually have been sighted in the area.

**Tropical Cyclones (Cyclones, Hurricanes, and Typhoons)**

A tropical cyclone is “the general term for a cyclone that originates over the tropical oceans. This term encompasses tropical depressions, tropical storms, hurricanes, and typhoons.”

A cyclone is “an atmospheric cyclonic circulation, a closed circulation. A cyclone’s direction of rotation (counterclockwise in the Northern Hemisphere) is opposite to that of an anticyclone. While modern meteorology restricts the use of the term cyclone to the so-called cyclonic-scale circulations, it is popularly still applied to the more or less violent, small-scale circulations such as tornadoes, waterspouts, dust devils, etc. (which may in fact exhibit anticyclonic rotation), and even, very loosely, to any strong wind.”

“Hurricanes and typhoons are large and sometimes intensely violent storm systems. In meteorological terms, they are tropical cyclones that have maximum sustained wind speeds of at least 119 km/h (74 mph).”

---


**-Tornado Alley—A term often used by the media to denote a zone in the Great Plains region of the central United States, often a north–south oriented region centered on north Texas, Oklahoma, Kansas, and Nebraska, where tornadoes are most frequent. Since statistics are variable on all timescales, the term has little scientific value. (Glossary of Meteorology, 2nd ed. American Meteorological Society. 2000. [http://amsrglossary.allenpress.com/glossary/browse?s=t&p=34>; May 27, 2008.)

---

In recent history, one of the worst hurricanes, Hurricane Katrina, occurred in the United States. “On August 28th, 2005, Hurricane Katrina hit the southern coast of the United States with devastating effect. It was reported that more than 1,800 people lost there lives, and more than $81 billion in damages occurred” (Disasters and emergencies. U.S. Department of Health & Human Services. [www.hhs.gov/disasters/emergency/naturaldisasters/hurricanes/katrina/index.html; December 17, 2008]. Included among facilities severely damaged by the hurricane and the subsequent flooding were office, hotel, and residential and apartment buildings. For example, of four downtown New Orleans office towers managed by Hertz Investment Group, according to Building Operating Management,

The tower with the worst damage had more than 1,600 windows blown out, damaging tenant offices throughout the building, Faucheux [of Hertz] says. Water entered through the broken windows and cascaded into the building through openings in the roof where vents had been torn off and large sections of the roof itself were ripped loose.

Inside the building, ceilings caved in, light fixtures and HVAC supply vents fell, drywall collapsed and some door frames were twisted. Every elevator and escalator pit in the building flooded, as did the parking garage.
166

HIGH-RISE SECURITY AND FIRE LIFE SAFETY

winds of at least 120 km/h (75 mph). Atlantic and eastern Pacific storms are called hurricanes, from the West Indian huracan (“big wind”), whereas western Pacific storms are
called typhoons, from the Chinese taifun, “great wind.”317
In addition to high winds, heavy rains characterize tropical cyclones. Although the
winds can cause serious damage, including broken building windows, the majority of
damage is a result of flooding during and after the tropical cyclone.

Floods and Landslides
Torrential rain, melting snow, a tsunami, or a hurricane may produce too much water
for land, rivers, and flood control channels to handle and therefore results in serious
flooding that will impact an entire area, including high-rise buildings. Floods also can
occur as a result of a public water main pipe break or a reservoir failing.
Subterranean parking garages located beneath high-rise buildings can become
flooded with water. This can result in damage to vehicles and substantial damage to
elevator systems because of water cascading into elevator shafts. Building operations can
be paralyzed for days as a result of the cleanup of impacted areas and repair of damaged
equipment. Also, a severe landslide318 could result in the collapse of a building.

Contractible Diseases (Pandemic Influenza, Severe Acute Respiratory
Syndrome, and Tuberculosis)
A disease is “an abnormal condition of an organism that impairs bodily functions and
can be deadly.”319
An infectious disease—also called a contractible or a communicable disease—
is caused by pathogenic microbial agents.320 “Transmission of an infectious disease
may occur through one or more of diverse pathways including physical contact with
infected individuals. These infecting agents may also be transmitted through liquids,

(Lobash M. Hertz Group: coming to grips with storm’s devastation. Building Operating Management: Milwaukee,
WI; November 2005:42).
317
Anthes RA. Hurricane and Typhoon. Grolier Online. www2.scholastic.com/browse/article.
jsp?id5179; August 22, 2008.
318
A landslide is “the movement of rocks, debris or earth flowing down a slope.” Cruden (1991) as quoted
in Samah FA. Paper 10: Landslides in the Hillside development in the Hulu Kland, Klang Valley; 150. http://
eprints.utm.my/1627/1/LANDSLIDES_IN_THE_HILLSIDE_DEVELOPMENT___IN_THE_HULU_KLANG,_
KLANG_VALLEY.pdf; August 23, 2008.

Two examples of landslides impacting high-rise apartment buildings (see http://daveslandslideblog.
blogspot.com/2008/03/landslide-in-alesund-norway.html) are:
1) June 18, 1972, a 12-story apartment building, located below Po Shan Road, in the Hong Kong Island
Mid-Levels district, was destroyed by a hillside collapse and resultant landslide, following heavy
rains, causing 67 deaths (www.csb.gov.hk/hkgcsb/doclib/showcasing_ced_e.pdf as reported on
Edward CY Yiu’s (Assistant Professor Department. of Real Estate and Construction, The University
of Hong Kong) blog Building Disaster Series 1-the 618 Landslides. http://hk.myblog.yahoo.com/
jw!hOyexcmXEw5KH7tRLPM/article?mid950; August 23, 2008).
2) December 11, 1993, a 12-story apartment building, Highland Towers, Selangor, Malaysia, collapsed
due to a landslide after 10 days of continuous rainfall, resulting in 48 deaths (Wikipedia. July 15, 2008.
319
320

safetymessage.com


food, body fluids, contaminated objects, airborne inhalation, or through vector-borne • spread.”  

Some diseases such as influenza, severe acute respiratory syndrome (SARS), and tuberculosis are infectious and contractable. These diseases are an ever-increasing threat to the public as outbreaks result in public health emergencies.

Pandemic Influenza

“Influenza (the flu) is a contagious respiratory infection caused by influenza viruses. It can cause mild to severe illness, and at times can lead to death.”

“An influenza pandemic • is an epidemic of an influenza virus that spreads on a worldwide scale and infects a large proportion of the human population.”

“Influenza pandemics occur when a new strain of the influenza virus is transmitted to humans from another animal species. Species that are thought to be important in the emergence of new human strains are pigs, chickens and ducks. These novel strains are unaffected by any immunity people may have to older strains of human influenza and can therefore spread extremely rapidly and infect very large numbers of people.”

Three influenza viruses within the 20th century have produced major outbreaks:

1. The 1918 Spanish Flu which took more than 500,000 American lives and up to 50 million worldwide;
2. The 1957 Asian Flu, which killed around 70,000 in the United States up to 2 million internationally;
3. And the 1968–69 Hong Kong flu which killed 34,000 in the United States and 700,000 worldwide.

“Pandemics become possible when the population has had no opportunity to build up immunity and no vaccine is available. In the case of the so-called Bird Flu or Avian Flu—the H5N1 flu virus—there is no evidence at this point that the strain has mutated to be easily transmitted from human to human. Most of the people who have died from

• A vector-borne disease is “one in which the pathogenic microorganism is transmitted from an infected individual to another individual by an arthropod or other agent, sometimes with other animals serving as intermediary hosts” (Changes in the Incidence of Vector-borne Diseases Attributable to Climate Change. <www.ciesin.columbia.edu/TG/HH/veclev2.html>; November 2, 2008).
• According to the World Health Organization, “a pandemic can start when three conditions have been met: (1) a new disease emerges among the population; (2) the agent infects humans, causing serious illness, and (3) the agent spreads easily and sustainably among humans. A disease or condition is not a pandemic merely because it is widespread or kills many people; it must also be infectious. For example, cancer is responsible for many deaths but is not considered a pandemic because the disease is not infectious or contagious (although certain causes of some types of cancer might be)” (Summary of the personal remarks at the May 2008 symposium, “Dealing with Today’s Asymmetric Threat to U.S. and Global Security,” co-sponsored by CACI International [CACI] and the National Defense University [NDU], CACI International; 2008:31).

324 ibid.
H5N1 in Asia have had very close contact with birds carrying it. However, the CDC claims that H5N1 is a rapidly mutating virus, and if it were to begin passing from human to human, a pandemic could ensue.\footnote{The CDC is the U.S. Department of Health and Human Services’ Centers for Disease Control.}

Because of the extended period needed to develop a vaccine for an influenza pandemic the number of deaths can be extremely high.

**Severe Acute Respiratory Syndrome (SARS)**

“Severe Acute Respiratory Syndrome (SARS) is a respiratory disease in humans which is caused by the SARS corona virus (SARS-CoV).”\footnote{Lang RF. Pandemic flu issues and your response. Security Technology & Design. January 2007: 58.} In November 2002, SARS originated in southern China and then spread to Hong Kong. Visitors in a Hong Kong hotel were then infected and traveled to Canada, Singapore, Taiwan, and Vietnam. The disease then spread to those countries.\footnote{Thiel V, ed. Coronaviruses: Molecular and Cellular Biology. 1st ed. Caister Academic Press; 2007 as referenced in Wikipedia. Severe acute respiratory syndrome. October 4, 2008. <www.wikipedia.com>; October 2, 2008.} Between November 2002 and July 2003, there were 8,096 known cases and 774 deaths worldwide.\footnote{Oehler RL. Severe acute respiratory syndrome (SARS): SARS symptoms. EMedicineHealth. <www.emedicinehealth.com/severe_acute_respiratory_syr...> ; October 5, 2008.}

“Symptoms of SARS can be similar to those of other viral infections. The first symptoms begin 2–7 days after exposure and may include the following: fever (temperature of more than 100.4°F), headache, fatigue (tiredness), muscle aches and pain, malaise (a feeling of general discomfort), decreased appetite, and diarrhea. Respiratory symptoms develop 3 or more days after exposure. Respiratory symptoms include the following: dry cough, shortness of breath, runny nose and sore throat (uncommon). By day 7–10 of the illness, almost all patients with laboratory evidence of SARS infection had pneumonia that could be detected on x-ray films.”\footnote{Tuberculosis. Wikipedia. October 11, 2008. <http://en.wikipedia.org/wiki/Tuberculosis#cite_note-Robbins-0>; October 11, 2008.} Diagnosis can be through a combination of observation, blood tests, and chest X-rays.

**Tuberculosis**

Tuberculosis, or “consumption” as it was previously known, is an infectious disease that causes lump-like lesions to form in the lungs. Inside the lesions there are degenerating macrophages and tuberculosis bacteria, which when ruptured can infect the lung and the entire body.\footnote{Seeley RR, Stephens TD, Tate P. Essentials of Anatomy & Physiology. New York: McGraw Hill; 2007.} “Tuberculosis usually attacks the lungs (as pulmonary TB) but can also affect the central nervous system, the lymphatic system, the circulatory system, the genitourinary system, the gastrointestinal system, bones, joints, and even the skin…. The typical symptoms of tuberculosis are a chronic cough with blood-tinged sputum, fever, night sweats and weight loss…. Tuberculosis is spread through the air, when people who have the disease sneeze, cough, or spit.”\footnote{World Health Organization. Summary of probable SARS cases with onset of illness from November 1, 2002 to July 31, 2003. <www.who.int/csr/sars/country/table2004_04_21/en/print.html>; based on data as of December 31, 2003 (October 11, 2008).}

Some people infected with tuberculosis may not be aware of it because they do not feel any symptoms or experience any discomfort. This is called latent
TB disease. “Transmission [of TB] can only occur from people with active—not latent—TB.”\(^{333}\)

“Treatment for TB uses antibiotics to kill the bacteria.”\(^{334}\)

“A rising number of people in the developed world are contracting tuberculosis because their immune systems are compromised by immunosuppressive drugs, substance abuse, or AIDS.”\(^{335}\)

The problem with contractible diseases such as pandemic influenza, severe acute respiratory syndrome (SARS), and tuberculosis is that any building user, including visitors, could be infected, and before symptoms develop they could infect many other building occupants with the disease.

Power Failure

Failure of electrical power to a building has a serious impact on its operations, including computer memory loss and equipment damage, particularly if the failure occurs when the building is fully occupied. A power failure may be a brownout (a partial reduction in service) or a total blackout.

Power failure can be caused by man-made or natural events. Man-made causes may include vehicle drivers who collide with utility poles or power transformers, human error in operating equipment within the building or outside of it (such as at the utility company supplying the power), or malicious tampering. Natural events include storms, floods, and earthquakes.

Slip-and-Falls

Because of the large numbers of tenants and visitors using high-rise buildings, slip-and-falls (whether a trip only, a slip only, a fall only, a trip-and-fall, a slip-and-fall, or a slip-trip-and-fall) do occur. It is most important that these incidents are properly handled according to established procedures, particularly as these types of events frequently lead to claims for compensation from the building owner, and they sometimes lead to litigation.

Stalking and Workplace Violence

Stalking

Although the legal definition of stalking varies from country to country and from state to state, a general definition is

\[
\text{a pattern of repeated, unwanted attention, harassment, and contact. It is a course of conduct that can include the following:}
\]

Following or laying in wait for the victim

Repeated unwanted, intrusive, and frightening communications from the perpetrator by phone, mail, and/or e-mail


\(^{335}\)ibid.
“Stalking is a distinctive form of criminal activity composed of a series of actions that taken individually might constitute legal behavior. For example, sending flowers, writing love notes, and waiting for someone outside her place of work are actions that, on their own, are not criminal. When these actions are coupled with intent to instill fear or injury, however, they may constitute a pattern of behavior that is illegal. Though anti-stalking laws are gender neutral, most stalkers are men and most victims are women.”

A study of the incidence of stalking behaviors conducted among 3,700 men and women in the Australian State of Victoria revealed the following:

The majority of those reporting stalking were female (75%). Some 43% were aged between 16–30 when the behaviour commenced, though all age groups were vulnerable to pursuit.

Perpetrators of stalking behaviours were overwhelmingly male (84%). In 24% of cases stalking victims were pursued by a person of the same gender, with males significantly more likely to experience such harassment than females (76% versus 8%).

The majority of those reporting stalking were pursued by someone previously known to them (57%). In 42% the perpetrator was a stranger to the victim, or someone whose identity, though suspected, was yet to be revealed.

Since the instigation and passage of antistalking legislation in the US, stalking has generated in most English-speaking nations a growing discourse in legal, scientific and popular domains. This study confirms that such attention and concern is not misplaced. Stalking is a prevalent and damaging form of behaviour to which all members of society are susceptible.

---

338 This finding closely correlated that of two surveys reported in “Report to Congress on Stalking and Domestic Violence, 2005 Through 2006,” U.S. Department of Justice, Office on Violence Against Women, which stated “78% or four out of five stalking victims were women” (p. 1). <www.ncjrs.gov/pdffiles1/ owv/220827.pdf>; May 30, 2008.
339 ibid.
340 Purcell R, Pathe M, Mullen PE. Victorian Institute of Forensic Mental Health and Department of Psychological Medicine, Monash University, Victoria, “The Incidence and Nature of Stalking Victimization”
Workplace Violence

Workplace violence is “any physical assault, threatening behavior, or verbal abuse occurring in the work setting. A workplace may be any location either permanent or temporary where an employee performs any work-related duty. This includes, but is not limited to, the buildings, and surrounding perimeters, including the parking lots, field locations, clients’ homes and traveling to and from work assignments.” 341 It is “any incident in which a person is abused, threatened or assaulted in circumstances relating to their work. This can include verbal abuse or threats as well as physical attacks.” 342

Howard 343 developed categories for describing workplace violence by defining the relationship between the victim and the perpetrator. Table 3–7 interprets these findings.

The following statements indicate that workplace violence is affecting workers in many parts of the world:

United Kingdom—according to the Health and Safety Executive (HSE), 345 Estimates from the 2006/07 British Crime Survey (BCS) indicated that there were approximately 397,000 threats of violence and 288,000 physical

<table>
<thead>
<tr>
<th>Type of Workplace Violence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. External/Intrusive</td>
<td>The perpetrator has no legitimate relationship to the business or its employees and is usually committing another crime (for example, robbery) in conjunction with the violence.</td>
</tr>
<tr>
<td>II. Customer/Client</td>
<td>The perpetrator has a legitimate relationship with the business and becomes violent while being served by the business. Perpetrators include customers, clients, students, and patients and their targets include health care providers, teachers, and police.</td>
</tr>
<tr>
<td>III. Coworker</td>
<td>The perpetrator is an employee or former employee of the workplace who attacks a supervisor, owner, or another employee.</td>
</tr>
<tr>
<td>IV. Personal/Family</td>
<td>The perpetrator usually does not have a relationship with the workplace but does have a personal relationship with the victim. Perpetrators may be spouses, boyfriends or girlfriends, relatives, or acquaintances of the victim.</td>
</tr>
</tbody>
</table>

Source: Courtesy of ASIS International Foundation Research Council CRISP Report by Dana Loomis. 344

---

343 Howard J. State and regulatory approaches to preventing workplace violence (Occupational Medicine: State of the Art Reviews. 11: 293–301, as stated in Preventing Gun Violence in the Workplace by Dana Loomis [CRISP REPORT Connecting Research in Security to Practice, ASIS International Foundation Research Council CRISP Report, Alexandria, VA, 2008:6]).
344 ibid.
assaults by members of the public on British workers during the 12 months prior to the interviews.

The highest estimated rates of fatal, major and over 3-day injuries reported to HSE through RIDDOR [the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations] were found in the minor occupational groupings of prison service officers below principal officer (1187 per 100,000 workers), police officers (sergeant and below) (478 per 100,000 workers) and bus and coach drivers (301 per 100,000 workers).

**United States**—according to the ASIS International Foundation Research Council CRISP Report by Dana Loomis.\(^{346}\)

Researchers from the National Institute for Occupational Safety and Health (NIOSH) estimate that between 1992 and 2001, workplace homicide cost society more than $600 million per year, or about $800,000 per worker. Data from the Census of Fatal Occupational Injuries conducted by the U.S. Bureau of Labor Statistics,\(^ {347}\) indicate that, in recent years, an average of 500 to 600 American workers die annually as a result of violence on the job. And according to Richardson and Windau,\(^ {348}\) about three-quarters of workplace homicides result from injuries inflicted with guns.

The seriousness of homicide has made it the focus of the concern about workplace violence. The rate of workplace homicide has declined gradually since the 1980s and fell somewhat more rapidly than the rate for all homicides in the 1990s.\(^ {349}\) Nevertheless, homicide is the third leading cause of death on the job for all workers in the United States, and the leading cause of death for women.

**Argentina, Australia, Belgium, Canada, Finland, France, Germany, Hong Kong and China, Japan, Kuwait, Malaysia, Poland, Spain, South Africa, Sweden, and Ukraine**—according to a study for the International Labour Organization (ILO) which shows that\(^ {350}\)

---


\(^{350}\)Statements by authors citing a survey of the European Union’s 15 member states in 2000 of Violence at Work (3rd edition) by Vittorio Di Martino, an international expert on stress and workplace violence, and Duncan Chappell, past president of the New South Wales Mental Health Review, Australia, and the Commonwealth Arbitral Tribunal, UK. 29 August 2006. <www.hrmguide.net/international/violence.htm>; May 31, 2006.
Violence at work is increasing worldwide and has reached epidemic levels in some countries. Situations described range from bullying and mobbing (where a group of workers targets an individual), to threats, sexual harassment and homicide. Professions once regarded as largely immune are increasingly involved in both developed and developing countries.

In Germany, a 2002 study estimated that more than 800,000 workers were the victims of mobbing. In Spain, an estimated 22 per cent of officials in public administration were victims of this form of violence. In France, reported acts of aggression against transport workers rose from 3051 in 2001 to 3185 in 2002.

In Japan, 625,572 consultation requests were brought before court counsellors between April 2002 and March 2003 of which almost 32,000 (5.1 per cent) were related to harassment and bullying. This compares to data for April to September 2003 when 9.6 per cent of 51,444 requests concerned bullying and harassment.

In Malaysia, 11,851 rape and molestation cases in the workplace were reported between 1997 and May 2001. Widespread sexual harassment and abuse were major concerns in a number of countries including South Africa, Ukraine, Kuwait and Hong Kong and China.

Australia has estimated costs to employers to be between A$6 and 13 billion. Many countries have explicitly recognized violence in occupational health and safety legislation. Argentina, Belgium, Canada, Finland, France, Poland and Sweden are among countries that have recently adopted legislation or amended existing laws and regulations to address workplace violence.

Workplace Violence Profiles

The building occupancies discussed in this book—office, hotel, residential and apartment, and mixed-use buildings—could be the setting for someone to commit workplace violence. For office buildings, hotels, and residential buildings, the workplace violence may be as simple as the verbal abuse that security staffs, particularly security officers, doormen, and concierge/receptionists sometimes receive. Although it is difficult to make generalizations about the types of perpetrators of workplace violence, the following observations have been made about them:

**Frustrated employees, who in many instances are simply shuffled between jobs requiring only menial tasks with very little advancement opportunity open to them.**

**Professionals who are experiencing personal frustration and cannot handle emotional deflations such as workforce cutbacks or layoffs.**

**Individuals who are simply bitter, dissatisfied people and are unable to “shake” their negativity toward everything.**

**People unable to accept personal blame for their own problems.**

**Individuals with uncontrollable pent-up rage who operate on a “short fuse” when it comes to getting upset or mad over anything.**

**Persons who have little or no support systems such as family, friends, neighbors, and who are unable to vent their rage by either confiding in someone or having some other avenue of relief in which they can “blow off steam.”**
People who are prone to use firearms and have access to weaponry of any kind. Individuals suffering from depression and [those] who are potentially suicidal.\textsuperscript{351}

In dealing with employees, the ideal solution would be for employers to screen out, during the initial hiring process, those applicants who have an inclination for violence. This could include inquiring about an applicant's prior criminal convictions and conducting a thorough background check with previous employers. Despite some ethical questions and a degree of uncertainty about their predictive powers, psychological tests are also used to screen prospective employees—and still it is difficult to recognize potentially problematic employees.

The following are indicators of potential workplace violence:

- Intimidating, harassing, bullying, belligerent, or other inappropriate and aggressive behavior.
- Numerous conflicts with customers, co-workers, or supervisors.
- Bringing a weapon to the workplace (unless necessary for the job), making inappropriate references to guns, or making idle threats about using a weapon to harm someone.
- Statements showing fascination with incidents of workplace violence, statements indicating approval of the use of violence to resolve a problem, or statements indicating identification with perpetrators of workplace homicides.
- Statements indicating desperation (over family, financial, and other personal problems) to the point of contemplating suicide.
- Direct or veiled threats of harm.
- Substance abuse.
- Extreme changes in normal behaviors.\textsuperscript{352}

Sound personnel practices, such as preemployment screening and meaningful job performance evaluations, may help identify and screen out potential problem employees.

**Prevention Measures**

Employers may take the following preventive measures, some of which have been adapted from the *Cal/OSHA Guidelines for Workplace Security*, to address the workplace violence problem:

- **Control physical access through workplace design.** This can include controlling access into and out of the workplace and freedom of movement within it, in addition to placing barriers between service providers and clients. It may be appropriate, in certain situations, to use access cards or other locking devices, a receptionist who can unlatch a door, the installation of duress alarms as a back-up measure (in conjunction with a [CCTV] camera system to monitor the duress alarm locations), or security personnel.

- **Establish a clear anti-violence management policy and set boundaries as to what is considered acceptable behavior.** Policies should be applied consistently and fairly to all employees, including supervisors and managers.


Provide appropriate supervisory and employee training in workplace violence prevention.

Establish procedures for investigating occupational injury or illness arising from a workplace assault or a threat of assault. Implement procedures to handle threats of violence by employees, including a policy on when to notify law enforcement agencies. Establish procedures to allow employees to confidentially report threats, and to protect them from physical retaliation for these reports.

Provide training on how to recognize workplace security hazards, how to prevent workplace assaults, and what to do when an assault occurs, including emergency action and post emergency procedures. Give employees instruction in crime awareness, assault and rape prevention, and hostile situation diffusion. For example, if employees work late at night, encourage them to keep their doors locked, and either to leave the building with a fellow employee or to call security for an escort to their vehicle.

If a workplace assault occurs, reduce the short- and long-term physical and emotional effects of the incident by providing post event trauma counseling to those who desire such intervention.353

According to the ASIS International Foundation Research Council CRISP Report by Dana Loomis, “Enforcing a no-weapons policy for employees as allowed by law is a fundamental component of establishing effective countermeasures. Weapons policies should be written, made known to all employees, and consistently enforced.”354 This report also cautions that “Not enough rigorous research has been conducted to gauge the effectiveness of mandatory or voluntary measures for preventing workplace violence. To date, most research has focused on the use of crime prevention through environmental design (CPTED) concepts used to prevent robbery-related, or Type I [see Table 3–7], violence, in retail businesses.355,356”357

A number of preventive measures can be accomplished without great expense to the employer. For example, if workforce reductions are anticipated, they should be thoroughly planned with dignity and respect afforded to the affected employees. Workers who will be laid off need as much advance notice as possible. Giving severance benefits and offering placement counseling and assistance will help outgoing employees cope with their situation.

353 Cal/OSHA. Cal/OSHA Guidelines for Workplace Security (California Division of Occupational Safety and Health, Department of Industrial Relations, San Francisco, CA; August 15, 1994:7, 8).
and nurture a supportive work environment for the remaining employees. It has the added potential of lowering insurance premiums, because it may avoid triggering an incident of violence in the workplace and the expensive litigation that can result.

Traffic Accidents

Motor vehicles such as cars, buses, vans, and trucks commonly enter the parking areas of high-rise buildings. As on public thoroughfares, traffic accidents sometimes occur. Although the incident may have occurred on private property, depending on its seriousness, immediate medical aid or public law enforcement assistance may need to be summoned.

Water Leaks

A water leak in a high-rise building—particularly those on upper floors of a high-rise—can result in considerable damage to the structure and its contents. Water may drain down through multiple floors via stairwells, elevator shafts, and poke-throughs. This can lead to water in concealed ceiling spaces, soaked acoustical ceiling tiles that may fall from their own weight, water-soaked walls, and malfunction and possible failure of electrical systems if water comes in contact with them.

Leaks may be caused by a broken water pipe, a severed fire system sprinkler head, seepage through subterranean walls, overflow of a toilet receptacle, a backed-up sewer line, a blocked drain, failure of a sump pump, or a malfunctioning fountain. Someone deliberately leaving a water tap running in an area such as a public restroom may also cause a leak.

Summary

- There are many potential security and fire life safety threats to the people who use high-rise buildings and to the assets contained within them.
- Sometimes threats can become events that quickly develop into emergencies. These include aircraft collisions; bombs and bomb threats; daredevils, protestors, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstrations, and civil disorder; medical emergencies; natural disasters; contractible diseases; power failures; slip-and-falls; stalking and workplace violence; traffic accidents; and water leaks.

Key Terms

Aberrant behavior. Behavior that deviates from the norm, such as that caused by substance (drug or alcohol) abuse, may be a threat not only to the personal safety of the individual involved but also to other persons.

Arson. The malicious burning of another’s house. This definition, however, has been broadened by statutes and criminal codes to include starting a fire or causing an explosion with the purpose of (1) destroying a building or occupied structure of another or (2) destroying or damaging any property, whether one’s own or another’s, to collect insurance for such loss. Other statutes include the destruction of property by other means (e.g., an explosion).358

---

Assault. “Any willful attempt or threat to inflict injury upon the person of another, when coupled with an apparent present ability so to do, and any intentional display of force such as would give the victim reason to fear or expect immediate bodily harm, constitutes an assault. An assault may be committed without actually touching, or striking, or doing bodily harm, to the person of another.”

Assault and battery. “Any unlawful touching of another which is without justification or excuse.”

Asset. “Any real or personal property, tangible or intangible, that a company or individual owns, that can be given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary information, and related property.”

“A resource of value requiring protection. An asset can be tangible (e.g., people, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company’s information and reputation).”

Asymmetric threat. A threat that must satisfy three criteria: “First, it must involve a weapon, tactic, or strategy that a state or non-state enemy both could and would [use] against [a country].... Second, it must involve a weapon, tactic, or strategy that [the threatened country] would not employ.... Third, it must involve a weapon, tactic, or strategy that, if not countered, could have serious consequences.”

Bomb. See explosives and incendiary devices.

Burglary. Entering a vehicle or “building or occupied structure, or separately secured or occupied portion thereof, with purpose to commit a crime therein, unless the premises are at the time, open to the public or the [perpetrator] is licensed or privileged to enter.”

Chicane. ‘A sequence of tight serpentine curves (usually an S-shape curve ...) in a roadway, used in motor racing and on city streets to slow cars. On modern raceways, chicanes are usually located after long straightaways, making them a prime location for overtaking.”

Civil disorder. “Any public disturbance involving acts of violence by assemblages of three or more persons, which causes an immediate danger of or results in damage or injury to the property or person of any other individual.” Sometimes known as a civil disturbance.

Crime. “An act or omission which is in violation of a law forbidding or commanding it for which the possible penalties for an adult upon conviction include incarceration, for which a corporation can be penalized by a fine or forfeit, or for which a juvenile can be adjudged delinquent or transferred to criminal court for prosecution. The basic legal definition of crime is all punishable acts, whatever the nature of the penalty.”

---

359 ibid., p. 114.
360 ibid., p. 115.
363 Definition derived from “Thoughts on the meaning of ‘Asymmetric Threats,’” by Primmerman CA (Lincoln Laboratory, Massachusetts Institute of Technology: Lexington, MA; March 8, 2006:5). The original definition was U.S. centric and has been modified to be applicable to any threatened country.
Crime prevention through environmental design (CPTED—pronounced sep-ted). “The CPTED concept, coined by Dr. C. Ray Jeffery in his book by the same title, expands upon the assumption that the proper design and effective use of the built environment can lead to a reduction in the fear of crime and the incidence of crime, and to an improvement in the quality of life.”  

Cyberattack. “An assault against a computer system or network.”

Cyberterrorism. “The convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people to further political or social objectives. Moreover, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water and food contamination, or severe economic loss are examples. Serious attacks against critical infrastructures can be acts of cyberterrorism depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance are not.”

Cyclone. “An atmospheric cyclonic circulation, a closed circulation. A cyclone’s direction of rotation (counterclockwise in the Northern Hemisphere) is opposite to that of an anticyclone. While modern meteorology restricts the use of the term cyclone to the so-called cyclonic-scale circulations, it is popularly still applied to the more or less violent, small-scale circulations such as tornadoes, waterspouts, dust devils, etc. (which may in fact exhibit anticyclonic rotation), and even, very loosely, to any strong wind.”

Demonstration. A gathering of people for the purposes of publicly displaying their attitude toward a particular cause, issue, or other matter.

Dirty bomb. A radiological dispersal device (RDD) that uses conventional explosives to spread radioactive material.

Disaster. “A serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources.”

Disorderly conduct. “If, with purpose to cause public inconvenience, annoyance or alarm, or recklessly creating a risk thereof, he (a) engages in fighting or threatening, or in violent or tumultuous behavior; or (b) makes unreasonable noise or offensively coarse utterance, gesture or display, or addresses abusive language to any person

---

370 Denning DE. “Cyberterrorism,” testimony before the Special Oversight Panel on Terrorism; Committee on Armed Services; U.S. House of Representatives, Georgetown University; May 23, 2000, as quoted in “Dealing with Today’s Asymmetric Threat to U.S. and Global Security,” summary of the personal remarks at the May 2008 symposium co-sponsored by CACI International (CACI) and the National Defense University (NDU), CACI International; 2008:31.
372 Term radiological dispersal device (RDD) stated in “Cleanup after a radiological attack,” by Elizabeth Parker (The Nonproliferation Review: Fall-Winter 2004:167).
present; or (c) creates a hazardous or physically offensive condition.”

**Earthquake.** “A term used to describe both sudden slip on a fault, and the resulting ground shaking and radiated seismic energy caused by the slip, or by volcanic or magmatic activity, or other sudden stress changes in the earth.”

**Emergency.** “An event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response.”

**Espionage.** “The crime of ‘gathering, transmitting or losing’ information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the [country], or to the advantage of any foreign nation.” This could also be perpetrated by a business competitor engaging in industrial espionage.

**Explosives.** “Devices designed to explode or expand with force and noise through rapid chemical change or decomposition.” Also known as bombs.

**Fire alarm.** “A signal initiated by a fire alarm-initiating device such as a manual fire alarm box, automatic fire detector, airflow switch, or other device in which activation is indicative of the presence of a fire or fire signature.”

**Fire stop.** “Material or member that seals open construction to inhibit spread of fire.”

**Floor plan.** “Architectural drawings showing the floor layout of a building and including precise room sizes and their relationships. The arrangement of the rooms on a single floor of a building, including walls, windows, and doors.”

**Heat wave.** “A period of abnormally and uncomfortably hot and usually humid weather. To be a heat wave such a period should last at least one day, but conventionally it lasts from several days to several weeks.”

**Hoistway.** “The structural component in which the elevators move in a building.”

**Hostage.** “An innocent person held captive by one who threatens to kill or harm him if his demands are not met.”

---


Hurricane. “Hurricanes and typhoons are large and sometimes intensely violent storm systems. In meteorological terms, they are tropical cyclones that have maximum sustained winds of at least 120 km/h (75 mph). Atlantic and eastern Pacific storms are called hurricanes, from the West Indian huracan (‘big wind’), whereas western Pacific storms are called typhoons, from the Chinese taifun, ‘great wind.’”

Improvised explosive device (IED). “A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components.”

Incendiary devices. “Devices used or adapted for setting property on fire” and can be activated by mechanical, electrical, or chemical means. Also known as bombs.

Influenza pandemic. “An epidemic of an influenza virus that spreads on a worldwide scale and infects a large proportion of the human population.”

Kidnapping. “The forcible abduction or stealing and carrying away of a person.... A person is guilty of kidnapping if he unlawfully removes another from his place of residence or business ... or if he unlawfully confines another for a substantial period in a place of isolation.”

Larceny. “The unlawful taking and carrying away of property of another with intent to appropriate it to use inconsistent with the latter's rights.” Theft is a popular name for larceny. Larceny-theft includes offenses such as shoplifting, pocket-picking, auto theft, and other types of stealing where no violence occurs.

Lewd behavior. Relates to morally impure or wanton conduct; indecent exposure is included.

Manslaughter. “The unjustifiable, inexcusable, and intentional killing of a human being without deliberation, premeditation and malice.”

Mayhem. “A type of injury which permanently render[s] the victim less able to fight offensively or defensively; it might be accomplished either by the removal of (dismemberment), or by the disablement of, some bodily member useful in fighting. Today, by statute, permanent disfigurement has been added.”

Mobility impaired. “People with physical disabilities rely on a variety of artificial means for mobility. Such devices range from canes and walkers to motorized wheelchairs.”

---

390ibid., p. 881.
391ibid., p. 964.
392ibid., p. 979.
Murder. "The unlawful killing of a human being by another with malice aforethought, either express or implied." 394

Panic. "A sudden terror often inspired by a trifling cause or a misapprehension of danger and accompanied by unreasoning or frantic efforts to secure safety." 395

Partial or zoned evacuation. This strategy "provides for immediate, general evacuation of the areas of the building nearest the fire incident. A partial evacuation may be appropriate when the building fire protection features assure that occupants away from the evacuation zone will be protected from the effects of the fire for a reasonable time. However, evacuation of additional zones may be necessary." 396 Sometimes known as staged evacuation.

Performance-based codes. "Detail the goals and objectives to be met and establish criteria for determining if the objective has been reached.... Thus, the designer and builder gain added freedoms to select construction methods and materials that may be viewed as non-traditional as long as it can be shown that the performance criteria can be met." 397

Performance-based design. "Applies a procedure to predict and estimate damage or behavior anticipated of a structure's design to design events, compared against preselected objectives. The design is revised until the predictive methodology indicates that acceptable performance can be obtained." 398

Physical security. "That part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against espionage, sabotage, damage, theft and loss." 399

Poke-throughs. Holes cut through floors to allow the passage of conduits or ducts, primarily for the passage of electrical wiring, plumbing, heating, air-conditioning, communications wiring, or other utilities. Problems arise when the space between the conduit or the duct and the surrounding floor is not completely sealed with fire-resistant material, thereby negating the fire-resistance rating of the floor and potentially providing a passageway for deadly fire gases. 400

Prescriptive-based codes. "Spell out in detail what materials can be used, the building geometry (heights and areas), and how the various components should be assembled." 401 Also known as specification-based codes.

Prescriptive design approach. "Includes extensive detailed criteria for the design of systems that have been developed over many years of experience." 402

---


Progressive collapse. “The spread of local damage, from an initiating event, from element to element, eventually resulting in the collapse of an entire structure or a disproportionately large part of it.”\(^{403}\) Also known as disproportionate collapse.

Rape. “Unlawful sexual intercourse with a female without her consent.”\(^{404}\) Under some statutes, this crime may now include intercourse between two males.

Riot. “A form of civil disorder characterized by disorganized groups lashing out in a sudden and intense rash of violence, vandalism, or other crime. While individuals may attempt to lead or control a riot, riots are typically chaotic and exhibit herd behavior.... Riots typically involve vandalism and the destruction of private and public property.”\(^{405}\)

Robbery. “Felonious taking of money, personal property, or any other article of value, in the possession of another, from his [or her] person or immediate presence, and against his [or her will], accomplished by means of force or fear.”\(^{406}\)

Sabotage. In commerce, sabotage includes the “will[ful] and malicious destruction of employer’s property during a labor dispute or interference with his normal operations.”\(^{407}\) This act could also be perpetrated by a disgruntled employee or ex-employee seeking revenge or by a business competitor.

Severe Acute Respiratory Syndrome (SARS). “A respiratory disease in human which is caused by the SARS corona virus (SARS-CoV).”\(^{408}\)

Sexual harassment. “A type of employment discrimination, includes sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature prohibited by ... law.”\(^{409}\)

Staged evacuation. See partial or zoned evacuation.

Stalking. “A pattern of repeated, unwanted attention, harassment, and contact.”\(^{410}\)

Steel moment frames. “Consist of beams and columns joined by a combination of welding and bolting.”\(^{411}\)

Suicide. The taking of one’s own life.

Terrorism. “Terrorism is considered an unlawful act of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”\(^{412}\)

Terroristic threat. A person is guilty of a terroristic threat “if he [or she] threatens to commit any crime of violence with purpose to terrorize another or to cause evacuation...”\(^{413}\)
of a building, place of assembly, or facility of public transportation, or otherwise to cause serious public inconvenience, or in reckless disregard of the risk of causing such terror or inconvenience.”

**Theft.** “A popular name for larceny. The act of stealing. The taking of property without the owner’s consent…. It is also said that theft is a wider term than larceny and that it includes swindling and embezzlement and that generally, one who obtains possession of property by lawful means and thereafter appropriates the property to the taker’s own use is guilty of a ‘theft.’” Larceny-theft includes offenses such as shoplifting, pickpocketing, auto theft, and other types of stealing where no violence occurs. See also larceny.

**Threat.** “Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.”

**Tornado.** “A violently rotating column of air, in contact with the ground, either pendant from a cumuliform cloud or underneath a cumuliform cloud, and often (but not always) visible as a funnel cloud.”

**Trespass.** “Any unauthorized intrusion or invasion of private premises or land of another…. Criminal trespass is entering or remaining upon or in any land, structure, vehicle, aircraft or watercraft by one who knows he [or she] is not authorized or privileged to do so.” This includes remaining on property after permission to do so has been revoked.

**Tropical cyclone.** “General term for a cyclone that originates over the tropical oceans. This term encompasses tropical depressions, tropical storms, hurricanes, and typhoons.” See also cyclone.

**Tsunami.** “A large wave caused by earthquakes, submarine landslides, and, infrequently, by eruptions of island volcanoes. During a major earthquake, an enormous amount of water can be set in motion as the seafloor moves up and down. The result is a series of potentially destructive waves that can move at more than 500 miles [805 kilometers] per hour.”

**Tuberculosis.** A contagious disease that “usually attacks the lungs (as pulmonary TB) but can also affect the central nervous system, the lymphatic system, the circulatory system, the genitourinary system, the gastrointestinal system, bones, joints, and even the skin.”

**Typhoon.** “Hurricanes and typhoons are large and sometimes intensely violent storm systems. In meteorological terms, they are tropical cyclones that have maximum sustained

---


414 ibid., p. 1477.


winds of at least 120 km/h (75 mph). Atlantic and eastern Pacific storms are called hurricanes, from the West Indian *huracan* (‘big wind’), whereas western Pacific storms are called typhoons, from the Chinese *taifun*, ‘great wind’.”

**Vandalism.** “Such willful or malicious acts intended to damage or destroy property,” including the use of graffiti.

**Vehicle-borne IED (VBIED).** “A military term for a car bomb or truck bomb. These are typically employed by suicide bombers, and can carry a relatively large payload. They can also be detonated from a remote location. VBIEDs can create additional shrapnel through the destruction of the vehicle itself, as well as using vehicle fuel as an incendiary weapon.”

**Volcano.** “A geological formation, usually a conical mountain, that forms when molten rock, called magma, flows up from the interior of the Earth to the surface. Magma finds its way upwards along fissures or cracks in the planet’s crust and bursts out onto the surface, resulting in a volcano.”

**Workplace violence.** “Any physical assault, threatening behavior, or verbal abuse occurring in the work setting. A workplace may be any location either permanent or temporary where an employee performs any work-related duty. This includes, but is not limited to, the buildings, and surrounding perimeters, including the parking lots, field locations, clients’ homes and traveling to and from work assignments.”

**Zoned evacuation.** See partial or zoned evacuation.

**Additional Reading**


---


“Security and life safety needs are determined by identifying specific assets, the threats against those assets, and the risk of those threats materializing. Also of vital importance, if selected solutions [i.e., countermeasures or mitigation measures that address vulnerabilities] are going to be effective, is an understanding of the possible constraints (for example, culture, operations, economic factors, and codes and standards, etc.).”

An important tool for determining the security and fire life safety needs of a building is a risk assessment.

What Is a Risk Assessment?

Before discussing several methodologies for conducting risk assessments, it is important to define the term itself. Several definitions are as follows:

1. **Risk assessment** is “the process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an

---

An asset is “any real or personal property, tangible or intangible, that a company or individual owns, that can be given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary information, and related property” (ASIS Online Glossary of Terms. <http://www.asisonline.org/library/glossary/index.xml>; 2008). “A resource of value requiring protection. An asset can be tangible (e.g., people, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company’s information and reputation)” (FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; December 2003:B-3).


A countermeasure or a mitigation measure is an opposing measure to counteract the vulnerability of an asset to a threat.


organization’s operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls."\(^2\)

2. “Risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple, low cost mitigation measures, but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with identified vulnerability, allow prioritization of resources to implement mitigation measures.”\(^3\)

Risk management is the process of making decisions of where to minimize risks to assets and how to achieve this over a period of time.\(^4\)

One type of risk assessment is a security survey (sometimes called a security assessment).\(^5\) A security survey is defined as follows:

1. “Essentially an exhaustive physical examination of the premises and a thorough inspection of all operational systems and procedures. Such an examination or survey has as its overall objective the analysis of a facility to determine the existing state of its security, to locate weaknesses in its defenses, to determine the degree of protection required, and ultimately to lead to recommendations for establishing a total security program.”\(^6\)

2. “A critical on-site examination and analysis of an industrial plant, business, home, or public or private institution to ascertain the present security status, to identify deficiencies or excesses, to determine the protection needed, and to make recommendations to improve the overall security.”\(^7\)

3. “A thorough physical examination of a facility and its systems and procedures, conducted to assess the current level of security, locate deficiencies, and gauge the degree of protection needed.”\(^8\)

A security survey may focus on different aspects of a high-rise facility. It may include the area and businesses in the surrounding neighborhood, the building itself, a particular tenant or resident in the building, or defined aspects of the security operation.

---


such as policies and procedures, systems and equipment. A survey may also be used to investigate a particular incident or a security problem that has occurred or is occurring at the facility. If the focus of a survey is fire prevention, then a fire prevention survey can be conducted; if the focus is to reduce potential terrorist attacks against a building, then such a risk assessment can be conducted.

Risk Assessment Methodologies

Different risk assessment methodologies and risk management guides are available throughout the world. Some examples are as follows:

- **ASIS General Security Risk Assessment Guideline** by ASIS International
- **RAMCAP (Risk Analysis and Management for Critical Asset Protection) Methodology** sponsored by the U.S. Department of Homeland Security (DHS)
- **Sandia National Laboratories Risk Assessment Methodology (RAM)** as outlined in *The Design and Evaluation of Physical Protection Systems and Vulnerability Assessment of Physical Protection Systems* by Mary Lynn Garcia
- **The UK Government’s Risk Analysis and Management Method (CRAMM)** by the UK Security Service on behalf of the UK government
- **The U.S. Department of Defense (DoD) CARVER Methodology for Target Analysis and Vulnerability Assessment** (Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability)

In addition, various commercial risk assessment programs are available.

Whatever form the risk assessment takes, there is no real shortcut in effectively conducting it. Thomas Edison made the statement that “genius is 1 percent inspiration and 99 percent perspiration.” It may not take a genius to conduct a risk assessment—although technical expertise and experience are important aspects of the process—but there is no doubt that to thoroughly analyze the security or fire life safety of a facility, a considerable amount of work is required. To make the work as orderly as possible, it is helpful to use some form of a standardized methodology. This makes it more likely that vital areas are adequately covered and a uniform standard maintained for assessments repeated; it will also assist the surveyor in efficiently performing the task.

---

*In addition, an opinion survey may be conducted among security staff to measure their morale or elicit their ideas regarding the effectiveness of the overall security program and certain policies, procedures, systems, and equipment; such an opinion survey may also be conducted among building staff (management, janitorial, parking, and engineering) and building tenants and residents. An opinion survey of tenants is an important tool that enables building management to evaluate tenants’ perception of the security program, to identify areas that need to be changed or improved, or to evaluate the anticipated reaction of tenants if changes are made to the security program.


9Israel P. Life Lessons from Thomas Alva Edison. Interview of the associate editor of the Thomas A. Edison Papers at Rutgers University by Bottom Line (Boulder, CO; April 15, 1994:13). (Volumes I and II of the Edison papers are available from the Johns Hopkins University Press, Baltimore, MD.)
Systematic Ways to View a Building

Before addressing several risk assessment methodologies, it is helpful to consider three systematic ways for viewing a facility: interior spaces, rings, and layers of defense.

Interior Spaces

*The Protection of Assets Manual* states that within the high-rise structure there are three classes or types of interior spaces:

- Public access or common areas. These include street-level entrance lobbies, main elevator lobbies, access routes to retail sales spaces [and restaurants, etc.] in the structure, promenades, mezzanines, and—increasingly in new buildings—atria.
- Rented or assigned occupancies [i.e., tenant areas]. These are leased or owner-occupied spaces on the various floors. Depending on the occupant, such spaces may be open to public access during building hours, or may be restricted to identified and authorized persons.
- Maintenance spaces. These include mechanical rooms and floors, communications and utilities access points, elevator machine rooms, janitorial closets and other spaces with strict limited access.

Rings

“The classical approach to perimeter security views a property in terms of rings. The property boundary is the first ring. The building is the second, and the specific interior spaces are the third.”

“...This scheme needs only a slight variation to fit the high-rise building: The building line is usually the first ring since, in an urban environment, the building line is adjacent to a public sidewalk, access to vertical transportation (stairs, escalators, and elevators [lifts]) is the second and individual floors or floor sections are the third.”

Layers of Defense

Another approach to viewing a building, not dissimilar to the rings approach, is done within the concept of layers of defense (also known as protection-in-depth or security-in-depth) for protecting buildings against potential terrorist attacks. “The objective of layers of defense is to create a succeeding number of security layers more difficult to penetrate, provide additional warning and response time, and allow building occupants

---

•••Security-in-depth is “the proposition that multiple layers of security are better than a single protection mechanism. The layers may be technological, procedural, policy or other elements working in coordination to provide redundant and mutually supportive security measures” (SRMBOK Security Risk Management Body of Knowledge. Carlton South, Vic., Australia: Risk Management Institution of Australasia Limited; 2008:182).
Chapter 4 • Risk Assessments 189

to move into defensive positions or designated safe haven protection.”

The following material further explains this concept, with particular emphasis on the mitigation of potential terrorist attacks against buildings.

“Layers of defense” is a traditional approach in security engineering and use concentric circles extending out from an area or site to the building or asset that requires protection. They can be seen as demarcation points for different security strategies. Figure 4–1 shows the layers of defense described next.

First layer of defense. This involves understanding the characteristics of the surrounding area, including construction type, occupancies, and the nature and intensity of adjacent activities. It is specifically concerned with buildings, installations, and infrastructure outside the site perimeter. For urban areas, it also includes the curb lane and surrounding streets.

Second layer of defense. This refers to the space that exists between the site perimeter and the assets requiring protection. It involves the placement of buildings and forms in a particular site and understanding which natural or physical resources can provide protection. It entails the design of access points, parking, roadways, pedestrian walkways, natural barriers, security lighting, and signage. For urban areas, it refers specifically to the building yard.

Third layer of defense. This deals with the protection of the asset itself. It proposes to harden the structures and systems, incorporate effective heating, ventilation, and air-conditioning (HVAC) systems and surveillance equipment, and wisely design and locate utilities and mechanical systems. Note that, of all blast mitigation measures, distance is the most effective measure because other measures vary in effectiveness and can be more costly. However, often it is not possible to provide adequate stand-off distance. For example, sidewalks in many urban areas may be less than 10 meters (33 feet), while appropriate stand-off may require a minimum of 25 meters (82 feet). Designers should consider providing adequate stand-off distance when possible. In this case, the hardening* of the building is a second choice.

The layers of defense are not predetermined, and they may vary from site to site and from building to building. If a particular building requiring protection is part of a campus** or located in a rural, semirural, or urban area, a similar

---


14All of the following material on “layers of defense,” including Figure 4–1 and 4–2, is extracted from the FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; January 2005:2–1, 2–2.

*Building hardening is a term used to describe the “enhanced construction [hardening of physical structures beyond required building codes and standards] that reduces vulnerability to external blast and ballistic attacks” (FEMA 426: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; December 2003:2–1, B-5). “The hardening of the building envelope should be balanced so that the columns, walls, and windows have approximately equal response for damage and injury/casualty for the design basis threat weapon at the available stand-off distance” (FEMA 426: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; December 2003:3–1).

**A campus is “a site on which the buildings of an organization or institution are located” (msn Encarta® World English Dictionary. 2007. “campus.” <http://encarta.msn.com/dictionary_/campus.html>; August 21, 2008.
analysis may be applicable for all cases when determining the importance of the asset. However, the security elements necessary to protect the building can be entirely different, depending on its location. The approach suggests establishing different demarcation points to identify sound security strategies. The layers of defense concept proposes that each designer study a particular site and determine critical assets that need to be protected and how protection should take place.

Figure 4-2 depicts the security elements that may be considered in an urban setting. It shows how the second layer of defense becomes extremely important to protect a building in an urban area. Note that the elements described next may require a different method of protection for a campus or a rural site. Major layers for an urban setting include the following:

Curb lane (first layer of defense). This area refers to the lane of the street closest to the sidewalk. Typically it is used for curbside parking, passenger drop-off, loading, and service vehicles. Curbside parking should not be removed unless additional stand-off distance is absolutely required for high-target buildings. When required, sidewalks can be widened to incorporate the area devoted to the curb lane.

Sidewalk (first layer of defense). This area serves as the common space for pedestrian interaction, movement, and activity. If possible, sidewalks should be left open and accessible to pedestrians and security elements should not interfere with the circulation. The streetscape could include hardened versions of parking meters, streetlights, benches, planters, and trash receptacles. The use of retractable bollards is a great solution when the width of the street does not allow the placement of security elements.

Building yard (second layer of defense). This area refers to the exterior space between the building and the sidewalk. [For many existing high-rise buildings this building yard does not exist and the sidewalk is directly adjacent to the building.] It consists of a grassy area adjacent to the building flush with the sidewalk or a planted bed raised above the level of the sidewalk. It also includes pedestrian entries and loading docks. For the building yard, security components should complement the building architecture and landscaping. Security elements should be located near the outer edge of the yard. A planter or raised plinth\* wall provides a good security barrier in this layer.

Three risk assessment methodologies are now discussed: (1) an office building physical security survey, (2) a building fire prevention survey, and (3) a risk assessment to mitigate potential terrorist attacks against buildings.

**Office Building Physical Security Survey**

A physical security survey of an office building can be as extensive or as restricted as the surveyor determines. A formal documented survey basically will involve two major tasks: the fact-finding investigative process and writing the report that reflects the findings.

Fact-Finding Process

The fact-finding process may include the following:

1. Discuss with those commissioning the survey the scope of the survey, identify the individual(s) with authority to implement the survey recommendations, designate the time period in which the survey will be conducted, and determine to whom the final survey report will be presented. To help protect disclosure of the survey findings, the report may be commissioned by the legal firm representing the building owner or manager. By so doing, the survey becomes “privileged and confidential” information.

2. Review of codes and standards, and local zoning ordinances pertaining to required security measures.

3. “Obtain incident reports of all incidents that have occurred on the property for the past (minimum) three years or (preferred) five years.” Also, depending on the scope of the survey, it may be useful to conduct a crime pattern analysis examining “criminal activity in an effort to find patterns in the physical environment that makes it easy for a crime to occur. This tool has been used by police for a number of years ... its implications can be important in conducting a security evaluation of a specific location. The old-style, two-dimensional mapping process—using floor plans, stacking plans* and colour-coded labels [to indicate crimes and attempted crimes]—can be very helpful to facility and security managers who choose to conduct their own analyses.” In addition, other reports such as work orders, inspection logs, emergency services telephone call records, and security-related complaints might be reviewed.

4. Interview the crime analysis officer or community relations officer of the local police or sheriff’s department, to request crime statistics for the site and the neighboring area. (Although not all police agencies are willing to release such data, if possible, statistics should be obtained for the previous three to five years.)

5. Interview representatives of nearby businesses or observe the immediate neighborhood and areas surrounding the building to determine what security measures other buildings, particularly like ones, have implemented. Benchmarking is a process by which the security program at a facility can be compared with the best practices that exist for similar types of facilities. “Benchmarking ... serves as a barometer for determining what works best under comparable circumstances.”

---

* A stacking plan is “basically a side view of the [facility] showing the entire building, including all floors and a list of tenants inhabiting these floors” (Kitteringham G, CPP. Pinpointing problems: using two-dimensional mapping to determine security risks at a multi-use highrise complex. *Canadian Security*. December 2001:19).

** In North America and the United Kingdom, a source of information to complement police data is a crime prediction model that assesses Crimes Against Persons and Property (CAP Index). “By combining surrounding social characteristics, survey information and other databases with known indicators of crime, the CRIMECAST™ model is able to provide precise scores indicating a site’s risk of crime in comparison to national, state, and county averages. ... CRIMECAST™ data include current, past and projected scores for Crimes Against Persons (rape, robbery, homicide, aggravated assault) and Crimes Against Property (burglary, larceny, motor vehicle theft)” (*Information Brochure*. Exton, PA: CAP Index, Inc. <http://www.capindex.com>; 2008).

---


15In North America and the United Kingdom, a source of information to complement police data is a crime prediction model that assesses Crimes Against Persons and Property (CAP Index). “By combining surrounding social characteristics, survey information and other databases with known indicators of crime, the CRIMECAST™ model is able to provide precise scores indicating a site’s risk of crime in comparison to national, state, and county averages. ... CRIMECAST™ data include current, past and projected scores for Crimes Against Persons (rape, robbery, homicide, aggravated assault) and Crimes Against Property (burglary, larceny, motor vehicle theft)” (*Information Brochure*. Exton, PA: CAP Index, Inc. <http://www.capindex.com>; 2008).

6. Review any previous surveys conducted at the building. (Such documents, if available, may provide background information and details of the follow-up on previously noted deficiencies.)

7. Review available documentation such as a description of the building and its construction features (sometimes this can be found in marketing material for the site or from documents such as as-built drawings*), population information, stacking plans, site and floor plans (including layout of utility and communication systems), the security master plan,** security system drawings, the building emergency management plan, fire life safety systems information, plans for changes at the site, annual reports, records, tenant leases, security services agreements, data, files, organizational charts, job descriptions, manuals, policies, and operating procedures (including security instructions, standard operating procedures, or post orders) that are relevant to the survey.

8. Conduct a profile of tenant businesses within the building to ascertain which ones may constitute a high risk from a security perspective and may attract unbalanced individuals, criminals, terrorists, or activist groups. Such tenants may include day-care centers for young children; counseling offices; jewelers and retail banks; government agencies; foreign embassies and consulates, or foreign businesses; and furriers (or other businesses which may be a target for domestic activist groups). This profile may include the building itself. For example, if it is the tallest building in a city, a historic landmark or an embodiment of the economic strength of the nation, is the building considered a potential target for an act of international terrorism? (Likewise, buildings located in close proximity to such facilities may be at risk of suffering collateral damage.)

9. Interview persons who have knowledge of the building. These individuals may include architects, structural engineers, fire protection engineers, building management, building engineers, janitors, housekeepers, security and parking staff, couriers, elevator technicians, and the vendors of the security equipment currently in place or planned for installation.

10. Visit the site at different times during the day and night, business and nonbusiness hours, to become familiar with the

- Principal activities and usage
- Physical layout including the ingress and egress points, construction, and landscaping
- Occupant and visitor traffic flow patterns and how access is controlled
- Lighting and locking systems
- Electronic security systems
- Security operations

*As-built drawings (sometimes called record drawings) are “construction drawings revised to show significant changes made during the construction process; usually based on marked-up prints, drawings and other data furnished by the contractor or the architect” (Construction Dictionary. 9th ed. [Greater Phoenix, Arizona, Chapter 98. Phoenix, AZ: The National Association of Women in Construction; 1996:428]).

**A security master plan is the strategic plan for the protection of a facility’s assets (people, property, and information). “The ultimate goal of good strategic planning is to lay out specific long-range plan objectives and then devise short-term action plans to meet each major objective (or goal)” (Sennewald CA. Effective Security Management. 3rd ed. Woburn, MA: Butterworth-Heinemann; 1998:50). This plan may or may not be formally documented. Sometimes it is called the security plan or the security operations plan.
These visits may include testing various aspects of the security program. To check the operation of systems, particularly to determine whether policies and procedures are being implemented as intended, such testing—commonly known as penetration testing—might be done clandestinely.

11. In addition, insurance policies for the site may need review to determine whether the coverage adequately covers present risks. Of course, only a qualified risk manager or insurance adviser should conduct an in-depth review of insurance policies.

Survey Checklist

To assist in the fact-finding process, it is helpful to use a checklist of areas to be covered. Appendix 4–1 (on the CD-ROM accompanying this book) provides a sample checklist for a physical security survey of an office building. The main sections in this checklist are general information; site perimeter; building and building perimeter; maintenance spaces; loading dock/shipping and receiving areas; vehicular movement and parking areas; tenant offices; office computers; cafeteria, kitchen, and dining areas; intrusion detection and duress alarms, video surveillance systems, access control systems, metal detectors, and X-ray machines; key controls, locking devices, and containers; janitorial operation; security operation; security education; and insurance.

Every building, however, is different, and therefore no generic checklist can possibly cover all aspects of the facility being surveyed. In carrying out the fact-finding process, one may select as much, or as little, of the suggested checklist as one needs. The scope or extent of the survey being conducted will determine what is selected. As Gleckman summarized,

A checklist should be made up by the survey team (for extensive surveys there may need to be more than one surveyor) in preparation for the actual

---

*Penetration testing* is a process to evaluate the security status of a facility, or an aspect of its operation, by a person attempting to breach the program by exploiting any vulnerabilities or weaknesses that may exist.

+ In the United States, for high-profile, signature buildings, insurance is particularly important in view of the September 11, 2001, terrorist acts that destroyed the Twin Towers of the New York World Trade Center. “Prior to the events of September 11, 2001, property and casualty, and general liability insurance policies typically covered damages resulting from acts of terrorism, although most excluded damages relating to acts of war... By now, most states have permitted insurers to exclude terror insurance from their general property and casualty coverage” (Terrorism insurance. Chicago, IL: Institute of Real Estate Management; 2002:3). Commercial property owners requiring terrorism insurance have to purchase it from insurance underwriters. “Those policies have high deductibles, low limits and very high premiums. Property owners who succeed in obtaining terrorism coverage often do so by covering a large portfolio, thereby spreading the risk” (Gottlieb M. High profile. *California Real Estate Journal.* April 8, 2002:10).

* A structure is considered a signature building based on its size and height, its status, or the nature of its tenants. Doug Karpiloff, when manager of life safety and security for the New York World Trade Center, defined a significant or signature structure by posing the questions, “Is it the tallest building in the city, is it a symbol of the city itself, or does it house an organization whose activities are inimical to a large group of people?” (Gips MA. Building in terrorism’s shadow, a May 2000 *Security Management* magazine article republished in *Counterterrorism and Contingency Planning Guide* (a special publication from Security Management and ASIS International. Alexandria, VA: post–September 11, 2001:11).

** Before September 11, the risk of terrorist attacks [in the United States] was borne by the insurance industry. Covered by ‘all risk’ policies generally required by lenders, commercial business owners insured for this risk as part of ordinary business practice. From the insurer’s viewpoint, the cost of providing this coverage was not significant. After all, there had only been two significant acts of terrorism in the United States. One, the Oklahoma City bombing, involved a federal building that was self-insured by the government. So the only domestic act of terrorism that had resulted in an insurance payout was the 1993 bombing of the World Trade Center. The landscape has changed drastically since September 11. The insurance industry has withdrawn terrorism insurance from ‘all risk’ policies” (Creamer DE. Are the terrorists winning? *California Real Estate Journal.* May 6, 2002:1–2).
inspection. This checklist will be used to facilitate the gathering of pertinent information. The checklist is considered to be the backbone of the security survey or audit. This checklist will serve to systematically guide the survey team through the areas that must be examined.\(^{18}\)

The fact-finding process should include taking notes on paper, inputting information to a hand-held computer, or using a small voice recorder; also, it may be helpful to photograph various aspects of the site, particularly problem areas. (Digital cameras are extremely useful because quality images can be easily obtained, digitally stored, and imported into a written report.) Before taking photographs, permission should be obtained from the appropriate building representative. The fact-finding process, including planning the survey, will probably take 30 percent to 40 percent of the total time spent conducting the survey, whereas the other 60 percent to 70 percent will be spent writing the report.

**Writing the Report**

Writing the report will involve assembling the ideas and information obtained in the fact-finding investigative process. Weaknesses in the security program should indeed be pointed out and accompanied by recommendations to address them, but security strengths also should be documented. If a word processor is used to create the report, changes, modifications, and additions can be carried out in a relatively effortless manner. A standardized approach like the following will help to properly organize this information into a logical and understandable format. Again, every building is different, as is the scope of each survey, and individual surveyors will have their own specialized approaches. Hence, the suggested format is just that—a *suggested* one.

**Title Pages**

A typical title page indicates the confidentiality of the report, the name of the organization for whom the report is produced, the name of the site surveyed, the name of the person by whom the survey and report is compiled, the date, and a notation of the copy number. The next page should list the number of copies of the report and to whom each copy is distributed.

**Cover Letter**

The cover letter should be addressed to the individual who commissioned the report. It includes a brief statement of the scope of the survey, brief thanks to individuals who assisted with the report, a mention of anything pertinent to this particular report, and where to direct any inquiries regarding the report’s content.

**Table of Contents**

The table of contents is a listing by page number of all pertinent sections of the report.

**Introduction**

The introduction briefly states who commissioned the survey, why it was performed, and its scope. An example is as follows:

Mrs. Shirley Thomas, Asset Manager, Pauley and Partners, requested this survey and report. The primary objective for conducting the survey is to review strengths and weaknesses in the security program at the Pacific Tower Plaza high-rise complex, with reference, in particular, to after-hours access control procedures of building occupants and the control of business and personal property leaving the site after normal business hours.

Method of Compilation
The method of compilation includes a description of how information was obtained for the survey, the names of individuals interviewed, a list of documents reviewed, and the time period in which the survey was conducted. For example:

The survey was conducted on October 4–14, 2008, using information obtained from interviews with management personnel of Pauley and Partners; managers of the engineering, security, janitorial, and parking departments; individual security staff members; and a representative of Columbus Insurance Company. In addition, information was obtained by reviewing the Building Emergency Procedures Manual, a security survey previously conducted at Pacific Tower Plaza, current security instructions, security incidents reported since January 1, 2008, police crime statistics for the general area surrounding the site, a Tenant Information Manual (issued by building management to explain building policies and procedures), and crime coverage insurance policies in effect at the site.

Identification of Assets
The tangible and intangible assets of the site should be identified with an estimation of their value and financial impact if they were to be lost, made inaccessible, or destroyed.

Tangible assets include the people using the facility and the building itself, its fittings, and its equipment. The building equipment consists of the electrical, gas, mechanical, heating, ventilating, air conditioning, lighting, elevator, escalator, communication, security, and life safety systems. Other assets include telephones, computers, printers, typewriters, fax machines, photocopiers, audio-visual equipment, and general-use items—coffee machines, vending machines, refrigerators, microwaves, ovens, and furniture—and sometimes antiques and works of art, cash, and negotiable instruments. Also, there may be cafeterias, restaurants, retail shops, newsstands, copy/print services, and other common area facilities for office workers. Also, vehicles parked in the building’s parking garage are tangible assets.

Intangible assets include the livelihood of building users; intellectual property and information stored in paper files, reference books, microfilm, and within computer systems and peripherals; and the reputation and status of the facility.

Description of the Site, Building, and Surrounding Areas
The report should include a description of the site’s size, zoning, boundaries, and landscaping; a description of the building, including any overpasses or subterranean passageways; the building’s square footage, principal activities and usage, operating hours, and building population; nature of the surrounding area and occupancies; proximity to freeways, major roads, and public transportation terminals and stations; and the location or expected response times from the nearest police station and fire station. Any available maps, floor plans, or site photographs may be noted at this point. The following is a sample description of a high-rise office building and its surrounding area.

Pacific Tower Plaza is a prestigious, multiple-tenant, multiple-use high-rise complex used primarily for commercial office purposes. It is typically operational from 7 a.m. to 7 p.m. Monday to Friday and 9 a.m. to 2 p.m. on Saturday. It has restricted access at all other times. It is located in Toluga Hills, a major down-
Town financial district. It occupies one half of the city block bounded by Mount Waverley, Poppyfields, and La Perouse Boulevards and is located close to the Southwestern Freeway. The Toluga Hills Police Department has a main station within two miles of the complex, and Toluga Hills Fire Department Station 3, located within three city blocks, has an expected response time of three minutes. A high-rise residential building, a low-rise hotel, and a high-rise office building surround it.

Pacific Tower Plaza consists of a fully sprinklered 36-story office tower with a triple-level underground parking garage. The tower has 600,000 square feet of rentable office space, 7,000 square feet of rentable retail space, and 6,000 square feet of rentable storage space. The approximate size of each floor plate is 18,500 square feet. The perimeter of the building consists of sculptures, fountains, an open-air restaurant, and large planters containing flowers and small trees. The entrance to the building is through a large main lobby. The building has an approximate population of 2,400 occupants and 500 daily visitors. The onsite parking structure can accommodate up to 600 cars and connects to a subterranean pedestrian tunnel under Mount Waverley Boulevard.

The tower of Pacific Tower Plaza is a steel-framed reinforced concrete construction building. It has a conventional curtain wall consisting of glass in aluminum frames. The structural steel frame supports lightweight concrete floor slabs resting on metal decks atop horizontal steel beams, which are welded to vertical steel columns. The building is supported on a foundation of structurally reinforced concrete. The tower is designed with a concrete-reinforced center core, which houses the electrical, plumbing, and communications systems; the heating and air-conditioning (air supply and return) shafts; 17 passenger elevators, one service/freight elevator, and three parking shuttle elevators; and two major enclosed stairwells. Both stairwells provide egress to the street level and access to the roof (the doors leading to the roof are locked). The stairwells are pressurized and protected by fire-rated doors and walls.

Identification of Threats and Review of Past Incidents

Security and fire life safety threats to the assets are identified. This process should include a review of security-related incidents that have occurred at the site over a designated period of time. Shift activity and incident reports generated by security staff and police crime statistics for the reporting district encompassing the area should be considered.

In examining threats, consideration should also be given to those of neighboring facilities. For example, if an adjacent facility is a signature building at risk of an act of terrorism, this constitutes an indirect threat to the site being surveyed.

Security Measures and Recommendations

This section reviews the security measures currently in place to safeguard the assets. Areas that may be reviewed, depending on the scope of the survey, include perimeter barriers and fences, building construction and layout, lighting, intrusion detection and duress alarms, video surveillance systems, mobile patrols, access control of vehicles, people, and property, identification badges, locking and key controls, trash removal procedures, personnel security, written procedures and policies, and communications. Again, fear of crime and the incidence of crime, and to an improvement in the quality of life” (Crowe TD. Crime Prevention Through Environmental Design. 2nd ed. Woburn, MA: Butterworth-Heinemann; 2000:1).

“In its purest sense, CPTED is the passive use of the physical environment to reduce the opportunity for and fear of predatory stranger-to-stranger crime—burglary, robbery, assault, larceny, murder, rape, even bombing. CPTED relies on three main strategies: natural surveillance, natural access control, and territoriality—establishing boundaries and transitional spaces. CPTED looks at siting, landscaping, foot-prints, window schedules, facades, entrances, lobbies, layouts, lighting, materials, and traffic and circulation patterns” (Post NM. More than merely cops and robbers. Engineering News-Record. May 1, 1995:19). According to Atlas, CPTED incorporates five principles. The first is the use of natural surveillance. Sites are designed so that users can see farther and wider, making it harder for criminals to hide or carry out their activities. The second principle is the creation of natural access control, including spatial definition that encourages legitimate site users and discourages illegitimate ones. The third principle is the encouragement of territorial behaviors [i.e., encouraging the concept of owning and being responsible for a site or an area within it] by legitimate users. The fourth principle is management and maintenance of the facilities to meet industry standards of care. The fifth principle of CPTED is legitimate activity support, and encouraging and attracting legitimate and legal users and uses” (Atlas RI. Fear of parking. Security Management. Alexandria, VA; February 2008:54).
strengths as well as weaknesses or vulnerabilities should be pointed out to provide a balanced view of the security program. Also, the security measures should be benchmarked (i.e., evaluated relative to measures commonly found in office buildings, particularly neighboring ones). Recommendations should then be made for modifications or changes that reduce the risks to the assets. (Also, depending on the scope of the survey, monetary costs, if any, of the proposed recommendations might be included.)

The following is an example of a security measure with associated recommendations for improvement:

Access control of building occupants after normal business hours is determined by visual recognition of the tenants by the lobby security officer who then asks individuals authorized to enter to print their names, the name of the tenant by whom they are employed, and the date and time, and to sign their names on the after-hours building register. If the officer does not recognize an individual, a file of tenant occupants authorized for after-hours access is checked. If the individual is not listed, the lobby security officer calls the tenant suite to ask if anyone can authorize the individual’s entry. If no tenant is available, the individual is denied access. This procedure has caused continual problems because of the repeated denial of access to occupants who otherwise had permission from their employers to work in the building after hours. Two obvious reasons have been the failure of tenants to provide up-to-date listings of employees authorized to work after normal business hours and the high turnover of security personnel leading to many officers lacking familiarity with building users.

Recommendations

- Building management should approach all tenants who are not providing up-to-date, after-hour authorization lists, to reemphasize the need for such critical information.
- Building management should request that every tenant provide a list of key personnel who can be contacted after hours before any of their employees is denied after-hours access.
- Design an after-hours building access card, and request that tenants issue the completed card to all employees who need after-hours access.
- Obtain quotations from vendors to install a card access control system at the building.
- Investigate why the turnover of security staff is high.

Summary of Recommendations

This section is optional but may be included to summarize the findings of the survey. The recommendations for each security measure may be grouped together or separately listed, for example, according to monetary cost, those planned for immediate attention, and those to be addressed at a future time. Also, there could be a ranking of the recommendations, listing first those that, if implemented, would result in the greatest overall improvement in the performance and effectiveness of the security program; or the recommendations could be grouped into those providing low, medium, and high levels of security. Determining whether a particular security measure should be implemented will largely depend on the perceived vulnerability to the threat that the measure is designed to address and the anticipated consequences if the threat were actually to occur.

Executive Summary

This section is a summary of the report itself and should appear at its start. It provides the reader with a quick review of the survey and report by drawing attention to important items. A sample executive summary for Pacific Tower Plaza follows:

The survey was conducted on October 4–14, 2008. The primary objective for conducting this survey was to review the strengths and weaknesses in the security program at the Pacific Tower Plaza high-rise complex; in particular, reference is made to after-hours access control procedures of building occupants and the control of business and personal property leaving the site after normal business hours.

Interviews were conducted with management personnel of Pauley and Partners; managers of the security, engineering, janitorial, and parking departments; individual security staff members; and a representative of Columbus Insurance Company.
The survey revealed that building security staff has rigidly enforced after-hours access control procedures of the building. This has resulted in very few unauthorized persons gaining after-hours access to tenant offices but has led to the repeated denial of entry to occupants who otherwise had permission from their employers to work in the building after hours. The survey also revealed that there has been little control of business and personal property leaving the site after normal business hours. This factor is thought to have contributed considerably to the thefts of personal computers from secured tenant offices that have been occurring since the building was opened on January 1, 2008.

Some recommendations for improving the effectiveness of the security program at Pacific Tower Plaza are as follows:

Building management should approach all tenants who are not providing up-to-date, after-hour authorization lists, to reemphasize the need for such critical information.

Building management should request that every tenant provide a list of key personnel who can be contacted after hours before any of their employees is denied after-hours access.

Design an after-hours building access card, and request that tenants issue the completed card to all employees who need after-hours access.

Obtain quotations from vendors to install a card access control system at the building.

Design a property removal system to control the movement of business and personal property from the building. This system should be implemented as soon as possible after all tenants have been thoroughly informed of the new policy and their cooperation has been solicited in supporting it.

Encourage tenant representatives to inventory office equipment and to identify it clearly.

Encourage tenants to anchor items—personal computers and fax machines—using devices such as metal plates or steel cables.

Investigate why the turnover of security staff is high.

Building management representatives have indicated that they are very supportive of providing a sound security program for the tenants at Pacific Tower Plaza. They also appear willing, within reasonable cost constraints, to take whatever steps are necessary to achieve this goal.

Appendices
Any backup documentation and reference material that may help support the suggested recommendations, and floor plans, maps, diagrams, forms, and photographs may be included here to substantiate the work of the surveyor.

Presentation of the Report
Once the report is written it should be presented in an understandable manner that professionally reflects the work that has gone into preparing it. Each major section of the report should be tabbed and any photographs and drawings neatly mounted and labeled. The report should be placed in a three-ringed binder or professionally bound.

If at all possible, the survey report should be personally presented to the parties requesting the project. Depending on the time allotted, one can be thorough or brief in presenting the material. For a formal presentation one may elect to use computer screen displays, overhead transparencies, slides, or simply a page-by-page review of the report. Such presentations can be of immense value in making salient points clear and understandable. Also, the opportunity for questions and clarification of issues will increase the chance that the recommendations and suggestions will be implemented.

Word of Caution
A word of caution, learned through the bitter school of experience: the surveyor should reserve professional opinions as to the state of the overall security program until the fact-finding process and the writing of the report are nearing completion. Of course, there are exceptions to the rule, but, particularly with major surveys, one needs to assimilate all the information collected before thoroughly understanding what is happening within the security program. Often one aspect of the survey is closely interwoven with another.
For example, in conducting a security survey primarily to investigate theft occurring at an office building, one may immediately conclude that the solution to the problem is to implement a screening procedure in the building main lobby to control property removal. At the time, this may appear to be the complete answer to the problem. However, at a later stage in the survey, it may be discovered that building tenants can use passenger elevators at any time to exit their floor and travel directly down to the under-building parking garage, thereby bypassing the building main lobby and walking unobserved to a vehicle. In this case, property removal controls in the building main lobby will be ineffective unless other measures are incorporated into the security program. Such measures may include reprogramming the elevators, particularly after normal business hours, to descend from the tower and terminate service in the main lobby; other elevators can be programmed to serve the lower parking levels. This arrangement will cause occupants to pass through the building’s main lobby and thereby permit an effective property removal control procedure to be instituted.

Building Fire Prevention Survey

A fire life safety survey has similar objectives to a security survey. Its aims are “to ascertain the present [life safety] status, to identify deficiencies or excesses, to determine the [fire and life safety] protection needed, and to make recommendations to improve the overall [fire life safety]”\(^\text{19}\) of the building under evaluation.

A fire life safety survey also can be as extensive or as restricted as the surveyor determines. Like a formal security survey, a fire life safety survey will involve two major tasks: the fact-finding investigative process and the writing of the report that reflects the findings. The fire life safety survey is predominantly concerned with life safety threats that may be deliberately or accidentally caused; it tends to analyze preventive measures to reduce the risk of such occurrences that, particularly if left unattended, may result in serious property damage, injury, or even death.

Fact-Finding Process

The fact-finding process for the fire life safety survey resembles that of a security survey, with the following exceptions:

1. The principal activities and the usage of the facility are critical elements of any survey and are particularly important from a fire life safety perspective. For example, if the building is a hotel containing a casino where occupants will usually not be familiar with the layout of the facility, special measures may be required to safely evacuate people during an emergency.
2. A review of state and local building and fire prevention laws and codes for mandated fire life safety requirements is necessary to determine if the facility is in full compliance.
3. In reviewing documentation, the testing records of fire life safety equipment and systems and the Building Emergency Procedures Manual (described in Chapters 9 to 12) should be reviewed. Testing records need to be checked to ensure that testing is adequate, according to accepted practices, and is being conducted in a timely

manner by certified persons or companies. The Building Emergency Procedures Manual should be examined to ascertain if it is accurate, up-to-date, and adequately covers all emergencies that have occurred or are likely to occur at the site.

4. Insurance policies need to be reviewed to determine whether present or planned fire life safety measures are of an acceptable level and the fire life safety systems and equipment meet the standards as outlined in the policies.

Survey Checklist

To assist in the fact-finding process, it is helpful to use a checklist of areas to be covered. Such a checklist, emphasizing fire prevention, is provided in Appendix 4–2 (on the CD-ROM accompanying this book). The National Fire Protection Association’s *Fire Protection Handbook*\(^{20}\) is organized around six major fire safety strategies in designing building fire safety: prevention of ignition, design to slow early fire growth, detection and alarm, suppression, confinement, and evacuation of occupants. The fire prevention survey checklist in Appendix 4–2 touches on these areas. However, it does not specifically address the design or fire-resistive construction aspects of a high-rise building nor does it purport to cover all branches of the *Fire Safety Concepts Tree* used as a model by the National Fire Protection Association.\(^{21}\) If other types of surveys are to be conducted, then the checklist will need to be modified to make it appropriate. The local fire department may require or recommend a particular fire inspection form.

The sample fire prevention survey checklist in Appendix 4–2 is intended for use by a fire safety director, life safety manager, risk manager, security director, building engineer, or other member of building management who desires to evaluate the fire prevention program in place at their facility. It may be used for several reasons:

1. To review the fire prevention program with respect to certain incidents which have occurred
2. In preparation for a visit by the city or state fire marshal, a fire department inspector, a representative of the building’s owner or operator, or the insurance company providing coverage for the building
3. As part of a regular self-inspection program to ensure that the building’s fire prevention program is adequate and properly maintained in accordance with the policies of the building’s owner or operator

If a more extensive analysis of a building’s fire life safety program is required, an outside consultant or specialist, such as a registered fire protection engineer, could be considered. More will be said about consultants or specialists later in this chapter.

In the fact-finding process, a thorough walkthrough to observe fire prevention problems or violations of the building’s fire life safety practices should be conducted with the person who is most knowledgeable of the building and its fire life safety systems. This person will probably be the building engineer and/or the fire safety director. Consider starting the walkthrough on the roof of the building and proceed down the stairwells and throughout each floor of the building. The reason for starting on the

---


roof is that it is easier to walk down than to walk up a high-rise building, particularly if one is surveying a 60-floor skyscraper! In walking a floor, the actual areas visited will depend on the building’s occupancy, keeping in mind the following:

- **An office building.** Public access or common areas such as the elevator lobbies and corridors; loading dock areas; building conference and meeting rooms; building maintenance areas including elevator machine rooms, mechanical rooms, telecommunications equipment, janitorial closets, paint rooms or paint storage rooms, and other limited access spaces; and tenant suites.

- **A hotel building.** Public access or common areas such as the elevator lobbies and corridors; loading dock areas; conference and meeting rooms; health club, gymnasium, fitness rooms, and recreation areas; kitchen, restaurant, food preparation, and food storage areas; laundry and dry cleaning facilities; and building maintenance areas that may include elevator machine rooms, mechanical rooms, telecommunications equipment, janitorial closets, paint rooms or paint storage rooms, and other limited access spaces.

- **A residential and apartment building.** Public access or common areas such as the elevator lobbies and corridors; loading dock areas; building conference and meeting rooms; health club, gymnasium, fitness rooms, and recreation areas; kitchen, restaurant, food preparation, and food storage areas; laundry and dry cleaning facilities; tenant storage lockers or cages; and building maintenance areas that may include elevator machine rooms, mechanical rooms, telecommunications equipment, janitorial closets, paint rooms or paint storage rooms, and other limited access spaces.

When surveying a hotel or a residential and apartment building, unless there is a compelling reason to do so, one will usually not venture inside guest rooms or individual apartments. Sufficient reasons to enter would include past incidents of a fire life safety nature in an apartment, a spot check of fire prevention practices such as storage of combustible materials, or a structural build-out or alteration of an apartment that has occurred since the last inspection. Of course, there are exceptions, particularly with regard to hotel suites. For example, incidents have occurred in hotels where guests have set up a temporary methamphetamine drug laboratory in a guest room. After several days, they have departed leaving behind the room contaminated with dangerous drug-manufacturing process residues.

The purpose of the walkthrough is to observe fire prevention problems or violations of the building’s fire life safety practices.

The main sections in a fire prevention survey checklist may include general information; building information; building layout and exits; cafeteria/kitchen; building emergency exit signage; fire protective signaling systems; smoke control systems; fire suppression systems; portable fire extinguishers; emergency and standby power and lighting systems; testing and maintenance of fire life safety systems; surface finishes of interior ceilings, floors, and walls; general housekeeping, storage procedures, and adherence to safety; fire guard operations; building emergency management plan, fire life safety plan, or emergency action plan; fire life safety education; and insurance. (See Appendix 4–2 for complete details.)

Once again, because every building is different, this generic checklist does not cover all aspects of the facility being surveyed. If a checklist is to be used, it should be tailored specifically to the type of occupancy and its appropriate fire prevention program.
Writing the Report

Writing the report will involve assembling the ideas and information obtained in the fact-finding investigative process. Weaknesses in the fire prevention program should be pointed out, with suggested recommendations to address them, but strengths also should be listed. The suggested format previously outlined for writing the security survey also can be adapted for writing the fire prevention survey.

Risk Assessment to Mitigate Potential Terrorist Attacks against Buildings

A comprehensive risk assessment methodology, developed by the Federal Emergency Management Association (FEMA), can be used to mitigate the effects of potential terrorist attacks against buildings. Called Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings, the objective of this How-To Guide is to outline methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. Based on those considerations, the methods presented in this How-To Guide provide a means to assess the risk to the assets and to make risk-based decisions on how to mitigate those risks. The scope of the methods includes reducing physical damage to structural and non-structural components of buildings and related infrastructure, and reducing resultant casualties during conventional bomb attacks, as well as chemical, biological, and radiological (CBR) agents. This document is written as a How-To Guide. It presents five steps and multiple tasks within each step that will lead through a process for conducting a risk assessment and selecting mitigation options. It discusses what information is required to conduct a risk assessment, how and where to obtain it, and how to use it to calculate a risk score against each selected threat.


potential vulnerability of the critical assets against a broad range of identified threats/hazards. In and of itself, the vulnerability assessment provides a basis for determining mitigation measures for protection of the critical assets. The vulnerability assessment is the bridge in the methodology between threat/hazard, asset value, and the resultant level of risk.

The next step of the process is the risk assessment (Step 4). The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple low cost mitigation measures [countermeasures], but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with the identified vulnerability, allow prioritization of resources to implement mitigation measures.

The final step (Step 5) is to consider mitigation options that are directly associated with, and responsive to, the major risks identified during Step 4. From Step 5, decisions can be made as to where to minimize the risks and how to accomplish that over time. This is commonly referred to as Risk Management.23
The following material further explains the steps in this risk assessment model:

**Step I: Threat Identification and Rating**

The first step in the assessment process is to help to identify threats that are a priority concern in an area and that may pose a risk to its assets.

The threat identification and rating process involves the following tasks:

- Identifying the threats
- Collecting information
- Determining the design basis threat
- Determining the threat rating

**Identifying the Threats**

For this document, threat is defined as any indication, circumstance, or event with the potential to cause loss of or damage to an asset. In this guide, only manmade terrorist threats are considered.

Identifying the threats can be a difficult task. Because manmade hazards are different from other hazards such as earthquakes, floods, and hurricanes, they are difficult to predict. Many years of historical and quantitative data and probabilities associated with the cycle, duration, and magnitude of natural hazards exist. The fact that data for manmade hazards are scarce and that the magnitude and recurrence of terrorist attacks are almost unpredictable makes the determination of a particular threat for any particular site or building difficult and largely subjective.

With any terrorist threats, it is important to understand who the people are with the intent to cause harm. The aggressors seek publicity for their cause, monetary gain (in some instances), or political gain through their actions. These actions include injuring or killing people; destroying or damaging facilities, property, equipment, or resources; or stealing equipment, material, or information. In some cases, the threat may originate from more than one group, with differing methods and motives.

Aggressor tactics run the gamut: moving vehicle bombs; stationary vehicle bombs; bombs delivered by persons (suicide bombers); exterior attacks (thrown objects like rocks, Molotov cocktails, hand grenades, or hand-placed bombs); attack weapons (rocket propelled grenades, light antitank weapons, etc.); ballistic attacks (small arms handled by one individual); covert entries (gaining entry by false credentials or circumventing security with or without weapons); mail bombs (delivered to individuals); supply bombs (larger bombs processed through shipping departments); airborne contamination (chemical, biological, or radiological [CBR] agents used to contaminate the air supply of a building); and waterborne contamination (CBR agents injected into the water supply).

**Collecting Information**

When collecting information for the threat assessment, the following questions may be asked: What groups or organizations exist/are known? Do they have capability among
themselves or is that capability readily obtainable locally? Do they have a history of terrorist acts and what are their tactics? What are the intentions of the aggressors against the government, commercial enterprises, industrial sectors, or individuals? Has it been determined that targeting (planning a tactic or seeking vulnerabilities) is actually occurring or being discussed?

Many security and intelligence organizations are a good source of information and data for threat assessments. Additionally, most fire departments understand which industries in the local area handle the most combustible materials and the HazMat [hazardous materials] unit understands who handles materials that could have a negative impact upon people and the environment. In many jurisdictions, the HazMat unit is part of the fire department.

**Determining the Design Base Threat**

Unlike natural disasters, terrorists continually evaluate, plan, and seek to exploit the weakest building protective design features. Therefore, it becomes impossible both from a technical and benefit/cost point to try to protect everything from every type of attack. The building stakeholders have to make a determination as to what the design basis threat is for their building and what level of protection they can afford. As the terrorist threat changes over time, the building stakeholders may wish to revisit this part of the risk assessment process.

To select primary threats, the criteria described below have been provided.

- **Access to agent.** The ease by which the source material can be acquired to carry out the attack. Consideration includes the local materials of HazMat inventory, farm and mining supplies, major chemical or manufacturing plants, university and commercial laboratories, and transportation centers.
- **Knowledge/expertise.** The general level of skill and training that combines the ability to create the weapon (or arm an agent) and the technical knowledge of the systems to be attacked (heating, ventilation, and air conditioning [HVAC], nuclear, etc.). Knowledge and expertise can be gained by surveillance, open source research, specialized training, or years of practice in industry.
- **History of threats (building functions/tenants).** What has the potential threat element done in the past, how many times, and was the threat local, regional, national, or international in nature? When was the most recent incident and where, and against what target? Are the building functions and tenants attractive targets for the terrorist?
- **Asset visibility/symbolic.** The economic, cultural, and symbolic importance of the building to society that may be exploited by the terrorist seeking monetary or political gain through their actions.
- **Asset accessibility.** The ability of the terrorist to become well-positioned to carry out an attack at the critical location against the intended target. The critical location is a function of the site, the building layout, and the security measures in place.
- **Site population/capacity.** The population demographics of the building and surrounding area.
- **Collateral damage/distance to the building.** The potential of the threat to cause collateral damage or disruption to the building of interest. The building of interest is not considered the primary target.
**Determining the Threat Rating**

Having selected the primary threats for the site or building, the next step is to determine how the threat will affect the functions and critical infrastructure. The threat rating is an integral part of the risk assessment and is used to determine, characterize, and quantify a loss caused by an aggressor using a weapon or agent and tactic against the target (asset). The threat rating deals with the likelihood or probability of the threat occurring and the consequences of its occurrence.

For determining the threat rating, this How-To Guide provides a methodology based on consensus opinion of the building stakeholders, threat specialists, and engineers. (This group could be expanded as necessary to help refine the scoring process.) Table 4–1 provides a scale to help with this process. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). The key elements of this scale are the likelihood/credibility of a threat, potential weapons to be used during a terrorist attack, and information available to decision makers. The primary objective is to look at the threat, the geographic distribution of functions and critical infrastructure, redundancy, and response and recovery to evaluate the impact on the organization should a primary threat attack occur.

**Step 2: Asset Value Assessment**

The second step in the assessment process is to identify the assets of the area, site, and building that may be affected by a threat. Asset value can be defined as a degree of debilitating impact that would be caused by the incapacity or destruction of an asset. An asset refers to a resource of value requiring protection. It can be tangible (i.e., buildings,

<table>
<thead>
<tr>
<th>Threat Rating</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>10</td>
<td>Very high—The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat is credible.</td>
</tr>
<tr>
<td>High</td>
<td>8–9</td>
<td>High—The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat is credible.</td>
</tr>
<tr>
<td>Medium high</td>
<td>7</td>
<td>Medium high—The likelihood of a threat, weapon, and tactic being used against the site or building is probable. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat is credible.</td>
</tr>
<tr>
<td>Medium</td>
<td>5–6</td>
<td>Medium—The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat is credible.</td>
</tr>
<tr>
<td>Medium low</td>
<td>4</td>
<td>Medium low—The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat is known but is not verified.</td>
</tr>
<tr>
<td>Low</td>
<td>2–3</td>
<td>Low—The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat exists but is not likely.</td>
</tr>
<tr>
<td>Very low</td>
<td>1</td>
<td>Very low—The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat is nonexistent or extremely unlikely.</td>
</tr>
</tbody>
</table>
facilities, equipment activities, operations, and information) or intangible (i.e., processes or a company’s information and reputation).

The asset value assessment process involves the following tasks:

- Identifying the layers of defense
- Identifying the critical assets
- Identifying the building core functions and infrastructure
- Determining the asset value rating

**Identifying the Layers of Defense**
In this How-To Guide, the identification of the assets is done within the concept of layers of defense (discussed earlier in this chapter). The objective of layers of defense is to create a succeeding number of security layers that are more difficult to penetrate, provide additional warning and response time, and allow building occupants to move into defensive positions or designated safe haven protection. This approach is especially helpful for identifying mitigation options after conclusion of the risk assessment.

**Identifying the Critical Assets**
This task involves identifying critical assets within each layer of defense. The purpose is to help determine those assets essential to the minimum operation of a building and to ensure the health and safety of the building and its occupants.

**Identifying the Building Core Functions and Infrastructure**
The identification of the building core functions and infrastructure is one of the key elements of the assessment.

**Identifying Building Core Functions**
Determine the core functions and processes necessary for the building to continue to operate or provide services after an attack. The reason for identifying core functions/processes is to focus the Assessment Team on what a building does, how it does it, and how various threats can affect the building. This provides more discussion and results in a better understanding of asset value. Factors that should be considered include the following:

- What are the building’s primary services or outputs?
- What critical activities take place at the building?
- Who are the building’s occupants and visitors?
- What inputs from external organizations are required for a building’s success?

**Identifying Building Core Infrastructure**
After the core functions and processes are identified, an evaluation of building infrastructure should follow. To help identify and value rank infrastructure, the following should be considered, keeping in mind that the most vital asset for every building is its people:

- Identify how many people may be injured or killed during a terrorist attack that directly affects the infrastructure.
- Identify what happens to occupants if a specific asset is lost or degraded. (Can primary services continue?)
• Determine the impact on other organizational assets if the component is lost or cannot function.
• Determine if critical or sensitive information is stored or handled at the building.
• Determine if backups exist for the building’s assets.
• Determine the availability of replacements.
• Determine the potential for injuries or deaths from any catastrophic event at the building’s assets.
• Identify any critical building personnel whose loss would degrade or seriously complicate the safety of building occupants during an emergency.
• Determine if the building’s assets can be replaced and identify replacement costs if the building is lost.
• Identify the locations of key equipment and the impact if it is lost during a terrorist attack.
• Determine the locations of personnel work areas and systems.
• Identify the locations of any personnel operating “outside” a building’s controlled areas.
• Determine, in detail, the physical locations of critical support architectures:
  ○ Communications and information technology (i.e., the flow of critical information)
  ○ Utilities (e.g., facility power, water, air conditioning, etc.)
  ○ Lines of communication that provide access to external resources and provide movement of people (e.g., road, rail, air transportation)
• Determine the location, availability, and readiness condition of emergency response assets, and the state of training of building staff in their use.

A number of core infrastructures have been selected for this How-To Guide. Table 4–2 includes the selected examples.

Determining the Asset Value Rating
After building core functions and building infrastructure are analyzed, a value should be assigned. Table 4–3 provides a scale for selecting asset value. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). To determine a value, one should keep in mind that asset value can be defined as the degree

<table>
<thead>
<tr>
<th>Table 4–2 Building Core Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Core Infrastructure</td>
</tr>
<tr>
<td>Site</td>
</tr>
<tr>
<td>Architectural</td>
</tr>
<tr>
<td>Structural systems</td>
</tr>
<tr>
<td>Envelope systems (building envelope)</td>
</tr>
<tr>
<td>Utility systems</td>
</tr>
<tr>
<td>Mechanical systems</td>
</tr>
<tr>
<td>Plumbing and gas systems</td>
</tr>
<tr>
<td>Electrical systems</td>
</tr>
<tr>
<td>Fire alarm systems</td>
</tr>
<tr>
<td>IT/Communications Systems</td>
</tr>
</tbody>
</table>
of debilitating impact that would be caused by the incapacity or destruction of the building’s assets. To determine a [...] rating, one should consider the consequences of the loss or damage of the building’s assets (e.g., loss of life, injuries, loss of primary services, or major loss of core processes and functions). The key asset for every building is its people (e.g., employees, visitors, etc.), and they will always be assigned the highest asset value.

**Step 3: Vulnerability Assessment**

The third step in the assessment process is to prepare a vulnerability assessment of the assets that can be affected by a threat. For this document, vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to hazard damage. A vulnerability assessment is an in-depth analysis of the building functions, systems, and site characteristics to identify building weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities. During this step, an analysis will begin of the assets based on (1) the identified threat, (2) the criticality of the assets, and (3) the level of protection that has been chosen (i.e., the willingness or unwillingness to accept risk).

The vulnerability assessment process involves the following tasks:

- Organizing resources to prepare the assessment
- Evaluating the site and building
- Preparing a vulnerability portfolio
- Determining the vulnerability rating

**Organizing Resources to Prepare the Assessment**

An important task during Step 3 is organizing resources to prepare the assessment. This involves determining the level of the assessment to perform and the skills of the team necessary to conduct the assessment.
Selecting the Assessment Team

The selection of the Assessment Team is probably the most critical task in the [...] assessment process. An assessment has been found to be most effective when the team is composed of senior individuals who have a breadth and depth of experience and understand other disciplines and system interdependencies. The Assessment Team leader will work with the building owner and stakeholders to do the following:

- Determine the threat rating (Step 1)
- Determine the asset value (Step 2)

The Assessment Team will coordinate the preparation of an assessment schedule, assessment agenda, and onsite visit assessments with the building stakeholders. It is important to emphasize that the Assessment Team should be composed of professionals capable of evaluating different parts of the buildings and familiar with engineering, architecture, [security,] and site planning. Other members of the team may include [security professionals,] law-enforcement agents, first responders, and building owners and managers.

Determining the Level of Assessment

The level of the assessment for a given building is dependent upon a number of factors such as type of building, location, type of construction, number of occupants, economic life, and other owner specific concerns and available economic resources. The levels of the assessment provided in this How-To Guide are similar to the FEMA 310 process and provide increasing tiers of assessments. The underlying purpose is to provide a variable scale to meet benefit/cost considerations for a given building that meets the intent and requirements of available antiterrorism guidelines such as the DoD [Department of Defense] Minimum Antiterrorism Standards and the GSA [General Services Administration] Interagency Security Criteria.

Tier 1. A Tier 1 assessment is a screening phase that identifies the primary vulnerabilities and mitigation options, and is a “70 percent” assessment. A Tier 1 assessment can typically be conducted by one or two experienced assessment professionals in approximately 2 days with the building owner and key staff; it involves a “quick look” at the site perimeter, building, core functions, infrastructure, drawings, and plans. A Tier 1 assessment will likely be sufficient for the majority of commercial buildings and other non-critical facilities and infrastructure.

Tier 2. A Tier 2 assessment is a full on-site evaluation by assessment specialists that provides a robust evaluation of system interdependencies, vulnerabilities, and mitigation options; it is a “90 percent” assessment solution. A Tier 2 assessment typically requires three to five assessment specialists, can be completed in 3 to 5 days, and requires significant key building staff participation (e.g., providing access to all site and building areas, systems, and infrastructure) and an in-depth review of building design documents, drawings, and plans. A Tier 2 assessment is likely to be sufficient for most high-risk
buildings such as iconic commercial buildings, government facilities, schools, hospitals, and other designated high value infrastructure assets.

**Tier 3.** A Tier 3 assessment is a detailed evaluation of the building using blast and weapons of mass destruction (WMD) models to determine building response, survivability, and recovery, and the development of mitigation options. A Tier 3 assessment typically involves engineering and scientific experts and requires detailed design information, including drawings and other building information. Modeling and analysis can often take several days or weeks and is typically performed for high value and critical infrastructure assets. The Assessment Team is not defined for this tier; however, it could be composed of 8 to 12 people.

**Evaluating the Site and Building**

Understanding the type, nature, and geographic range of threats (Step 1) that can occur at a site or building, as well as the associated exposure of the assets (Step 2), is essential to conducting a vulnerability analysis. Each building, even if on the same campus or the same general area, can have different priority threats and hazards. A well-prepared risk manager must be aware of the types of threat and hazard events that can occur, the areas and resources most at risk, and the potential costs and losses that could accompany a threat or hazard event.

To prepare an effective assessment, the following activities should take place:

1. **Premeeting and preparation of a schedule and tentative agenda.** Before conducting the onsite building evaluation, a coordination meeting should take place. During this meeting, the type of assessment to be conducted, personnel availability, schedules, and outputs should be discussed in detail. In addition, firm timetables and an agenda for onsite visits should be discussed. The agenda schedule should include the sites to be evaluated and special areas to be protected.

2. **Onsite meeting(s).** For each assessment, a preparation meeting will take place with key stakeholders. Upon arrival at the site or building, the team should have an introduction meeting with key staff, review the available information, and review the vulnerability portfolio (discussed later).

3. **Windshield tour(s).** After the introduction meeting, the Assessment Team and stakeholders should conduct a “windshield” tour or walk-around of the key facilities. The Assessment Team may find areas that require special attention and feel the need to make adjustments to the assessment agenda.

4. **Assessment background information.** After the onsite tour, the Assessment Team and stakeholders are ready to conduct the onsite assessment.

5. **Review key documents.** The Assessment Team will review or evaluate a number of plans, procedures, and policies.

6. **Review emergency procedures.** The Assessment Team and building stakeholders should review the security master plan and the engineering operations and maintenance, emergency operations, and disaster recovery plans to understand the critical assets of the building and establish a baseline organization response and recovery capability in case of an attack or event.

7. **Prepare the assessment.** Preparing the assessment can be as simple as a quick review and analysis of existing documents and a short walk around the site or a more detailed in-depth review and analysis of the documents, plans, and
other information and a thorough walk-through of the building [i.e., the level of the assessment—such as Tier 1, Tier 2, or Tier 3 as described in the previous section—will determine the extent of the preparation of the assessment].

8. Data gap analysis. The Assessment Team may feel that the data gathered for onsite assessment [is] not enough. The team should assess the following information:
   - Do we know where the greatest damages may occur in the threat/hazard areas?
   - Do we know whether critical facilities will be operational after a threat/hazard event?
   - Are there enough data to determine which assets are subject to the greatest potential damages?
   - Are there enough data to determine whether significant elements of the community are vulnerable to potential threats?
   - Are there enough data to determine whether certain areas of historic, environmental, political, or cultural significance are vulnerable to potential threats?
   - Is there concern about a particular threat because of its severity, frequency, or likelihood of occurrence?
   - Are additional data needed to justify the expenditure of community or state funds for mitigation initiatives?
   - If the team decides that more data will be beneficial to conduct the assessment, a determination should be made as to what type of data [is] needed and what resources are available for collecting new data. If stakeholders and the team agree on collecting new data, the team needs to prioritize areas for additional data collection.

Preparing a Vulnerability Portfolio

To carry out the assessment, the team should have a vulnerability portfolio available. This portfolio should include the following:

- Assessment agenda
- Assessment background information (to be collected by Assessment Team and building owners)
- Threats rating
- Asset value ranking
- Key documents (plans, procedures, and policies)
- Emergency procedures (baseline organization response and recovery capability in case of an attack or event)
- Building Vulnerability Assessment Checklist
- Risk assessment matrices (described in Step 4)

*There are various worksheets provided to accompany these portfolio items. They are contained within FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; January 2005.

**The Building Vulnerability Assessment Checklist appears in Appendix A of FEMA 452 and “compiles many best practices based on technologies and scientific research to consider during the design of a new building or renovation of an existing building. It allows a consistent security evaluation of designs at various levels.

“The Checklist is a key tool in the preparation of the threat assessment and a fundamental element of your vulnerability portfolio. When performing a walk-through of the facility to be assessed, the team should use the Checklist as a screening tool for preparing the vulnerability assessment and make observations when reviewing the questions included in the Checklist” (FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; January 2005:3–12).
Prioritization of observations in the checklist

Risk Assessment Database

The Building Vulnerability Assessment Checklist and the Risk Assessment Database can be used to collect and report information related to the building infrastructure.

Determining the Vulnerability Rating

This task involves determining a vulnerability rating that reflects the weakness of functions, systems, and sites in regard to a particular threat. Weakness includes the lack of redundancies that will make the building system operational after an attack.

For this How-To Guide, the following scale for vulnerability has been selected. Table 4-4 provides a scale for selecting the vulnerability rating. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). The key elements of this scale are the weaknesses of the building and easiness and/or difficulties that the aggressors may face when wishing to generate damage to the building. Also, the loss of operations in case of an attack and the lack of redundancies are considered.

Step 4: Risk Assessment

The fourth step in the assessment process is to prepare a risk assessment for the site and building. The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood of the threat occurring and the consequences of the occurrence.

Risk is the potential for a loss or damage to an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it. Risk is based on the likelihood or probability of the hazard occurring and the consequences of the occurrence. A risk assessment analyzes the threat (probability of occurrence), asset value (consequences of the occurrence), and vulnerabilities to ascertain the level of risk for each asset against each applicable threat/hazard. The risk assessment provides engineers

“The Checklist can be used as a screening tool for preliminary design vulnerability assessment and supports the preparation of all steps in this How-To Guide.

“The Checklist is organized into 13 sections: 1) site, 2) architectural, 3) structural systems, 4) building envelope, 5) utility systems, 6) mechanical systems, 7) plumbing and gas systems, 8) electrical systems, 9) fire alarm systems, 10) communications and information technology (IT) systems, 11) equipment operations and maintenance, 12) security systems, and 13) security master plan. To conduct a vulnerability assessment of a building or preliminary design, each section of the Checklist should be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area. Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. The observations made during this Step will be prioritized during Step 4. The observations in the Checklist should be supplemented with photographs, if possible. The results of the 13 assessments should be integrated into a master vulnerability assessment and provide a basis for determining vulnerability ratings during the assessment process” (FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; January 2005:A-1 [Appendix A]).

To support the risk assessment process, an easy-to-use Risk Assessment Database is available as part of FEMA 452. This database is a stand-alone application that has functions to import and display digital photos, emergency plans, digital floor plans, and certain GIS products. This Risk Assessment Database can be downloaded from the FEMA website (http://www.fema.gov/plan/prevent/rms/rmsp452.shtm) (FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. January 25, 2008.

The use of the term risk assessment here to describe Step 4 may be somewhat confusing to the reader because this step is but one in the entire “Risk Assessment” Process Model.
and architects [and security professionals] with a relative risk profile that defines which assets are at the greatest risk against specific threats.

There are a number of methods and means to conduct a building risk assessment, and the steps can be accomplished in different sequences. However, they all have one common objective, which is to apply a quantitative assessment process that identifies those assets at highest risk and evaluate mitigation measures that can reduce that risk.

For this How-To Guide, the approach is to assemble the results of the threat assessment, asset value assessment, and vulnerability assessment and determine a numeric value of risk for each asset and threat/hazard pair in accordance with the following formula:

\[
\text{Risk} = \text{Asset Value} \times \text{Threat Rating} \times \text{Vulnerability Rating}
\]

The results of the risk assessment should be used to help prioritize which mitigation measures should be adopted, given limited resources, in order to achieve a desired level of protection.

**Step 5: Consider Mitigation Options**

The fifth step in this How-To Guide is to identify and evaluate various mitigation options that are directly associated with, and responsive to, the major risks identified.
during Step 4. After the risk assessment process is completed, the stakeholders are frequently left with several areas where assets require mitigation measures and are limited by factors discussed in this step. Thus, decisions need to be made to focus the available resources on the most practical mitigation options.

The “consider mitigation options process” involves the following tasks:

- Identifying preliminary mitigation options
- Reviewing mitigation options
- Estimating cost
- Reviewing mitigation options, cost, and the layers of defense

Step 5 emphasizes mitigation measures that can reduce the destructive effects against buildings in case of a terrorist attack. During this step, the mitigation options are examined from the point of view of their effectiveness, acceptability, and feasibility with respect to prevailing implementation conditions. The proposed procedure for examining the mitigation options is not meant to replace full and thorough analysis of the technical assessment; it is meant to help narrow down options and focus attention on those measures that have the greatest chance of effective implementation.

In order to identify, select, and implement the most appropriate mitigation measures, general mitigation goals and objectives and the merits of each potential mitigation measure should be examined. The building owner may make the final decision regarding which mitigation measures should be implemented. However, engineers, architects, landscape architects, [security professionals,] and other technical people should be involved in this process to ensure that the results of the risk assessment are met with sound mitigation measures that will increase the capability of the building to resist potential terrorist attacks.

The selection of the level of protection is building-dependent.

To select, evaluate, and prioritize potential mitigation options, this How-To Guide has selected criteria that help to answer the following questions:

- Which mitigation measures are most appropriate for the types of risks faced by the assets?
- Are resources and capabilities sufficient to implement these measures and what additional resources might be needed?
- What impacts will the implementation of these measures have in areas surrounding the building(s) or in the community?

Within the United States, various government agencies, such as “The General Services Administration (GSA) and DoD [the Department of Defense] have developed standards and recommendations that can be applicable to buildings leased by or used to support Federal Government agencies. These standards and recommendations are not required for non-Federal buildings; however, building owners can evaluate and select those standards that meet their specific needs and criteria.

“A primary concern is the protection of buildings from explosive blast and CBR attacks. To protect against blast, the level of protection is dependent upon the type of construction and the blast pressures (stand-off distance). The amount of explosive and the resulting blast dictate the level of protection required to prevent a building from collapsing or minimizing injuries and deaths....

“The DoD prescribes minimum stand-off distances based on the required level of protection. Where minimum stand-off distances are met, conventional construction techniques can be used with some modifications. In cases where the minimum stand-off cannot be achieved, the building must be hardened to achieve the required level of protection” (FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. FEMA Risk Management Series, Washington, DC; January 2005:2–20).
Identifying Preliminary Mitigation Options
Mitigation measures can be viewed from many different perspectives. In this How-To Guide, the emphasis is on addressing building infrastructure and core building functions. The purpose is to identify sound mitigation measures directed at reducing the effects of potential terrorist attacks on the built environment. For this task, three broad categories have been identified:

- Regulatory measures
- Repair and strengthening of existing structures
- Protective and control measures

Regulatory Measures
Regulatory measures include legal and other regulatory instruments that governments use to prevent, reduce, or prepare for the losses associated with manmade hazard events that affect commercial buildings, which are the central topic of this How-To Guide. Examples include the following:

- Legislation that organizes and distributes responsibilities to protect a community from manmade threats
- Regulations that reduce the financial and social impact of manmade hazards through measures, such as insurance
- New or updated design and construction codes
- New or modified land use and zoning regulations
- Incentives that provide inducements for implementing mitigation measures

In most cases, regulatory measures should be considered before implementing other measures because regulatory measures provide the framework for decision making, organizing, and financing of mitigation actions.

Repair and Strengthening of Existing Structures
As its name implies, repair and strengthening deals with structural and nonstructural modifications of existing buildings and infrastructure facilities. Although new construction can include protective measures to reduce the potential impact against terrorist attacks, existing buildings may be at risk because they were constructed without the appropriate safety measures to withstand potential terrorist attacks. Thus, improving the safety and structural integrity of existing buildings and infrastructure facilities is often the best way to reduce the impact of manmade events on such structures.

When a manmade hazard occurs, it can directly damage a target building or indirectly cause secondary effects in adjacent buildings. The level of damage is impacted by each structure’s quality of design and construction. Poorly engineered and constructed buildings are usually not able to resist the forces generated by a blast event or serve as safe havens in case of CBR (chemical, biological, and radiological) attacks.

Protective and Control Measures
Unlike other mitigation measures that improve the resistance of buildings and infrastructure to disasters, protective and control measures focus on protecting structures by deflecting the destructive forces from vulnerable structures and people.

Ideally, a potential terrorist attack is prevented or pre-empted through intelligence measures. If the attack does occur, physical security measures combine with operational forces (e.g., surveillance, guards, and sensors) to provide layers of defense that delay and/or
thwart the attack (for more information, see [“Layers of Defense” section at the commence ment of this chapter]). Deception may be used to make the facility appear to be a more protected or lower-risk facility than it actually is, thereby making it a less attractive target. Deception can also be used to misdirect the attacker to a portion of the facility that is noncritical. As a last resort, structural hardening is provided to save lives and facilitate evacuation and rescue by preventing building collapse and limiting flying debris.

Because of the interrelationship between physical and operational security measures, it is imperative for the owner and security professional to define, early in the design process, what extent of operational security is planned for various threat levels. If properly implemented, physical security measures will contribute toward the goals listed below in prioritized order.

- **Preventing an attack.** By making it more difficult to implement some of the more obvious attack scenarios (such as a parked car in the street) or making the target appear to be of low value in terms of the amount of sensation that would be generated if it were attacked, the would-be attacker may become discouraged from targeting the building. On the other hand, it may not be advantageous to make the facility too obviously protected or not protected, because this may provide an incentive to attack the building.

- **Delaying the attack.** If an attack is initiated, properly designed landscape or architectural features can delay its execution by making it more difficult for the attacker to reach the intended target. This will give the security forces and authorities time to mobilize and possibly stop the attack before it is executed. This is done by creating a buffer zone between the publicly accessible areas and the vital areas of the facility by means of an obstacle course, a serpentine path, or a division of functions within the facility. Alternatively, through effective design, the attacker could be enticed to a noncritical part of the facility, thereby delaying the attack.

- **Mitigating the effects of the attack.** If these precautions are implemented and the attack still takes place, structural protection efforts will serve to control the extent and consequences of damage. In the context of the overall security provided to the building, structural protection is a last resort that only becomes effective after all other efforts to stop the attack have failed. In the event of an attack, the benefits of enhancements to life-safety systems may be realized in lives saved.

The goal of the assessment process is to achieve the level of protection sought through implementation of mitigation measures in the building design. These measures may reduce risk by deterring, detecting, denying, or devaluing the potential threat element prior to or during execution of an enemy attack. The Department of Homeland Security uses the following methodology to achieve this purpose.

- **Deter:** The process of making the target inaccessible or difficult to defeat with the weapon or tactic selected. It is usually accomplished at the site perimeter using highly visible electronic security systems, fencing, barriers, lighting, and security personnel and in the building by securing access with locks and electronic monitoring devices.
• Detect: The process of using intelligence sharing and security services response to monitor and identify the threat before it penetrates the site perimeter or building access points.

• Deny: The process of minimizing or delaying the degree of site or building infrastructure damage or loss of life or protecting assets by designing or using infrastructure and equipment designed to withstand blast and chemical, biological, or radiological effects.

• Devalue: The process of making the site or building of little to no value or consequence, from the terrorists’ perspective, such that an attack on the facility would not yield their desired result.

[Note: This is a variation of the traditional “deter-detect-delay-deny-and-respond (or defend)” methodology for applying mitigation measures.]

### Reviewing Mitigation Options

At this point, after having identified a preliminary list of mitigation options ... they should be analyzed further in order to select those that are more feasible to be implemented. The selected criteria include the following:

- **Available political support.** Political support involves examining the proposed mitigation options by seeking the opinions of local and state elected officials, as well as the community as a whole. Most communities have learned that success of mitigation efforts hinges on political- and community-wide support. Building an effective political constituency for implementation of mitigation measures in most cases requires time and patience. However, some mitigation options will garner such support more easily than others.

- **Community acceptance.** Community acceptance cannot be viewed separately from the need for political support for the proposed mitigation options. Both are necessary preconditions for their successful implementation. In many cases, community-wide campaigns are necessary to explain the risks, the reasons for, and the expected benefits from the proposed measures.

- **Cost.** Although the implementation of mitigation measures hinges on political commitment and technical capacity, it also depends heavily on the costs involved. After identifying the preliminary mitigation measures, one will have some idea of the cost involved and opportunities for implementation.

- **Benefit.** When implementing a mitigation measure, it is important to consider that the benefit of implementing the option outweighs the cost. After identifying the mitigation measures, one will have some idea of the benefits that may result from implementing the mitigation measures.

- **Available financial resources.** [I]t is important to have some knowledge of the available resources for implementing mitigation options. The team should discuss this issue with the site and building owners because the amount of financial resources may define the type of mitigation options to be adopted. The team should also discuss any federal and state programs available for financing large-scale mitigation measures.
Legal authority. Without the appropriate legal authority, a mitigation action cannot lawfully be undertaken. One will need to determine whether the building owner has the legal authority to implement the selected mitigation options or whether it is necessary to wait for new laws or regulations. For example, creating stand-off distances in urban areas can be against zoning ordinances and building set-back requirements.

Adversely affected population. While implementing the mitigation measures to solve problems related to blast and CBR resistance, one may want to consider that some segments of the population may be adversely affected. For example, the construction of barriers and bollards can inhibit the number of tourists visiting a particular city and might affect the community and the hospitality sector.

Adverse effects on the already built environment. Some mitigation measures may have a negative effect on the already built environment. When selecting mitigation measures, the following should be strictly scrutinized:

- Effects on traffic/vehicular mobility
- Effects on pedestrian mobility
- Effects on ingress and egress to the building
- Effects on other building operations
- Effects on aesthetics
- Potential interference with first responders

Impact on the environment. When considering mitigation options, it is important to consider whether the recommended mitigation options will have a negative effect on environmental assets.

Technical capacity. Some mitigation measures require highly skilled and specialized engineering expertise for implementation. Although experts can be hired on a short-term basis, the technical complexity of some mitigation solutions may require the expertise for long-term maintenance. It is therefore necessary to examine the technical capacities of all stakeholders and identify key technical expertise needed for each proposed mitigation option. If adequate technical capabilities are available for proposed mitigation measures, one should rank them higher on the priority list.

Funding for maintenance and operations. When considering the implementation of your mitigation options, you should be sure that funding is available for maintenance and operations.

Ease and speed of implementation. Different mitigation measures require different kinds of authority for their implementation. The team must identify public authorities and responsible agencies for implementing mitigation measures and must examine their rules and regulations. The team must identify all legislative problem areas and institutional obstacles as well as the incentives that can facilitate mitigation and implementation. The team will have to balance the desirability of the mitigation measure against the community’s rules and regulations in order to decide which takes precedence.

Timeframe and urgency. Some mitigation measures require immediate implementation due to their nature (i.e., repetitive security breaches), political desire (i.e., platform project), or social perception (i.e., recent damage and disaster) of the risk. These perceptions can be the drivers to determining the timeframe for implementation of your mitigation options.
• **Short-term solutions/benefits.** When considering your mitigation options, you may want to evaluate your short-term solutions (i.e., mitigation options that will solve a particular problem temporarily but may require additional funding in the future for follow-on projects). A short-term solution can be quickly accomplished and can demonstrate immediate progress in satisfying community needs.

• **Long-term solutions/benefits.** When considering mitigation options, one may want to evaluate long-term solutions (i.e., mitigation options that cannot be funded immediately but will solve the problem permanently in the future when funds are available). A long-term solution can be more cost-effective in the long run than a short-term one.

**Estimating Cost**

The initial construction cost of protection has two components: fixed and variable. Fixed costs include such items as security hardware and space requirements. These costs do not depend on the level of an attack (i.e., it costs the same to keep a truck away from a building regardless of whether the truck contains 500 or 5,000 pounds [227 or 2,270 kilograms] of TNT). Blast protection, on the other hand, is a variable cost. It depends on the threat level, which is a function of the explosive charge weight and the stand-off distance. Building designers have no control over the amount of explosives used but are able to change the level of protection by defining an appropriate stand-off distance, adopting hardening measures for their buildings, and providing sacrificial spaces that can be affected by terrorist attacks, but, at the same time, can protect people and critical building functions and infrastructure.

The optimal stand-off distance is determined by defining the total cost of protection as the sum of the cost of protection (construction cost) and the cost of stand-off (land cost). These two costs are considered as a function of the stand-off for a given explosive charge weight. The cost of protection is assumed to be proportional to the peak reflected pressure at the building envelope while the cost of land is proportional to the square of the stand-off distance. The optimal level of protection is the one that minimizes the sum of these costs.

If additional land is not available to move the secured perimeter farther from the building, the required floor area of the building can be distributed among additional floors. As the number of floors is increased, the footprint decreases, providing an increased stand-off distance. By balancing the increasing cost of the structure (due to the added floors) and the corresponding decrease in protection cost (due to added stand-off), it is possible to find the optimal number of floors to minimize the cost of protection.

These methods for establishing the best stand-off distance are generally used for the maximum credible explosive charge. If the cost of protection for this charge weight is not within the budgetary constraints, the design charge weight must be modified. A study can be conducted to determine the largest explosive yield and corresponding level of protection that can be incorporated into the building, given the available budget.

---

*Footprint is “the shape and orientation of the ground floor of a structure” on a site or a lot (Answers.com, Footprint (Building). 2008. <http://www.answers.com/topic/footprint-building>; September 25, 2008).*
Although it is difficult to assign costs to different upgrade measures because they vary, based on the site-specific design, some generalizations can be made (Figure 4–4). Below is a list of enhancements arranged in order from least expensive to most expensive:

- Hardening of unsecured areas
- Measures to prevent progressive collapse
- Exterior window and wall enhancements

**Life-Cycle Costs**

Life-cycle costs need to be considered as well. For example, if it is decided that two guarded entrances will be provided, one for visitors and one for employees, they may cost more during the life of the building than a single well-designed entrance serving everyone. Also, maintenance costs may need to be considered. For instance, the initial costs for a CBR detection system may be modest, but the maintenance costs are high. Finally, if the rentable square footage is reduced as a result of incorporating robustness into the building, this may have a large impact on the life-cycle costs.

**Setting Priorities**

If the costs associated with mitigating manmade hazards are too high, there are three approaches available that can be used in combination: (1) reduce the design threat, (2) reduce the level of protection, or (3) accept the risk. In some cases, the owner may decide to prioritize enhancements, based on their effectiveness in saving lives and reducing injuries. For instance, measures against progressive collapse are perhaps the most
effective actions that can be implemented to save lives and should be considered above any other upgrades. Laminated glass is perhaps the single most effective measure to reduce extensive nonfatal injuries. If the cost is still considered too great, and the risk is high because of the location or the high-profile nature of the building, then the best option may be to consider building an unobtrusive facility in a lower-risk area instead. In some cases (e.g., financial institutions with trading floors), business interruption costs are so high they outweigh all other concerns. In such a case, the most cost-effective solution may be to provide a redundant facility.

Early consideration of manmade hazards will significantly reduce the overall cost of protection and increase the inherent protection level provided to the building. If protection measures are considered as an afterthought or not considered until the design is nearly complete, the cost is likely to be greater, because more areas will need to be structurally hardened. An awareness of the threat of manmade hazards from the beginning of a project also helps the team to determine early in the process what the priorities are for the facility. For instance, if extensive teak paneling of interior areas visible from the exterior is desired by the architect for the architectural expression of the building, but the cost exceeds that of protective measures, then a decision needs to be made regarding the priorities of the project. Including protective measures as part of the discussion regarding trade-offs early in the design process often helps to clarify such issues.

Applicability of Benefit/Cost to Terrorist Threats

When prioritizing hazard mitigation alternatives, a benefit/cost analysis is generally conducted for each proposed action. A benefit/cost analysis involves calculating the costs of the mitigation measure and weighing them against the intended benefits, frequently expressed as losses avoided. However, applying benefit/cost analysis to terrorist threats can be challenging due to the following three main factors (for more information on this subject, see FEMA 386–7, Integrating Human-Caused Hazards into Mitigation Planning):

1. *The probability of an attack or frequency is not known.* The frequency factor is much more complex in the case of manmade hazards than for natural hazards. Although it is possible to estimate how often many natural disasters will occur (i.e., a structure located in the 100-year floodplain is considered to have a 1 percent chance of being flooded in any given year), it is very difficult to quantify the likelihood of a terrorist attack or technological disaster. Quantitative methods to estimate these probabilities are being developed but have not yet been refined to the point where they can be used to determine incident probability on a facility-by-facility basis. The Assessment Team may use a qualitative approach based on threat and vulnerability considerations to estimate the relative likelihood of an attack or accident rather than the precise frequency. Such an approach is necessarily subjective but can be combined with quantitative estimates of cost-effectiveness (the cost of an action compared to the value of the lives and property it saves in a worst-case scenario) to help illustrate the overall risk reduction achieved by a particular mitigation action.

2. *The deterrence rate may not be known.* The deterrence or preventive value of a measure cannot be calculated if the number of incidents it averts is not known. Deterrence in the case of terrorism may also have a secondary impact in that, after a potential target is hardened, a terrorist may turn to a less protected facility, changing the likelihood of an attack for both targets.
The life span of the action may be difficult to quantify. The life span of a mitigation action presents another problem when carrying out a benefit/cost analysis for terrorism and technological hazards. Future benefits are generally calculated for a natural hazard mitigation action in part by estimating the number of times the action will perform successfully over the course of its useful life. However, some protective actions may be damaged or destroyed in a single manmade attack or accident. For example, blast-resistant window film may have performed to 100 percent effectiveness by preventing injuries from flying glass, but it may still need replacement after one “use.” Other actions, such as a building setback, cannot be “destroyed” or “used up” per se. This is in contrast to many natural hazard mitigation actions, where the effectiveness and life span of a structural retrofit or land use policy are easily understood and their value over time is quantifiable.

Improving the Accuracy of Cost Estimates

To improve the accuracy of cost estimates consult the Building Vulnerability Assessment Checklist.

Risk Assessment Database


Reviewing Mitigation Options, Cost, and the Layers of Defense

A general spectrum of site mitigation measures ranging from the least protection, cost, and effort to the greatest protection, cost, and effort are provided in Figures 4–5 and 4–6. These mitigation measures have been arranged by layers of defense (second and third layers), following the principle that the layers of defense create a succeeding number of security layers more difficult to penetrate. The underlying purpose of this task is to provide examples of mitigation measures for each layer and give a broad idea on the potential correlation between protection and cost.

FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings (January 2005) provides the complete explanation of this risk assessment methodology and should be consulted when embarking upon such a risk assessment.
Place trash receptacles as far away from the building as possible.

- Remove any dense vegetation that may screen covert activity.
- Use thorn-bearing plant materials to create natural barriers.
- Identify all critical resources in the area (fire and police stations, hospitals, etc.).
- Identify all potentially hazardous facilities in the area (nuclear plants, chemical labs, etc.).
- Use temporary passive barriers to eliminate straight-line vehicular access to high-risk buildings.
- Use vehicles as temporary physical barriers during elevated threat conditions.
- Make proper use of signs for traffic control, building entry control, and so on. Minimize signs identifying high-risk areas.
- Introduce traffic calming techniques, including raised crosswalks, speed humps and speed tables, pavement treatments, bulbouts, and traffic circles.
- Identify, secure, and control access to all utility services to the building.
- Limit and control access to all crawl spaces, utility tunnels, and other means of under-building access to prevent the planting of explosives.
- Utilize Geographic Information Systems (GIS) to assess adjacent land use.
- Provide open space inside the fence along the perimeter.
- Locate fuel storage tanks at least 100 feet [30 meters] from all buildings.
- Block sight lines through building orientation, landscaping, screening, and landforms.
- Use temporary and procedural measures to restrict parking and increase stand-off.
- Locate and consolidate high-risk land uses in the interior of the site.
- Select and design barriers based on threat levels.
- Maintain as much stand-off distance as possible from potential vehicle bombs.
- Separate redundant utility systems.
- Conduct periodic water testing to detect waterborne contaminants.
- Enclose the perimeter of the site. Create a single controlled entrance for vehicles (entry control point).
- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed circuit television cameras.
- Mount all equipment to resist forces in any direction.
- Include security and protection measures in the calculation of land area requirements.
- Design and construct parking to provide adequate stand-off for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Do not site the building adjacent to potential threats or hazards.
- Locate critical building components away from the main entrance, vehicle circulation, parking, or maintenance area. Harden as appropriate.
- Provide a site-wide public address system and emergency call boxes at readily identified locations.
- Prohibit parking beneath or within a building.
- Design and construct access points at an angle to oncoming streets.
- Designate entry points for commercial and delivery vehicles away from high-risk areas.
- In urban areas with minimum stand-off, push the perimeter out to the edge of the sidewalk by means of bollards, planters, and other obstacles. In extreme cases, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or through street closings. For this measure, you need to work with your local officials.
- Provide intrusion detection sensors for all utility services to the building.
- Provide redundant utility systems to support security, life safety, and rescue functions.
- Conceal and/or harden incoming utility systems.
- Install active vehicle crash barriers. Ensure that exterior doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.
- Secure roof access hatches from the interior. Prevent public access to building roofs.
- Restrict access to building operation systems.
- Conduct periodic training of HVAC operations and maintenance staff.
- Evaluate HVAC control options.
- Install empty conduits for future security control equipment during initial construction or major renovation.
- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls.
- Minimize interior glazing near high-risk areas.
- Establish emergency plans, policies, and procedures.
- Establish written plans for evacuation and sheltering in place.
- Illuminate building access points.
- Restrict access to building information.
- Secure HVAC intakes and mechanical rooms.
- Limit the number of doors used for normal entry/egress.
- Lock all utility access openings.
- Provide emergency power for emergency lighting in restrooms, egress routes, and any meeting room without windows.
- Install an internal public address system.
- Stagger interior doors and offset interior and exterior doors.
- Eliminate hiding places.
- Install a second and separate telephone service.
- Install radio telemetry distributed antennas throughout the facility.
- Use a badge identification system for building access.
- Install a CCTV surveillance system.
- Install an electronic security alarm system.
- Install rapid response and isolation features into HVAC systems.
- Use interior barriers to differentiate levels of security.
- Locate utility systems away from likely areas of potential attack.
- Install call buttons at key public contact areas.
- Install emergency and normal electric equipment at different locations.
- Avoid exposed structural elements.
- Reinforce foyer walls.
- Use architectural features to deny contact with exposed primary vertical load members.
- Isolate lobbies, mailrooms, loading docks, and storage areas.
- Locate stairwells remotely. Do not discharge stairs into lobbies, parking, or loading areas.
- Elevate HVAC fresh-air intakes.
- Create “shelter-in-place” rooms or areas.
- Separate HVAC zones. Eliminate leaks and increase building air tightness.
- Install blast-resistant doors or steel doors with steel frames.
- Physically separate unsecured areas from the main building.
- Install HVAC exhausting and purging systems.
- Connect interior nonload bearing walls to structure with nonrigid connections.
- Use structural design techniques to resist progressive collapse.
- Treat exterior shear walls as primary structures.
- Orient glazing perpendicular to the primary façade facing uncontrolled vehicle approaches.
- Use reinforced concrete wall systems in lieu of masonry or curtain walls.
- Ensure active fire system is protected from single-point failure in case of a blast event.
- Install a Backup Control Center (BCC).
- Avoid eaves and overhangs or harden to withstand blast effects.
- Establish ground floor elevation 4 feet [1.2 meters] above grade.
- Avoid re-entrant corners on the building exterior.

**FIGURE 4-6 Mitigation Options for the Third Layer of Defense.**
Building Security Rating Program Promoting Logical Unified Security (PLUS™)

Guidelines such as the FEMA Risk Management Series provide invaluable information to stakeholders interested in the protection of buildings and their occupants against the threat of terrorism. In addition, there are other initiatives, such as the Building Security Rating Program-Promoting Logical Unified Security (PLUS®) produced by the Building Security Council (BSC), that assist in these endeavors.

Developed by the Applied Research Associates, Inc., under the direction of the BSC Rating System Development Committee, PLUS is “a comprehensive program that develops and maintains building physical and operational criteria to enhance the security and safety of buildings, their missions, and their life-safety services in the face of terrorist assault.”

The BSC’s Promoting Logical Unified Security (PLUS) rating program is a system that building owners and operators, as well as building designers, can use to determine their building security needs. The PLUS program used existing guidelines to design its rating program. Guidelines such as the FEMA Risk Management Series, especially FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks against Buildings, FEMA 452: Methodology for Preparing Threat Assessments for Commercial Buildings, and FEMA 430: Primer for Incorporating Building Security Components in Architectural Design were utilized to create PLUS.

When design professionals consider security in a holistic manner, such as required by the BSC rating program, they will produce better, more innovative solutions which will enhance building security. Using the PLUS program building owners and their consultants will be able to decide what to do [and] how to do it. The PLUS system will also help them determine if their efforts have been successful.

The process of obtaining a PLUS rating is very simple. Building owners will voluntarily apply for a security rating level awarded by the BSC for their buildings. The owners will submit detailed information about the design and operation of their buildings, and a set of reviewers will evaluate the submittal against standardized rating criteria. The reviewers will suggest an appropriate rating level to the BSC’s Building Evaluation Committee, and the final rating will be given. The owners will be required to pay a fee for this service.

The Building Security Certified Professional (BSCP™) certification program was created in 2006 to provide design and security professionals with a

---


credential that demonstrates a comprehensive, multidisciplinary understanding of building security issues. The certification was also designed to help the BSC support its PLUS (Promoting Logical Unified Security) ratings program by providing building owners and operators with a pool of individuals to assist them in their pursuit of a PLUS rating. Hence the BSC has created a database of individuals who have earned their BSCP on its PLUS website that building owners can reference when they pursue their PLUS rating. Ultimately, the long-term goal of the BSCP program is to integrate security into every stage of the facility life-cycle-planning, design, construction, and operation.26

Use of Consultants and Specialists

In carrying out a risk assessment, it may be advisable at times to use a consultant or specialist to conduct the assessment or to analyze specific areas of the security and fire life safety programs. The International Association of Professional Security Consultants defines a consultant as “a person who provides security advice, information, and recommendations to management.”27 A consultant or specialist is a person who, through some combination of study and experience, has acquired expertise in a particular discipline or area.

Reasons for Engaging a Consultant or Specialist

Some reasons for hiring a consultant or specialist to conduct a risk assessment or to analyze specific areas of the security and fire life safety programs are as follows:

1. The consultant or specialist is very knowledgeable in state-of-the-art security or fire life safety systems and code compliance issues and is experienced in conducting assessments of the specific areas in which objective professional advice is required. According to Aggleton,

   My area of business is analyzing client’s security needs and developing applicable solutions to their vulnerabilities, mostly in the area of security technology…. As technology gets more complex, the security directors, human resources directors, facilities directors, whoever is responsible for security, don’t keep up with the technology applications and need help to understand what is out there and how it should be applied…. In my opinion, the role of consultants is to educate them to understand what the process is, how they analyze what they need, how they get where they want. They need someone in their corner to help them do that.28

2. The consultant or specialist is already employed by the manufacturers or distributors of the security or fire life safety equipment installed or planned for

---

installation or by the contractor supplying security personnel at the building. This person may be well acquainted with the site and the issues that need to be addressed. Of course, if manufacturers or distributors of equipment, or the contract security provider, employ the consultant or specialist, there is always a concern that the person may not be completely objective and may present recommendations not specifically geared to the client’s needs.

3. At the time the assessment is needed, there may be no person within the building operation who has the expertise or time to perform the task within the required period.

4. The individuals who have the authority to implement the recommendations of an assessment have previously been made aware of what is needed but, for whatever reasons, do not want to accept the advice of the person(s) who brought these matters to their attention. Also, it may be that a particular security or fire life safety problem with several possible solutions has provoked disagreement within building management as to what is the best course of action.

5. The consultant or specialist has a well-established professional relationship with local law enforcement or the fire authority having jurisdiction, and therefore is able to achieve certain objectives that others cannot.

6. The consultant or specialist may have certain professional qualifications or certifications that would qualify him or her to be called, in the event of future litigation, as an expert witness to testify on behalf of the building owner or operator.

Issues to Consider

Those who hire a consultant or specialist to conduct the survey or to analyze specific areas of the security and fire life safety programs should adhere to the following procedures:

1. Request a résumé of the consultant or specialist and review his or her education, qualifications, professional experience, and professional affiliations. Examine any potential conflict of interest on the part of the consultant or specialist. Check client references.

---

*The term authority having jurisdiction, or AHJ, may not be specifically used in some countries. However, in the United States, it refers to “a federal, state or local entity that has statutory authority” (U.S. Department of Health and Human Services, National Head Start Training and Technical Assistance Resource Center. <http://www.hsnrc.org/Facilities/glossary.cfm>; August 8, 2008). More specifically, the NFPA Glossary of Terms (2005) National Fire Code, defines it as “the organization, office, or individual responsible for approving equipment, materials, an installation, or a procedure.” The National Fire Code further states that the “phrase ‘authority having jurisdiction’ is used in NFPA documents in a broad manner, since jurisdictions and approval agencies vary, as do their responsibilities. Where public safety is primary, the authority having jurisdiction may be a federal, state, local, or other regional department or individual such as a fire chief; fire marshal; chief of a fire prevention bureau, labor department, or health department; building official; electrical inspector; or others having statutory authority. For insurance purposes, an insurance inspection department, rating bureau, or other insurance company representative may be the authority having jurisdiction. In many circumstances, the property owner or his designated agent assumes the role of the authority having jurisdiction” (Quincy, MA: National Fire Protection Association; 2001:A-1–3).

2. Determine if the consultant or specialist has the necessary skills to carry out the project.
3. Ensure the scope of the project is clearly communicated to the consultant or specialist by the individual(s) requesting the project.
4. Direct the consultant or specialist to submit a written proposal of how the project is to be carried out, how long it is expected to take, and what form the final written report will take. This proposal should also address how costs of the project will be handled. (A total fixed cost may be proposed for the project, or hourly or daily costs quoted; in addition, transportation, accommodation, and administrative costs may be specified for separate billing. A retainer fee may be stipulated on acceptance of the proposal or commencement of the work, with additional regular payments scheduled during the project.)
5. When the terms of the agreement are accepted, draw up a written contract, including the above proposal and incidental items such as a confidentiality agreement. Once the contract is fully executed, the work should commence as outlined in the agreement.

Sources of Consultants and Specialists

A consultant or specialist may be selected from a number of sources. There are individuals and consulting firms, which specialize in providing consulting services, and professional groups\* whose members are consultants.

Law enforcement and crime prevention departments, fire prevention departments, and the local fire marshal will be most amenable to providing information and possible sources of consultants and specialists.

References for consultants or specialists may also come from the manufacturers and distributors of security and fire life safety equipment or from representatives of the contract security company providing services at the building. A careful screening process can reduce the concern that such persons may not be fully objective and totally geared to the client’s needs. Finally, personal recommendations of a consultant or a specialist may come from other security directors, fire safety directors, risk managers, building owners and managers, and insurance agents.

Summary

- Risk assessments are invaluable in helping high-rise building owners, managers, security and life safety directors, and consultants effectively and safely operate high-rise buildings and thereby reduce premises liability.
- To identify specific assets and the threats to these assets, assess vulnerabilities or weaknesses to such threats, and devise measures to counter such weaknesses, the survey is an essential tool. To conduct a thorough analysis of a facility, it is helpful that it be carried out in a methodical fashion. If the expertise for such a task does not exist on site, the selection of a professional consultant or specialist is vital.

\*Some examples are ASIS International, NFPA International, the International Association of Professional Security Consultants (IAPSC), the Building Security Council (BSC), the International Professional Security Association (IPSA), and the Security Institute.
Key Terms

All hazards. By the very nature of the term, it encompasses all hazards that can threaten an asset. See hazard and threat.

As-built drawings (sometimes called record drawings). “Construction drawings revised to show significant changes made during the construction process; usually based on marked-up prints, drawings and other data furnished by the contractor or the architect.”

Asset. “Any real or personal property, tangible or intangible, that a company or individual owns, that can be given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary information, and related property.”

Asset criticality. This refers to how critical an asset is to the operation of a building and to the life safety of people.

Asset value. “The degree of debilitating impact that would be caused by the incapacity or destruction of an asset.”

Authority having jurisdiction (AHJ). “A federal, state or local entity that has statutory authority.”

Benchmarking. A process by which the security program at a facility can be compared with the best practices that exist for similar types of facilities. “Benchmarking ... serves as a barometer for determining what works best under comparable circumstances.”

Building hardening. “Enhanced construction [hardening of physical structures beyond required building codes and standards] that reduces vulnerability to external blast and ballistic attacks.” A ballistic attack primarily involves the use of small weapons.

Building offset. An upper floor is set back from the floors beneath it. Sometimes a building offset is referred to as a building setback (or set-back). See setback.

Campus. “A site on which the buildings of an organization or institution are located.”

Countermeasure. An opposing measure to counteract a vulnerability of an asset to a threat. Sometimes called a mitigation measure.


Crime prevention through environmental design (CPTED—pronounced sep-ted). “The proper design and effective use of the built environment can lead to a reduction in the fear of crime and the incidence of crime, and to an improvement in the quality of life.”

**Floor plate.** The entire floor area of a building including the public access or common areas, tenant areas, and maintenance spaces.

**Footprint.** “The shape and orientation of the ground floor of a structure” on a site or a lot.

**Gap analysis.** “Consists of defining the present state, the desired or ‘target’ state and hence the gap between them.”

**Hazard.** “A source of potential danger or adverse condition.” “Natural hazard” typically refers to a natural event such as a flood, wind or seismic disaster. ‘Human-caused (or manmade) hazards’ are ‘technological hazards’ and ‘terrorism’ and are distinct from natural hazards primarily in that they originate from human activity. ‘Technological hazards’ (i.e., a HazMat leak from a railcar) are generally assumed to be accidental and that their consequences are unintended.” See also threat.

**Layers of defense.** “A traditional approach in security engineering and use concentric circles extending out from an area or site to the building or asset that requires protection. They can be seen as demarcation points for different security strategies.” See also security-in-depth and protection-in-depth.

**Mitigation measure.** See countermeasure.

**Penetration testing.** A process to evaluate the security status of a facility, or an aspect of its operation, by a person attempting to breach the program by exploiting any vulnerabilities or weaknesses that may exist.

**Plinth.** A “projecting base to external walls.”

**Protection-in-depth.** “The strategy of forming layers of protection is known as designing for protection-in-depth. The purpose of the protective layers is to make it progressively more difficult for an intruder to reach critical targets and to escape undetected.” See also security-in-depth and layers of defense.

**Risk.** “The possibility of loss resulting from a threat, security incident, or event.” “Risk is the potential for loss or damage to an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it.”

---

39The term crime prevention through environmental design was first used by C. Ray Jeffrey in 1971 in a book by that name and subsequently by Timothy D. Crowe (1991) in the book titled Crime Prevention Through Environmental Design. 2nd ed. Woburn, MA: Butterworth-Heinemann; 2000:1, 46. This definition is used by the National Crime Prevention Institute (NCPI), University of Louisville.


44Ibid., p. 21–2.


Risk assessment. “The process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization’s operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.”

This process “analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence.... The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with [the] identified vulnerability, allow prioritization of resources to implement mitigation measures.”

Risk management. The process of making decisions of where to minimize risks to assets and how to achieve this over time.

Security assessment. See security survey.

Security audit. A process that enables confirmation that a security program, or certain areas within it, complies with applicable standards, provides assurance that quality requirements are attained and continued, and reveals parts that can be corrected or improved.

Security master plan. The strategic plan for the protection of a facility’s assets (people, property, and information). “The ultimate goal of good strategic planning is to lay out specific long-range plan objectives and then devise short-term action plans to meet each major objective (or goal).” This plan may or may not be formally documented. Sometimes it is called the security plan or the security operations plan.

Security program. The action plan for the protection of a facility’s assets (people, property, and information).

Security survey. “A thorough physical examination of a facility and its systems and procedures, conducted to assess the current level of security, locate deficiencies, and gauge the degree of protection needed.” Also known as a security assessment.

Security-in-depth. “The proposition that multiple layers of security are better than a single protection mechanism. The layers may be technological, procedural, policy or other elements working in coordination to provide redundant and mutually supportive security measures.” See also protection-in-depth and layers of defense.

Setback (or set-back). “The distance of a structure or other feature from the property line or other feature” or the “placing of a face of a building on a line some distance to the rear of the building.” Sometimes the latter definition refers to a building

---

56 ibid.
offset where an upper floor is set back from the floors beneath it.\textsuperscript{57} See building offset.

**Signature building.** Significance of a building based on its size and height, its status, or the nature of its tenants.

**Stacking plan.** “Basically a side view of the [facility] showing the entire building, including all floors and a list of tenants inhabiting these floors.”\textsuperscript{58}

**Stand-off distance.** “A distance maintained between a building or portion thereof and the potential location for an explosive detonation or other threat.”\textsuperscript{59}

**Threat.** “Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.”\textsuperscript{60} See also hazard.

**Threat rating.** “Deals with the likelihood or probability of the threat occurring and the consequences of its occurrence.”\textsuperscript{61}

**Threat assessment.** The process “wherein the threat or hazard is identified, defined, and quantified.”\textsuperscript{62}

**Vulnerability.** Any weakness that can make an asset susceptible to loss or damage.\textsuperscript{63}

**Vulnerability assessment.** “Evaluates the potential vulnerability of the critical assets against a broad range of identified threats/hazards.”\textsuperscript{64}

### Additional Reading


\textsuperscript{60} ibid., p. B–37.


\textsuperscript{62} ibid., p. ii.


Building Security Systems and Equipment

High-rise buildings have many types of security systems and equipment that can be deployed as potential solutions to address specific vulnerabilities. Their purpose is to help ensure that a building is safe to use and that protection is provided “for materials, equipment, information, personnel, physical facilities, and preventing influences that are undesirable, unauthorized, or detrimental to the goals of the particular organization being secured.”¹ This chapter describes security systems and equipment commonly found in many high-rise buildings.

Monitoring of Security Systems

The focal point for the monitoring of the security operations and communications for a building may be local annunciator and control panels built into an open-style desk arrangement in the main lobby, or a more complex and sophisticated security command center housed in a separate room (Figure 5–1). There are two obvious drawbacks to the former system. First, the security staff monitoring the equipment may also be required to monitor passing pedestrian traffic and assist people with inquiries and service requests. This additional activity can erode the effectiveness in monitoring annunciator and control panels. Second, the placement of the building security systems and equipment out in the open somewhat compromises security and makes it more susceptible to interference and (in a highly unusual but nonetheless possible) direct attack. Equipment may need to be housed in an open-style arrangement because there may not be enough activity to justify a security command center, or budgetary constraints may not support extra security personnel to staff a security command center and also meet the needs of the lobby itself. If the security command center is located in a separate room, access to it should be controlled at all times, and it should not be used for any purpose other than that for which it is designed.

The security command center often contains the following equipment:

- Building and elevator keys
- Systems for remote locking and unlocking of emergency exit stairwell doors when doors are locked from the stairwell side, roller shutter doors and gates, and so on
- Control systems for card access and biometric readers

Telephones, personal data assistants, portable two-way radio systems, public address (PA) systems, megaphones, intercom systems, and speaker systems

- Monitoring and recording systems for closed-circuit television video (CCTV)
- Monitoring and control systems for intrusion detection systems
- Key control systems
- Monitoring systems of fire detection, sprinkler control valve and water flow alarm devices, and other fire protection equipment (as discussed in Chapter 6)
- Monitoring and control systems for elevators (also discussed in Chapter 6)
- Controls for building lighting systems
- Operator terminals and printers for security and fire life safety systems and equipment

Some facilities permit commercial televisions to be displayed in the security command center. This permits the security department to be informed of news-breaking events, particularly those that may impact the building or the surrounding community. Either the television remains on at all times, or can be switched on when an incident has occurred or is expected.

All security systems should have met minimum standards required by the local authorities or are commonly accepted by the industry. “If standards do not exist or existing standards are inadequate or inappropriate, new standards should be considered.”

Before examining property control systems, intrusion detection systems, duress alarms, security mirrors, lighting systems, communication systems, closed-circuit television video systems, and patrol management devices, it is appropriate to review the types of physical barriers, locks, and locking systems that may be found in high-rise buildings.

---

Physical Barriers and Perimeter Control

A barrier is “a natural or man-made obstacle to the movement of persons, animals, vehicles, or materials.” A security barrier is an obstruction designed to deter, detect, delay, and deny movement of persons, animals, vehicles, or materials into and out of an area. It can assist in channeling the movement of such items through a secured location. It may also obstruct audio or visual surveillance of an area. Barriers commonly associated with high-rise buildings are described in the following sections.

Perimeter Landscaping, Walls, Fences, Sidewalks, and Pathways

All perimeter landscaping—including plants, trees, shrubs, ditches, and berms—should be chosen, located, and maintained so that it does not provide any concealing cover for surprise attacks on persons, cannot be used to gain entry to upper levels (such as promenades, walkways, etc.), and does not obstruct lines of sight, lighting, CCTV, or intrusion detection systems. Earth berms, in conjunction with lights, may also be useful to silhouette an intruder moving over them.

Walls may be of masonry construction using materials such as brick, stone (for example, granite, marble, travertine, or limestone), concrete block, or glass brick. They may also be covered with tiles made of ceramic (with a hard glaze finish), marble, granite, slate, or glass. Some masonry walls, particularly concrete ones, are strengthened with steel bars (commonly known as rebar). Walls should be of sufficient height to discourage people from climbing over them and may be topped, in areas where it is deemed fitting, with materials to prevent scaling of the wall. To deter graffiti, climbing ivy or prickly or thorny plants—cactus, boxwood, bougainvillea, quince, locust, or natal plum—can be planted at the base of the wall.

Fences may be constructed using wrought iron, steel, or aluminum. (Metal or aluminum chain link, expanded metal and welded wire fabric, barbed wire, barbed tape, and vinyl fences are usually not appropriate in the urban high-rise environment; however, architecturally designed wooden fences and fence cabling systems may be appropriate.) The type of fence, its style, its spacing between vertical bars or rods, its fence top (either a top rail covering the tops of vertical bars or rods, or bars or rods located above the top rail and sometimes having pointed tops), its strength, and its height will be determined by its intended use. Some fences are constructed with a concrete base (Figure 5–2).


• A berm is a mound of earth usually covered in grass.

• Masonry is the building of structures from individual units laid in and bound together by mortar, and the term ‘masonry’ can also refer to the units themselves” (Masonry. Wikipedia. <http://en.wikipedia.org/wiki/Masonry>; October 22, 2008).

• A rebar, or reinforcing bar, is a common steel bar, and is commonly used in reinforced concrete and reinforced masonry structures. It is usually formed from carbon steel, and is given ridges for better mechanical anchoring into the concrete. It can also be described as reinforcement or reinforcing steel. In Australia it is colloquially known as reo” (Rebar. Wikipedia. October 15, 2008. <http://en.wikipedia.org/wiki/Rebar>; October 22, 2008).

• “It is generally accepted that ‘wrought’ means any metal that is hammered, twisted or bent into shape, as compared to ‘cast’ which is poured at a foundry” (Daniel T. Clearing the Confusion Over Wrought Iron. May 3, 1997. <www.artmetal.com/project/NOMMA/WROUGHT.HTM>; June 7, 2008).
Whatever the type of wall or fence, it should be constructed with as few openings as possible. For vehicles, the opening and closing of these openings may be manual or automatic using a variety of methods that include a parking attendant, a valet, or a security person using a remote control device or a key switch; a ticket dispenser (recording date and time on the ticket) at the entrance (and sometimes a pay-on-exit machine); an electronic card reader reading the vehicle occupant’s card; an alphanumeric key pad; a vehicle detector embedded in the roadway; or a vehicle identification system such as a transponder. Similarly for pedestrians, the opening and closing of these openings (which may vary from a simple gate or door to a full-height security turnstile) may be manual or automatic using a variety of methods that include security personnel, an electronic card reader, or an alphanumeric key pad.

Because high-rise buildings usually are located in urban areas where real estate is at a premium, there may be little exterior landscaping, and the perimeter boundary may actually be the walls of the building itself. Pedestrian sidewalks and pathways should be well lighted and provide the most direct access possible to the building.

Fountains, Reflecting Pools, Sculpture, Boulders, Stairs, Concrete Planters, Concrete Barricades, Reinforced Light Poles, Bollards, Benches, Bus Shelters, and Rubbish Bins

Streetscape security elements such as fountains, reflecting pools, large pieces of sculpture, sizable boulders, stairs, concrete planters, concrete barricades, reinforced light poles, bollards, reinforced and anchored benches, bus shelters, and trash/rubbish/litter bins* (Figure 5–3) strategically placed near a building can be used to deny vehicle access

---

*For trash/rubbish/litter receptacles situated in high-traffic public/common areas, due to the concern that improvised explosive devices may be placed in them, some buildings use only bomb- or blast-resistant containers that can withstand an explosion, or these receptacles (along with post boxes) have been completely removed from use in such locations.
to the building and maintain a spatial separation—commonly referred to as stand-off distance—of vehicles (particularly car bombs and explosive-laden trucks) from the building’s structure (Figure 5-4).

**Planters**

Large, heavy planters made of glass-fiber reinforced concrete and strengthened with rebar, placed about three feet (0.9 meters) apart (so that the opening between them is less than the width of a standard vehicle frame) and anchored to the ground, can provide an effective passive or immobile barrier. In some applications, one or more of the planters is designed in a manner that if special access is required, the planter can be temporarily moved aside using a heavy-duty mechanical platform.

---

*The effectiveness of a truck or a car bomb explosion largely depends on the position of the vehicle at the time of the explosion, the type and amount of explosives being used, and the ability of the building itself to withstand such an explosion.*
Concrete Barriers
Concrete barriers, commonly called Jersey barriers or K-rails, originally used to separate traffic lanes on highways, are about three feet (0.9 meters) high and made of poured concrete. They are usually not rated as to the size and speed of the vehicle they can stop. However, interlocking and anchoring them to the ground can increase their stopping. These types of barriers do not fit with the architectural style of high-rise buildings and are usually only temporary until permanent properly designed, aesthetically pleasing barriers can be selected.

Bollards
A bollard (Figure 5–5) is a cylindrical post firmly anchored to the ground and usually constructed of heavy steel. Bollards can be fixed in position or hydraulically or pneumatically raised or lowered as needed (the latter commonly are called pop-up or retractable bollards). For many existing buildings, the use of bollards as a barrier to reduce the impact of vehicle-borne improvised explosive devices (VBIEDs) is impracticable due to the lack of available space at the building perimeter.

FIGURE 5–5 A series of two-foot high, aesthetically pleasing bollards that provide an effective physical barrier to vehicles. These bollards can be blended with a building’s architecture by using ornamental steel trim attached directly to the bollard or cast sleeves of aluminum, iron, or bronze, which slip over the crash tube. Courtesy of Delta Scientific Corporation (www.deltascientific.com).

---

When selecting a vehicle barrier it is critical that “the security manager estimate the likely size and weight of an attack vehicle and the maximum speed that vehicle could achieve on the streets” leading to the building. [Also], the security manager should ask to see the vehicle barrier crash certification, which should list the model of the barrier, the weight and speed of the vehicle it stopped, and the federal agency that supervised the [crash] test. 5

For many high-rises located in major urban centers, the use of barriers is impracticable or ineffective against mitigating the impact of vehicle explosions due to the lack of available space at the site perimeter for their positioning. However, properly designed barriers can prevent a vehicle from crashing into a building.

Antiskateboard Barriers
Tamper-free metal brackets, decorative objects (Figure 5–6), and rubber strips can be installed on smooth concrete and wooden surfaces to deter people using skateboards, roller skates, and similar devices.

Parking Controllers and Barriers
A vehicle height restrictor hinged top bar at the point of vehicle entry to parking garages will help restrict the type of vehicles entering. The height at which the bar is positioned will depend on the type of vehicles permitted to enter. Commonly, the height restriction is approximately 6-1/2 feet (1.98 meters) to 7 feet (2.1 meters). Most buildings have such bars, with the height restrictions displayed on them, to warn drivers of oversized vehicles before they enter and cause damage to the vehicle and possibly the overhead structure itself.

Many parking garages and parking lots use a horizontal wood, aluminum, or plastic gate arm or gate boom to control vehicle entrances and exits (see Figure 5–8, presented later, which depicts a raised horizontal gate arm). The opening and closing of these barriers may be manual or automatic using a variety of methods that include a parking attendant, a valet, or a security person using a remote control device or a key.

---


*If possible, straight, level sections where an approaching vehicle could build up speed should be reconfigured or obstacles placed on them in a serpentine pattern to force the vehicle to slow down.
switch; a ticket dispenser (recording date and time on the ticket) at the entrance (and sometimes a pay-on-exit machine); an electronic card reader reading the vehicle occupant's card; an alphanumeric key pad; a vehicle detector embedded in the roadway; or a vehicle identification system such as a transponder. Such parking gate arms are usually not designed to physically stop vehicles (unless a steel or aluminum heavy-duty, crash-rated gate arm or gate boom is used).

For higher security applications, particularly at the entry to under-building parking garages and loading docks of high-rise buildings, crash-rated steel barricades (Figure 5–7) can be mounted either on a level driveway or a ramp. These barriers can control the flow of traffic of authorized vehicles and also have the capacity in emergency situations to stop and disable a fast-moving vehicle attempting to crash through the entrance. The raising and lowering of the barricade can be controlled manually or automatically by a variety of methods including a remote control device, a key switch, an alphanumeric key pad, a radio control device, an electronic card reader reading the vehicle occupant's card, a vehicle identification system such as a transponder, or a velocity sensing device.

*These barriers can either be those that are set in the ground and designed to spring up when activated or those that remain fully raised and drop down when an authorized vehicle is to enter. The advantage of the former is that because they are out of sight when not in use, they are more aesthetically pleasing (True T. Raising the ramparts. Security Management. Alexandria, VA; October 1996:51, 52).
(that senses an approaching high speed vehicle and can trigger an alarm or activate the barricade).

A word of caution about the use of such barricades is that sometimes operating staff can make mistakes and damage vehicles. “In high traffic cycle operations, [staff] can make errors by pushing controls at the wrong time, lifting authorized vehicles. If vehicle-sensing loops are placed in the roadway directly in front and behind the barricade, the coupled loop detector will suppress accidental operation. The [staff] still have complete control using the emergency mode, which overrides the safety loop.”

“Training of operating personnel is strongly recommended. In addition to general training of these employees, at least two key people should be trained in all aspects of the system so that if something irregular or unusual happens, the [building] has personnel that can help. For instance, the [building] may have a major power outage and might require that the barriers be operated manually during this situation.”

Guard Houses and Guard Booths

Guard houses and guard booths—sometimes referred to as guard shacks or security booths—are structures used to house security personnel and security equipment in a variety of places, including the entrances to parking structures and parking lots (Figure 5–8) and loading dock/shipping and receiving areas, where pedestrian and vehicular traffic are

---


monitored and controlled. Typically they are constructed with a steel frame and insulated wall panels and roof. Equipped with electrical power, they should provide comfort and protection in all weather conditions.

“To facilitate communication with visitors, for instance sliding windows and doors can be included. Transaction drawers, cabinets, bullet-resistant glass, roof overhangs, locks, restroom facilities, electrical outlets, various HVAC [heating, ventilation, and air-conditioning] options, and floor construction are other considerations.” They may also be equipped with a duress or panic alarm. These buildings are similar to parking booths, cashier booths, and ticket booths.

Right to Pass Signs or Plates

Various types of signs can be used at a facility’s perimeter, particularly at its entrance and exit points. “Controls at this layer are generally designed to define the property line and channel people and vehicles through designated and defined access points. Intruders or casual trespassers will notice these property definitions and may decide not to proceed to avoid trespassing charges.” Often buildings, particularly those located in urban areas, have sidewalk plates located outside the building, which state the following:

“RIGHT TO PASS BY PERMISSION, AND SUBJECT TO CONTROL, OF OWNERS” or “PERMISSION TO PASS REVOCABLE AT ANY TIME.”

Some may also include a reference to the code that states this lawful right (Figure 5–9).

Also, within a building there may be various types of signs that provide information about important security policies and procedures. For example, sometimes a sign is posted in office building lobbies that states, “From 6:00 p.m. to 6:00 a.m., Monday to Friday, and on weekends and holidays, all persons entering the building must sign in at the main lobby desk.”

Building Envelope

The building envelope is “the separation between the interior and the exterior environments of a building. It serves as the outer shell to protect the indoor environment as well as to facilitate its climate control.... The physical components of the envelope include

---

Chapter 5 • Building Security Systems and Equipment

the foundation, roof, walls, doors and windows. The dimensions, performance and compatibility of materials, fabrication process and details, their connections and interactions are the main factors that determine the effectiveness and durability of the building enclosure system.”\(^{10}\)

**Building Exterior Walls and Roof**

The building’s exterior walls should be of sufficient strength to make unauthorized entry difficult. Walls at least eight inches (0.2 meters) thick are difficult to penetrate using hand tools. However, hand tools in conjunction with small amounts of explosives can be used to penetrate them.\(^*\)

The roofs of high-rises vary due to the design and construction of the building itself. The roof is the site of building utilities and mechanical areas that may include cooling towers, air-intake or air-vent openings, elevator machine rooms, window-washing staging equipment, and telecommunications equipment, such as antenna farms. Also, there are one or more fire doors leading to the building’s emergency exit stairwell(s).

Due to height, the roof is usually not considered an easy point of access. However, the presence of a helipad or heliport (Figure 5–10) does make it vulnerable. Openings and maintenance “accessways should be strengthened to the degree of being as penetration-resistant as the rest of the roof.”\(^{11}\)

Openings in the building’s exterior permit ingress and egress of pedestrians to lobbies and utility and delivery vehicles to loading dock areas. If there is a parking structure, openings are provided for vehicles to enter and leave. In addition, there may be open roof tops and openings in exterior walls of the parking garage for providing natural light and ventilation; underground common-use tunnels, cable tunnels and conduits for conveying electrical power, water, gas, and telecommunications; and drains or sewers leading away from the building. Such openings, including doors and windows, should be properly secured.

**Fire Escapes**

Many older high-rise buildings have fire escapes attached to the exterior of the building. The exterior stairways are usually made of steel. Some older retrofitted buildings have both interior stairwells and exterior fire escapes. “If in good condition they can be very useful, not only in evacuating occupants but also for fire department access [for fire fighting and rescue operations]. Fire escapes can be hazardous too.”\(^{12}\) “Fire escapes are poor substitutes for interior stairs, and their structural integrity is sometimes questionable,


\(^*\)Structural design features, such as explosion resistance and blast deflection, traditionally are not incorporated into commercial buildings. However, such counterterrorism features and the reinforcing of building structural members (including, for example, critical support columns exposed in areas such as loading docks and shipping and receiving areas) have received more attention in the United States since the 1995 Oklahoma City and the 1993 and 2001 World Trade Center incidents.


especially when large numbers of people are using the fire escape. However, when properly maintained, they are the closest thing to an interior stairway.\textsuperscript{13} Because they are made of steel and are exposed to the outside elements, they are susceptible to rust and corrosion.

**Doors**

Several types of exterior doors are associated with high-rise buildings; these include lobby doors and stairwell exterior fire doors.

**Lobby Doors**

These doors are single or double and can be constructed of tempered plate glass or stronger burglar-resistant glass or polycarbonate glazing material. The glass often is secured in aluminum, stainless steel, or other metal framework. Such doors are designed to swing out and are fitted with a door closer.\textsuperscript{•}

In some high-rises, security revolving doors (Figure 5–11) regulate the flow of pedestrian traffic in and out of building lobbies without exposing the building to the outside elements. “A revolving door is the only building entrance that can be always open and always closed.”\textsuperscript{14} Each of these doors has several wings that separate the door into compartments.


\textsuperscript{•}In the United States, the Americans with Disabilities Act (ADA) requires these doors to be operable by a disabled person in a single effort, with no grasping motion; this requirement can be met by the provision of a low-energy powered door opener such as a push button or push plate switch or by fully automatic operation with doors activated by motion detectors on the door transom or header bar or by floor pressure pads or mats. For other pedestrians, the door can open manually from the outside or inside.

Some systems only permit one person at a time to occupy a single door section. “In a properly designed security door system, when the door sensors detect two persons in the same section, at the same time, the door stops then slowly reverses automatically to back the two individuals out of the door. This is referred to as ‘anti-piggybacking.’ A security revolving door also prevents passage of unauthorized persons who attempt to get a ‘free ride’ in the opposite or adjacent section to the authorized user. Once again, system sensors will detect inappropriate use, stop the door and slowly reverse, backing both people out of the entrance. This feature is referred to as ‘anti-tailgating.’”

The door can be activated using a push button start, an overhead motion detector to automatically operate the door, or a door’s control system can be interfaced with an access control system such as a card reader mounted on the exterior. Such doors are excellent for controlling access, particularly when no security staff is present.

Modern security revolving doors are designed so that in the event of a fire alarm or power failure, the door wings will automatically collapse to a book-fold position so

---

*Other revolving doors, particularly those serving as the main entrance portal for hotels, accommodate multiple persons in each compartment.


**It is critical that a door’s sensors are calibrated according to the manufacturer’s specifications. By so doing, the risk of serious accidents, particularly those involving young children, can be mitigated.
as to provide two unobstructed lanes for occupants to exit and responding emergency personnel to enter the building (for older generation revolving doors, during an emergency, the doors have to be manually collapsed to enable straight-through access). With revolving doors, many codes require an adjacent side-hinge swinging door (Figure 5–12) to be provided.

Stairwell Exterior Fire Doors
These doors can be single (Figure 5–13) or double. They are of solid-core construction, often with heavy-gauge sheet metal or steel plating. Door hinges should be designed so that they are not accessible from the outside; however, if they are accessible, the hinges themselves should be of heavy-duty construction to resist destruction, and hinge pins should be made unremovable by being welded or flanged. “Regardless of how the pin is protected, if the knuckle [the part of the hinge that holds the hinge pin] is exposed on the outside, it is generally possible to saw off or otherwise remove and/or destroy the assembly and thus gain entry by prying open the door from the hinge side.”¹⁶ This statement provides a compelling reason for never exposing door hinges in buildings, and its originators suggest

a possible countermeasure to this vulnerability. This involves the use of a piano hinge that consists of a continuously interlocking hinge system running the full length of the door.

The actual frame in which a door is mounted should be secured to the wall in such a fashion that it resists penetration to at least the same degree as the door itself. Figure 5–14 shows common attack methods on doors and frames. A small metal plate firmly attached to the front of a door can help protect from sawing of the bolt with a hacksaw.

**Vehicle Openings**

Overhead gates protecting vehicle openings to parking structures tend to be corrugated steel shutters or metal, open-grille roller gates. This is because these openings are usually too large to accommodate a sliding gate. (Open-grille gates, as in Figure 5–15, may suit exterior openings because they can be seen through. They also allow ventilation of vehicle exhaust fumes and, in the case of a fire, smoke, and other products of combustion to escape.) After normal operating hours, when the parking structure is closed, these gates may be raised and lowered:

- Automatically using an electric motor to raise the gates when activated by an alphanumeric key pad, a radio control device, an electronic card reader reading the vehicle occupant’s card, a vehicle presence detector embedded in the roadway,\* or a vehicle identification system such as a transponder

\*Allowing any vehicle to automatically enter in this manner is not a sound security measure.
FIGURE 5–14 Common attack methods on doors and doorframes. Reprinted courtesy of the National Crime Prevention Institute, School of Justice Administration, University of Louisville, from The Use of Locks by Edgar et al. (Boston, Butterworth-Heinemann, 1987, pp. 72–76).
• Remotely from another location (often in conjunction with a CCTV system so that the gate operator can remotely observe the gate area)
• Manually using a chain or an electric motor

Another physical barrier to protect openings for vehicles consists of rotating steel wedges installed in the ground across vehicle exits. This barrier can be driven over safely when a vehicle is exiting a parking area, but it will cause severe tire damage if a vehicle attempts to reverse direction or drive in through an exit.

Another barrier, already addressed in the previous section (Figure 5–7), is a crash-rated steel barricade that can be mounted either on a level driveway or a ramp. Such a barrier can also be deployed to stop the unauthorized exiting of vehicles from a parking garage and parking lot (for example, in a residential parking garage where high-value vehicles are parked).

Within multi-level parking structures, roller steel shutters (Figure 5–16) are used as fire barriers.* Each door is equipped with a fusible link in the chain used to hold the door open. During a fire, the fusible link is designed to melt at a predetermined temperature, causing the door to automatically descend, thereby limiting the spread of fire and restricting the movement of smoke.

* A fire barrier is “a continuous vertical or horizontal construction assembly designed and constructed to limit the spread of heat and fire and to restrict the movement of smoke…. A continuous membrane, either vertical or horizontal, such as a wall or floor assembly that is designed and constructed with a specified fire resistance rating to limit the spread of fire and that also will restrict the movement of smoke. Such barriers might have protected openings” (NFPA Glossary of Terms, National Fire Code. Quincy, MA: National Fire Protection Association; 2005).
Openings for Ventilation, Natural Light, Utilities, Drains and Sewers, and Outdoor Air Intakes

Openings for ventilation and natural light; underground common-use tunnels, cable tunnels, and conduits for conveying electrical power, water, gas, and telecommunications; and drains or sewers leading away from the building may be physically protected using materials such as chain-link fabric, welded wire fabric, expanded metal, barbed wire, razor ribbon, metal grates, metal louvers, metal grilles, metal covers, steel bars, or steel rods.

Openings for outdoor air intakes and ducts for the heating, ventilation, and air-conditioning (HVAC) systems and air handling units require special attention. Figure 5–17 shows ways to enclose vulnerable outdoor air intakes.

Windows and Glazing Protection

Windows

Windows in modern high-rise buildings are either permanently fixed in place or can be opened. The different types of glass are annealed, tempered, wired, or laminated glass.

*Also, security measures such as intrusion detection devices, security personnel, and CCTV can be used to detect security breaches.

**A measure that is sometimes overlooked but important for the safety of glass panels found in buildings is the placement of window decals on the glass—usually at eye level—to visually warn persons that a glass panel is present. In addition, sometimes building operators will place sizable objects (such as a piece of sculpture, a planter, or a piece of furniture) in front of the panel to reduce the chance of a person inadvertently walking into it.
Annealed Glass

“Regular polished plate, float, sheet, rolled, and some patterned surface glasses are examples of annealed glass.” 17 “Annealed glass breaks into large, jagged shards that can cause serious injury and thus, the reason it is considered a hazard in architectural applications.” 18

Tempered Glass

Tempered glass has “a greater resistance to explosions than annealed glass.” 19 If a tempered glass window breaks, it separates into small shards or pieces of glass without sharp edges. Building codes require tempered glass at the lobby level for the safety of persons if the glass should break and on upper floors for the purpose of mechanical smoke ventilation (when a nonopening window is broken out; as shown in Figure 5–18, such windows are usually identified with an identifying “Tempered” decal*). This alleviates the danger of large sharp pieces of glass dropping from the upper floors and seriously injuring people below or cutting exterior fire hoses during a fire situation. The use of tempered glass also reduces the risk of injuries from broken glass during a major earthquake, storms, tornadoes, windblown debris, vandalism, and explosions. Blast-resistant windows can be made of tempered glass.

---


* For example, in Los Angeles high-rise buildings, tempered safety glass is required every 50 feet (15.2 meters) in upper-floor windows so the windows can be broken out for smoke ventilation. As noted, these windows are usually marked with an identifying “Tempered” decal (Figure 5–18) at the lower corner of the window.
Wired Glass
Wired glass is sometimes used for sidelight panels\(^{+}\) adjacent to a door and transoms\(^{**}\) above doors. “The glass, which consists of wire sandwiched between two layers of annealed glass, has a fire protection rating of 45 minutes.”\(^{20}\) It resists shattering and fragmentation on impact, but it is not aesthetically appealing. “Unfortunately, wired glass has its shortcomings. It has an industrial appearance some designers dislike, and isn’t a particularly strong material…. When broken, the wire within the glass keeps it from shattering into sharp shards, but it can still cut and cause serious injuries.”\(^{21}\)

Laminated Glass
Laminated architectural glass (laminated glass or laminated security glazing) “is constructed by bonding a tough polyvinyl butyral (PVB) plastic interlayer between two pieces of glass under heat and pressure to form a single piece.”\(^{22}\) It has considerable resistance to impact and the glass tends to hold together by adhering to the plastic interlayer when cracked or broken. “Laminated glass can reduce danger of flying or falling glass; resist penetration and forced entry; block out unwanted noise; be made in any color; and be used in a variety of applications, including protection against disaster, hurricane, earthquakes, commercial safety and security, bomb blasts, etc. In addition, some laminated glass provides ballistic protection.”\(^{23}\) Blast-resistant windows can be made of laminated security glazing. Laminated glass has “a greater resistance to explosions than annealed glass.”\(^{24}\)

---

\(^{+}\)A sidelight panel is the section immediately adjacent to a door.

\(^{**}\)The transom is the section immediately above a door.


\(^{21}\)ibid., p. 78.


\(^{23}\)ibid.

Burglar-Resistant or Bullet-Resistant Glass
Where unauthorized penetration is expected, or where added expense could be justified by an insurance premium reduction, stronger burglar-resistant glass or bullet-resistant glass (sometimes referred to as ballistic-resistant glass) might be used. Burglar-resistant glass is of laminated construction. Bullet-resistant glass is classified according to its strength to withstand various weapons and calibers of bullets. Sometimes, bullet-resistant glass is used for guard booths.

Weakness of Windows
The glass itself is often the weakest part of the window because it can be broken or a section of it removed using a glasscutter, thereby affording access to a facility.

Another weakness of window openings is that the glass itself can be removed and replaced, often with no telltale sign. Either putty or molding is removed and on replacing the glass the original molding is reused, or putty of a similar color to the adjoining windows is used. Such surreptitious removal and replacement of glass is much more difficult to achieve if the glass has been secured in grooves in the window frame using an elastic glazing compound.

In addressing the issue of windows in the protection of buildings against car-bomb attacks, Hinmann suggested,

For new buildings, minimize size and number of windows. Place larger windows facing directions which offer more protection from external threat (overlooking an internal courtyard for instance). If this is not possible, use mylar coating on the back of windows to hold glass shards together if breakage occurs. Other alternatives are to use specially designed curtains to capture glass shards, or to replace existing panels with tempered glass or laminated security glazing.

Security Window Film
Security window film—sometimes called security film, safety window film, safety film, protective film, fragment retention film, or shatter-resistant film—can be very useful when applied to windows. Synthetic materials, such as polyester film (e.g., Mylar), can be applied to plate glass. “While it does not add strength to the glass, it creates a less lethal failure mode.”

Security window film is comprised of either optically, clear, tinted or reflective layers of polyester film (from 4 mils to 15 mils thick) that can be adhered to the interior surface of existing glass. Typical film installations cover the visible portion of the interior surface of the glass all the way to the edge of the frame.

---


If the glass breaks (when subjected to earthquakes, explosions, storms, vandalism, and windblown debris, or someone breaks the window), the pieces adhere to the coating to reduce the effects of broken glass and flying glass shards.

According to Smith,

Because security window film has the ability to stretch before tearing, it can absorb a significant explosive shock. As this explosive force moves towards the glass and pushes it inward, the glass eventually cracks and breaks. However, the security film applied to the rear of the glass continues to absorb the shock wave and stretches until it reaches the point that it can no longer bear the pressure, at which time it will burst.

While strong enough to break the glass, the shock wave may not be strong enough to shear the security film. This results in glass not being broken but being held intact by the film. Not only are there reduced injuries, but there is also little damage to the property inside the building. If the shock wave is sufficient to break the glass and shear the film, often the glass collapses attached to the security film with minimal damage and injuries. In multi-story buildings, security film also may prevent glass from falling out of its frames to the street below, especially if it is anchored to the window frame.30

Security window film is inexpensive to install (as compared with installing tempered safety or laminated glass) but may require replacement. Some high-rise buildings in preparation for turbulent events, such as planned protests and demonstrations outside of their buildings, have installed security window film on windows near the ground level.

**Blast Curtains**

Blast curtains are “heavy curtains made of blast-resistant materials that could protect the occupants of a room from flying debris.”31 “This is a specially designed curtain that catches the pieces of glass while permitting the airblast pressure to pass through the curtain. The British originally developed this device to counter the IRA threat.”32

Blast curtains might also be installed to protect areas such as elevator lobbies in a building’s main lobby.

**Security Bars, Grilles, Screens, and Shutters**

Security bars, grilles, screens, and shutters can be used to protect windows and balconies.

---


31The August 1998 bombings of the American embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, killed 280 [224, according to The 9/11 Commission Report. July 2004:70] and injured more than 5,000 people. The bombs that destroyed these structures, like the one that brought down the Alfred P. Murrah building in the 1995 Oklahoma City bombing [described in Chapter 3], were of such strength that no window system would have been able to survive. However, the broken glass in adjacent buildings that injured thousands of people may not have done so had the windows in these buildings been protected by security window film” (Smith DL. Window film: the most cost-effective means to protect existing windows. Security Technology & Design. Cumming, GA; June 1999:88).

Sometimes an authority having jurisdiction will permit the installation of security bars, or so-called burglar bars, on windows. On lower floors, these bars are usually designed to prevent break-ins (or break-outs depending on the use of the area), whereas on upper floors they are primarily used as a life safety measure (for example, to prevent young children from climbing out of windows). In case of an occupant being trapped, these bars should always be equipped with a quick-release mechanism.

Metal grilles are used for security purposes on ground-floor shop windows and, when enclosing upper floor balconies, for life safety purposes.

Screens and shutters “can be either the roll-up type, with horizontal interlocking slats (usually made of aluminum or polyvinyl chloride) which roll up into a box located at the top of the window; or the accordion type, with vertical interlocking slats which slide to the sides of the window. These shutters can be operated manually, or electrically using remote controls, weather sensors, or timers.”

Screens and shutters can be used for security or life safety purposes by providing additional protection for windows.

**Balconies**

Balconies may be protected with glass walls, metal grilles, or shutters. Primarily, the purposes of such protective barriers are to prevent people from falling or jumping from upper levels of a building and to prevent objects being accidentally knocked over or thrown from the balcony. (In some structures, particularly residential buildings and possibly hotels, doors leading to balconies are designed to automatically lock during high winds and deploy sensors to notify security staff if the doors are opened.)

**Atriums**

Usually located immediately inside a building’s main entrance, an atrium (plural atria) is a large open space within a structure that is two or more floors high. Some buildings, particularly “larger-scale hotel building configurations often have atria two or three stories high and sometimes up to sixty stories high, which are often the focal point of building design. Atrium areas themselves may include several occupancies or mixed functions associated with hotel operations.”

**Building Floors, Ceilings, Interior Walls, and Interior Stairs or Stairways**

**Floors and Ceilings**

Modern high-rise buildings have concrete floors that provide a substantial barrier to unauthorized physical access upward or downward through the floor or ceiling to an adjoining floor.

**Suspended or Dropped Ceilings**

Ceilings may be constructed of noncombustible acoustical ceiling tiles that are supported in a metal grid hung on metal hangers attached to the floor above. The concealed space created above the ceiling often extends throughout an entire floor area (apart from

---

mandatory firewalls extending from a base floor slab to the floor slab of the floor above, and in restrooms and corridors where fire-rated plasterboard ceilings are used for fire protection). It can provide a possible means of ingress to a tenant area. A person might remove the ceiling tiles on one side of a wall (i.e., a nonfloor slab-to-floor slab wall), climb up into the ceiling space, crawl over the wall partition, and again remove ceiling tiles to drop down into the tenant area. There are two obvious physical measures to prevent this from happening: use floor slab-to-floor slab partition walls for all sensitive areas or, if floor slab-to-floor slab partition walls surrounding these areas do not exist, install steel bars or rods above the partition walls to deter unauthorized entry. Further, intrusion detection devices may be installed to signal possible intrusions.

The concealed space could also be used to hide unauthorized listening or viewing equipment such as microphones or cameras. The central heating, ventilation, and air-conditioning (HVAC) duct systems also provide a similar means for unauthorized listening and viewing. Countermeasures—steel bars or rods and intrusion detection devices, or providing a separate, stand-alone HVAC system for sensitive areas—are possible solutions to this potential security problem.

### Raised Floors

Previously only found in computer data centers where underfloor power and data cabling is run, some modern office buildings have raised floors which house electrical, plumbing, and air-conditioning systems, as well as cables, telephone wiring conduits, and computer wiring. Raised floors are particularly useful for underfloor air-conditioning. Of course, this concealed space could also be used to hide unauthorized listening or viewing equipment such as microphones or cameras. Periodically checking these areas may detect such devices.

### Interior Walls

Interior walls can be constructed of lath and plaster or prefabricated sheets of material such as fire-rated drywall, plasterboard, plywood, or wooden paneling attached to wooden or metal studs.

### Interior Stairs or Stairways

Stairs are “a series of steps leading from one level of floor to another, or leading to platforms, pits, boiler rooms, crossovers, or around machinery tanks and other equipment... A series of steps and landing having three or more rises constitutes stairs or [a] stairway.”

In high-rise buildings, stairs may be found in mechanical areas; also, interior stairways or staircases are sometimes installed for access between floors of a multifloor tenant. Depending on the security needs of the tenant, the free access that these stairways afford may need to be controlled.

### Building Interior Doors

**Doors to Offices, Hotel Rooms, Residences and Apartments, and Interior Areas**

Doors leading to offices, hotel rooms, residences and apartments, and other interior areas, can be single or double. Perimeter doors to these areas, and inner doors, are usually

---

constructed of solid-core materials (of course, by code any fire doors must be of solid-core construction), although some doors are made of glass (in particular, many office entrance doors leading from passenger elevator lobbies and conference rooms have glass doors and possibly a glass wall that affords visibility).

Doors to sensitive areas, depending on the degree of physical security needed, may have heavy-gauge sheet metal or steel plating.

Door hinge and frame construction requirements are the same as that discussed earlier in the “Stairwell Exterior Fire Doors” section.

**Door Viewer**

Some opaque doors in high-rise buildings may be equipped with a conventional door viewer (sometimes called a peephole or view port) to provide a view of the area exterior to the door.

The selection of a specific model viewer will vary depending on the security or safety reason for installing such a device. From a security standpoint, a door viewer allows one to see the person requesting entry before the access is granted or denied. For safety reasons, the person about to exit a door that swings out into a public corridor may use the door viewer. Doing so reduces the chance of the door swinging out and hitting a passerby. In addition, door viewers are installed on conference room doors to allow a person to see in to the room. This helps prevent unnecessary interruptions during meetings. The advent of electronic viewers provides an opportunity for significant extension of the potential security, safety, and operational functions of these devices.

“Optical viewers, installed in a hole drilled through the door, are passive devices generally assembled from small diameter metallic tubes fitted with one or more optical lenses. Typically the image provided is of low resolution and limited field of view. Such devices also require that the observer position their eye in close proximity to the door surface.”

Digital or electronic door viewers (Figure 5–19) are also available. These products are video surveillance systems that eliminate optical tubes with an LCD monitor mounted on the occupant side of the door and a digital camera on the door exterior.

“Electronic viewers offer several advantages over direct viewing tubes. The size of the visual display provided by the LCD panel is many times larger and the image resolution greater than that of a tube. The image provided by digital viewers may be seen from a distance without the need to place the eye very near to the device as in conventional peepholes, a distinct advantage for the visually or physically impaired. Additionally, electronic viewers may be equipped with image storage capacity, environmental sensors and connected to building security systems.”

---

**Footnotes:**


Stairwell Doors

These single doors are of solid-core construction and made of wood, heavy-gauge sheet metal, or steel plating. They must always swing in the direction of egress travel and are required to be equipped with self-closing and self-latching devices. Because these doors constitute openings in fire barriers, they are required to have a fire protection rating to limit the spread of fire and restrict the movement of smoke. A label indicating the rating is required on both the door and the doorframe. These doors should be inspected after an area has been painted to ensure that the fire protection–rating label has not been obscured.

As for the stairwells to which these doors lead, their construction details are outlined in the laws, codes, and standards adopted by the authority having jurisdiction. These details include the following: the requirement that each floor in a high-rise has two or more stairwells (some countries only require one stairwell), exit capacity, fire resistance rating of the walls, interior finish of walls and ceilings, width of stairwell, types of stairs, tread construction, types of guards and handrails, access to the roof and ground levels, natural ventilation, mechanical ventilation, stairwell pressurization, lighting, signage, and so on. Figure 5–20 shows the inside of a typical emergency exit stairwell.

In some high-rise buildings, there are scissor stairs. These are two stairways that are located close together in the same stair shaft. “The stairways are disposed adjacent to each other in parallel vertical planes and configured in an X shape. A fire wall separates each stairway.”

Won Doors

Won doors are special accordion-style doors found in the elevator lobbies of some high-rise buildings. Normally, they are in a contracted position. On activation of a fire
alarm, the Won doors on the floor where the alarm is occurring will automatically open (expand) to enclose and protect the elevator lobby. This compartmentation of the elevator lobby assists in preventing fire and smoke from intruding into the lobby.

Doors to Maintenance Spaces

Doors leading to maintenance spaces can be single or double, of solid-core construction. They usually are made of wood, heavy-gauge sheet metal, or steel plating. (For preferred hinge and frame construction, see the “Stairwell Exterior Fire Doors” section.) These doors should be locked at all times. They should be equipped with automatic door closers and self-latching mechanisms to prevent them from being accidentally left open.

Restroom Doors

The single doors usually used as restroom doors are of solid-core construction and made of wood, heavy-gauge sheet metal, or steel plating. Doors to private restrooms situated in public access or common areas should be locked at all times. They should be equipped with automatic door closers and self-latching mechanisms to prevent them from being accidentally left open. Keys or keycards to restrooms should not provide access to any other areas.

If advice is required about doors in commercial buildings, a certified door consultant or an architectural hardware consultant should be contacted.

* A keycard is another name for an electronic access card.
Elevators; Escalators; Moving Walks; Dumbwaiters; and Rubbish, Mail, Laundry, and Linen Chutes

The operation of elevators, escalators, moving walks, dumbwaiters, and rubbish, mail, laundry, and linen chutes varies from system to system and building to building. Elevators and escalators are particularly important due to their security and safety significance. Because elevators usually provide access to all levels of a high-rise building, they are of security importance. Escalators, which are used for moving people usually to and from the ground floor main lobby area to several upper floors or to subterranean levels, are important from a safety aspect.

Elevators

Types of Elevators

The following material, with some adaptations, is extracted from Tell Me about Elevators39 and About Elevators40 by Otis Elevator Company.

Gearless Traction Electric Elevators

In 1903, the Otis Elevator Company designed gearless traction electric elevators, which today are used in buildings over 10 stories high typically operate at speeds greater than 500 feet (152 meters) per minute. (Elevators could be designed to go faster but because it may take from 10 to 12 floors to bring the car up to speed and slow it down again, it is impractical to consider this. Also, some people may not feel comfortable traveling at high speeds.)

In a gearless traction machine, six to eight lengths of wire cable, or “hoisting ropes” or “hoisting cables” as they are known in the industry, are attached to the top of the elevator and looped around the drive sheave—a wheel with a grooved rim—in special grooves. The other ends of the hoist cables are attached to a counterweight that slides up and down in the elevator hoistway on its own guiderails. With the weight of the elevator car on one end of the hoisting ropes, and the total mass of the counterweight on the other, the cables are pressed down on the grooves of the drive sheave. Thus, when the motor turns the sheave, it moves the cables with almost no slippage. Actually, the electric hoisting motor does not have to lift the full weight of the elevator car and its passengers. The weight of the car and about half its


Examples of these elevators can be found in the Empire State Building (where the elevators move at speeds of up to 1200 feet [366 meters] per minute), the John Hancock Building in Chicago (where express elevators are designed to move at speeds of up to 1800 feet [549 meters] per minute), and, before its destruction, the Twin Towers of the World Trade Center in New York City (express elevator speeds were up to 1600 feet [488 meters] per minute).
passenger load is balanced out by the counterweight, which is sliding down as the car is going up (Figure 5–21).

Safety is provided by a governing device that engages the car's brakes, should the elevator begin to fall. A powerful clamp clutches the steel governor cable, which activates two safety clamps located beneath the car. Movable steel jaws wedge themselves against the guiderails until sufficient force is exerted to bring the car to a smooth stop.

Geared Traction Electric Elevators

Geared traction elevators, which operate similarly, are designed for lower speeds varying from 38 to 152 meters (125–500 ft) per minute and for loads up to 13,600 kilograms (30,000 lb). As a result, geared systems are used for a wide range of passenger elevator, freight/service elevator, and dumbwaiter applications.

A governor is a safety device that prevents an elevator car from falling or from moving downward too fast.
Hydraulic Elevators

"Hydraulic elevators are used extensively in buildings [including parking structures] up to five or six stories high. These elevators—which can operate at speeds up to 46 meters (150 ft) per minute—do not use the large overhead hoisting machinery the way geared and gearless systems do. Instead, a typical hydraulic elevator is powered by a piston that travels inside a cylinder. An electric motor pumps oil into the cylinder to move the piston. The piston smoothly lifts the elevator cab. Electrical valves control the release of the oil for a gentle descent." 41

Machine Roomless Elevators

*Designed initially for buildings between 2 and 20 stories, this system employs a smaller sheave than conventional geared and gearless elevators. The reduced sheave size, together with a redesigned motor, allows the machine to be mounted within the hoistway itself—eliminating the need for a bulky machine room on the roof.*

Observation Elevator

*The observation elevator puts the cab on the outside of the building. Glass-walled elevator cars allow passengers to view the cityscape or the building’s atrium as they travel. By eliminating the hoistways, the observation elevator also offers owners, architects and builders valuable space-saving advantages.*

Double-Deck Elevator

*Double-deck elevators save time and space in high-occupancy buildings by mounting one car upon another. One car stops at even floors and the other stops at the odd floors.*

Freight Elevator

*These elevators [sometimes called service elevators] are specially constructed to withstand the rigors of heavy loads. [They are larger in size to handle the transport of oversized items such as furniture and equipment, and accommodate the use of gurneys* by emergency personnel responding to medical incidents within buildings (and sometimes in hotels and apartment buildings, for the transport of deceased persons from offices, hotel guest rooms, apartments and residences)].*

Configuration of Elevator Systems

**Elevator Banks**

Elevator cars in high-rise buildings are separated into banks that serve different levels such as low-rise, mid-rise, and high-rise. The number of banks will depend on the size of the building itself. For example, in the hypothetical 36-floor high-rise tower Pacific Tower Plaza, described in Chapter 4, there are 17 passenger elevators, one service/freight elevator, and three parking shuttle elevators. The configuration of the elevators is as follows:

- Low-rise bank—six elevators (numbered 1 to 6) serve floors 1 to 12
- Mid-rise bank—six elevators (numbered 7 to 12) serve floors 13 to 23

---

*A gurney is “a metal stretcher with wheeled legs, used for transporting patients”* (The Free Dictionary by Farlex, Inc. <www.thefreedictionary.com/gurney>; October 30, 2008).
High-rise bank—five elevators (numbered 13 to 17) serve floors 23 to 36
Freight/service elevator—one elevator (numbered 18) serves floors 1 to 36
Parking shuttle elevators—three elevators serve floors P3 to P1

Cross-Over Floor or Sky-Lobby
A cross-over floor, or sky-lobby, is where occupants can cross over from an express elevator to another group of elevators. In the aforementioned building, a cross-over floor is located at the 23rd floor.

As for the sky-lobby, the principle consists of a variation on the arrangement of elevators in batteries [banks], each serving a group of floors. In this case, each battery [bank] begins at the lowest level of the floors it serves. This level is reached by an express elevator directly linked to the ground floor. The sky-lobby therefore is the transfer area between an express elevator and a battery [bank] of local elevators.... The system is a requirement in the case of mixed-use buildings, where each group of floors—offices, apartments, a hotel—functions as a separate unit.42

The sky-lobby idea was conceived to address an elevator space problem in the construction of the 110-story New York World Trade Center Twin Towers.43 As described in Twin Towers by Angus Kress Gillespie,

The higher you go, the more people in the building. The more people in the building, the more elevators you need. The more elevators you have, the less floor space you have to rent. The problem was so serious that it was seen as the limiting factor, the real reason why skyscrapers seldom exceeded eighty stories.

During the planning stage, Herb Tessler, one of the staff architects, came up with an idea to solve the elevator problem. [Tessler described the concept to Malcolm Levy and then to Guy Tozzoli, the head of planning for the project.] “We could divide each tower building into three parts, or zones. For express elevators from the lobby, we will construct the biggest elevators in the world each carrying 55 passengers. Then we will stick the three local parts on top of one another. Each zone will have its own lobby. People will transfer from express to local in the second and third zones by crossing the lobby. Therefore, all the locals will sit on top of one another within a single shaft, and it will solve the problem of usable space.”

[After presenting the idea to Otis and Westinghouse elevator companies,] Herb Tessler came back and said that Otis could build elevators where the first person in was the first one out. Elevators could be built with doors on both the front and the back of the car. People could get through the front door at the lobby level, and get off through the rear door when they reached the desired floor.... It was a new thing.44

In some very tall buildings, such as the Sears Tower in Chicago, “double-deck express cabs serve the sky lobbies and single deck cabs provide intra-zone travel.”

In terms of security, the access an elevator affords to floors in a high-rise is of critical importance. Many elevators are fitted with access control systems that control the use of elevators. The types of access control systems are discussed later in this chapter.

In Chapter 6, there is a discussion of elevator safety developments and basic elevator controls.

Escalators

An escalator is just a simple variation on the conveyor belt. A pair of rotating chain loops pull a series of stairs in a constant cycle, moving a lot of people a short distance at a good speed. The escalator system isn’t nearly as good as an elevator at lifting people dozens of stories, but it is much better at moving people a short distance. This is because of the escalator’s high loading rate. Once an elevator is filled up, you have to wait for it to reach its floor and return before anybody else can get on. On an escalator, as soon as you load one person on, there’s space for another.

Escalators have certain safety features (Figure 5–22), such as emergency stop buttons, built into them.

Locks and Locking Systems

Pin Tumbler Locks

The pin tumbler lock (or mortise cylinder lock) is the type of key-operated, mechanical lock most widely used in architectural or builders (door) hardware (Figure 5–23). In office buildings and residential apartment buildings, these locks may be found on various perimeter, stairwell, and maintenance areas, and on tenant and apartment doors. For hotel guest room doors, the locks are usually keycard operated rather than key operated. This type of lock is installed by hollowing out a portion of the door along the front or leading edge and inserting the mechanism into this cavity. The security afforded by the pin tumbler mechanism ranges from fair (in certain inexpensive cylinders with wide tolerances and a minimum of tumblers) to excellent (in several makes of high-security cylinders). An irregularly shaped keyway and a key that is grooved on both sides characterize locks as manipulation and pick resistant. Pin tumbler locks can be master keyed and are extremely useful in buildings where large numbers of keys are required.

A tumbler mechanism is any lock mechanism having movable, variable elements (the tumblers) that depend on the proper key (or keys) to arrange them into a straight
line permitting the lock to operate (Figure 5–24). The pin tumbler is the lock barrier element that provides security against improper keys or manipulation. The specific key that operates the mechanism (which is called the change key) has a particular combination of cuts or bittings that match the arrangement of the tumblers in the lock. The combination of tumblers usually can be changed by inserting a new tumbler arrangement in the lock and cutting a new key to fit this changed combination. This capability provides additional security by protecting against lost or stolen keys. The different arrangements
of the tumblers permitted in a lock series are its combinations. The total possible combinations available in a specific model or type of lock depends on the number of tumblers used and the number of depth intervals or steps possible for each tumbler. Master keying greatly reduces the number of useful combinations.

Pin tumbler mechanisms vary greatly in their resistance to manipulation. Poorly constructed inexpensive cylinders with wide tolerances, a minimum number of pins, and poor pin chamber alignment may be manipulated quickly by persons of limited ability. Precision-made cylinders with close tolerances, a maximum number of pins, and

*A problem with low-security locks is called key bumping. Medeco High Security Locks states that it occurs when “a modified key is bumped with a hammer, piece of wood or any type of object to open the lock. The bump key works in a similar way to a pool cue ball hitting another ball—causing both balls to
accurate pin chamber alignment may resist picking attempts even by experts for a considerable time. (Picking a lock involves the use of metal picks to align the tumblers in the same manner as an authorized key would do, thus making it possible for the lock to operate.)

Numerous variations of the pin tumbler cylinder are on the market. The removable core cylinder (Figure 5–25) often is used in high-rise buildings. The Best Universal Lock Company, whose initial patents have now expired, originally produced it. This type of cylinder uses a special key called the control key to remove the entire pin tumbler mechanism (called the core) from the shell. This makes it possible to quickly replace one core with another having a different combination and requiring a different key to operate it.

Removable core cylinders provide only moderate security. Most systems operate on a common control key, and possession of this key will allow entry through any lock in the system. It is not difficult to have an unauthorized duplicate of the control key made. If this is not possible, any lock of the series (particularly a padlock) may be borrowed and an unauthorized control key may be made. Once the core is removed from a lock, a screwdriver or other flat tool is all that is necessary to operate the mechanism. Additionally, the added control pins increase the number of shear points in each chamber, thus increasing the mechanism’s vulnerability to manipulation.
Bolts and Strikes
Before discussing the master keying of tumbler locks, it will be helpful to our understanding of locking systems to review two parts of locking mechanisms, namely bolts and strikes.

Bolts
There are two types of bolts used for most door applications: the latch bolt and the deadbolt (Figure 5–26). They are easily distinguished from each other. A latch bolt always has a beveled face, whereas the face on a standard deadbolt is square. (A latch is a mechanical device for keeping a door or a gate closed.)

A latch bolt—which sometimes is called a latch, a locking latch (to distinguish it from nonlocking latches), or a spring bolt—is always spring loaded. When the door on which it is mounted is closing, the latch bolt retracts automatically when its beveled face contacts the lip of the strike. Once the door is fully closed, the latch springs back to extend into the hole of the strike, securing the door.

A latch bolt has the single advantage of convenience. A door equipped with a locking latch will automatically lock when it is closed. No additional effort with a key is required. It does not, however, provide very much security.

The throw on a latch bolt is usually 3/8 inch (7.62 cm), but it is seldom more than 5/8 inch (12.7 cm). (Throw is the maximum distance that the bolt can extend.) Because it must be able to retract into the door on contact with the lip of the strike, it is difficult to make the throw much longer. However, because there is always some space between the door and the frame, a latch projects into the strike no more than 1/4 inch (5.08 cm) (often as little as 1/8 inch [2.54 cm] on poorly hung doors). Most doorjambs can be spread at least 1/2 inch (10.16 cm) with little effort, permitting an intruder to circumvent the lock quickly.

Another undesirable feature of the latch bolt is that it can easily be forced back by any thin shim (such as a plastic credit card or a thin knife) inserted between the face-plate of the lock and the strike. Antishim devices have been added to the basic latch bolt to defeat this type of attack (Figure 5–27a). They are designed to prevent the latch bolt from being depressed once the door closes. These often are called deadlocking latches, a term that is mildly deceptive because these latches do not actually deadlock and are not nearly as resistant to jimmying as deadlocks. Often a thin screwdriver blade can be

![Figure 5–26 The basic types of bolts. From Edgar, James M., and William D. McInerney, “The use of locks in physical crime prevention,” in L. Fennelly, The Handbook of Loss Prevention (Boston, Butterworth-Heinemann, 1989, p. 236), with permission.](safetymessage.com)
inserted between the faceplate and the strike, then pressure is applied to break the anti-shim mechanism and force the latch to retract.

An antifriction latch bolt (Figure 5–27b) reduces the closing pressure required to force the latch bolt to retract, which permits a heavier spring to be used in the mechanism. Most modern antifriction latches also incorporate an antishim device. Without it, the antifriction latch is extremely simple to shim.

The deadbolt is a square-faced solid bolt that is not spring loaded and must be turned by hand into either the locked or unlocked position. When a deadbolt is incorporated into a locking mechanism, the result usually is known as deadlock. The throw on a standard deadbolt is also about 1/2 inch (10.16 cm), which provides only minimal protection against jamb spreading. A long-throw deadbolt, however, has a throw of 1 inch (20.32 cm) or longer. One inch (20.32 cm) is considered the minimum for adequate protection. When properly installed in a good door using a secure strike, this bolt provides reasonably good protection against efforts to spread or peel the jamb.

The ordinary deadbolt is thrown horizontally. On some narrow-stile doors (stile refers to the vertical uprights forming the frame around the glass panels), such as aluminum-framed glass doors, the space provided for the lock is too narrow to permit a long horizontal throw. The pivoting deadbolt is used in this situation to get the needed longer throw (Figure 5–28). The pivoting movement of the bolt allows it to project deeply into the frame—at least the recommended minimum of 1 inch (20.32 cm) and usually more. When used with a reinforced strike, this bolt can provide good protection against efforts to spread or peel the frame.

**Strikes**

Strikes are an often overlooked but essential part of a good lock. A deadbolt must engage a solid, correctly installed strike or its effectiveness reduces significantly (Figure 5–29).

---


---

* A small metal plate firmly attached to the front of a door can help protect from this type of attack on the latch bolt.

** Note: For guest safety, some hotel guest room entrance doors have a spring-activated deadbolt that automatically engages when the guest enters the room and closes the door.

*** Again, a small metal plate firmly attached to the front of a door can help protect from the use of a hacksaw to attack the deadbolt.
Master Keying of Pin Tumbler Locks

Master keying is a variation of pin tumbler locks that has been in widespread use for many years. Almost any pin tumbler cylinder can easily be master keyed. Additional tumblers called master pins are inserted between the drivers and key pins. These master pins enable a second key, the master key, to operate the same lock (Figure 5–30).

Generally, an entire series of locks is combined and operated by the same master key. There may also be levels of master keys including submasters that open a portion, but not all, of a series, master keys that open a larger part, and grand masters that open the entire series. In very involved installations, there may even be a fourth level (a grand grand master key).
A description of the various keys in a typical high-rise office building master key system follows:

1. The change key operates a single lock within the master key system. For example, individual occupants of a tenant space have a key that unlocks the door of their office but does not unlock perimeter doors leading to the tenant space.
2. The submaster key operates all locks within a particular area or group. For example, a tenant office manager has a key that unlocks all perimeter doors leading to his or her tenant space and all interior office doors within this space.
3. The floor master key operates one or more submaster systems. For example, a janitorial supervisor has a key that unlocks all perimeter doors leading to tenant spaces on a multiple-tenant floor, all interior office doors within these tenant spaces, and all maintenance spaces on that floor.
4. The grand master key operates one or more master systems. For example, a member of building management has a key that unlocks all perimeter doors leading to tenant spaces, all interior office doors within tenant spaces, and all maintenance spaces within the building.
5. The grand grand master key operates one or more grand master systems. For example, in a high-rise project where there are several high-rise buildings, a member of building management has a key that unlocks all perimeter doors leading to tenant spaces, all interior office doors within tenant spaces, and all maintenance spaces on all floors of all buildings.

An example of a master key arrangement is shown in Figure 5–31. Master keys and control keys for removable core cylinders should be kept under strict control by building management. Keys should be issued only to those who have an absolute need for them.
FIGURE 5-31 Diagram of a sample master key arrangement for a seven-story building.
Master Key Problems

There are a number of security problems with master keys. The most obvious one is that an unauthorized master key will permit access through any lock of the series. Loss of a master key compromises the whole system, necessitating an entire building to be rekeyed at a considerable cost. Finneran advised, “If rekeying becomes necessary, it can be accomplished most economically by installing new locking devices in the most critical points of the locking system and moving the locks removed from these points to less sensitive areas. Of course, it will be necessary to eventually replace all the locks in the system, but by using the method just described the cost can be spread out over several budgeting periods.”

Whether to immediately rekey the building or delay in this suggested manner is a risk-based decision that should only be undertaken by the building owner or manager. If delaying the rekeying can potentially affect the life of people or seriously impact other vital assets, then, despite the costs involved, it should not be delayed.

Another possible solution to mitigate the cost of rekeying is a high-security lock system called InstaKey. This system allows locks to be rekeyed by simply inserting and turning a specially designed key (Figure 5–32). According to InstaKey, its lock permits up to 12 changes without removing cores or lock hardware. It is done using a special key that removes wafers from different stacks within the lock cylinders. The lock also allows any level—grand master, master, and change key—to be changed individually without affecting the operation or keying of any other level. Once all wafers have been removed, the cylinder can be repinned to a new sequence of changes and the cycle begun again.

An important feature of this system is that it allows locks to be changed immediately by the simple turn of a key. This is crucial from a security standpoint because a potential security breach can be addressed immediately. The expense of the lock change is restricted to the replacement keys for the affected level only. InstaKey is compatible with a broad range of cylinder types.

A less obvious security problem with master key systems is the fact that master keying reduces the number of useful combinations because any combination used must not only be compatible with the change key, but also with the master key. If a submaster is used in the series, the number of combinations is reduced further to those compatible with all three keys. If four levels of master keys are used, the number of useful combinations becomes extremely small. If a large number of locks are involved, the number of locks may exceed the number of available combinations. When this occurs, it may be necessary to use the same combinations in several locks, which permits one change key to operate more than one lock (cross keying). This creates an additional security hazard.

One way of increasing the number of usable combinations and decreasing the risk of cross keying is to use a master sleeve or ring. This sleeve fits around the plug, providing an additional shear line similar to the slide shear line in a removable core system. Some of the keys can be cut to lift tumblers to the sleeve shear line and some to the plug shear line.
shear line. This system, however, requires the use of more master pins. Any increase in master pins raises the susceptibility of the lock to manipulation because the master pins create more than one shear point in each pin chamber, increasing the facility with which the lock can be picked.

The basic pin tumbler mechanism has been modified extensively by a number of manufacturers to improve its security. High-security pin tumbler cylinder mechanisms used in high-rise buildings commonly are produced with extremely close tolerances and provide a high number of usable combinations. Additional security features include the use of very hard metals in their construction to frustrate attacks by drilling and punching.

Key control is an essential part of any building locking system. Before addressing perimeter locking devices, it is appropriate to review key control measures.

FIGURE 5-32 InstaKey four-step key change. Courtesy of InstaKey Lock Corporation (www.instakey.com).
Key Control

The following information regarding key control was largely obtained (with slight modifications) from _Security Supervision: A Handbook for Supervisors and Managers_ by Eugene D. Finneran:49

Before an effective key control system can be established, every key to every lock used to protect a facility must be accounted for. However, the chances are good that it will not even be possible to account for the most critical keys or to be certain that they have not been copied or compromised. If this is the case, there is but one alternative—to rekey the entire facility.

Once an effective locking system has been installed, positive control of all keys must be gained and maintained. This can be accomplished only if an effective key record is kept. When not issued or in use, keys must be adequately secured. A good, effective key control system is simple to initiate, particularly if it is established in conjunction with the installation of new locking devices. One of the methods that can be used to gain and maintain effective key control follows.

**Key Cabinet**

A well-constructed steel cabinet for keys is essential. The cabinet must be of sufficient size to hold the original key to every lock in the system. It also should be capable of holding any additional keys that are in use in a facility. (Of course, building tenants and residents will have files, safes, and locks whose keys are not supplied to building management, and therefore these keys will not be stored here.) The cabinet should be well installed to make it difficult, if not impossible, to remove it from the facility. It should be secured at all times when the person designated to control the keys is not actually issuing or replacing a key. The key to the cabinet itself must receive special handling, and when not in use, it should be placed in a locked compartment inside a locked safe.

A popular device for key control and accountability is an electronic key cabinet (Figure 5–33) or drawer where keys and key sets are individually secured until released by an authorized user. The steel cabinet or drawer may be accessed using a keypad, an access card, logging onto a computerized system with a user name and password, or utilizing a biometric reader. The advantages of such an electronic key management system include the following:

- Rugged steel storage cabinet with intrusion detection monitoring of cabinet tampering
- Ease of locating keys with illuminated key slots
- Accountability for each key by time and date
- Time zones can be programmed for each key and each user
- Eliminates manual reports (and manual input errors)
- Provides detailed electronic reports
- Connectivity to computers, printers, and networks
- Battery backup power supply during power failure
- Scalability potential for adding multiple cabinets50

---


FIGURE 5-33 Morse Watchman KeyWatcher Key Management System. Courtesy of Morse Watchman, Inc. (www.morsewatchman.com).
Key Record
Some administrative means must be set up to record key code numbers and indicate to whom keys to specific locks have been issued. This record may take the form of a ledger book, a card file, or computerized key control records.

Key Blanks
Blanks to be used to cut keys for issue to authorized personnel must be distinctively marked for identification to ensure that no employees have cut their own keys. Blanks must be kept within a combination-type safe or an electronic key cabinet or drawer and issued only to the person authorized to cut keys and then only in the amount authorized by the person responsible for key control. Such authorization should always be in writing (or possibly in an electronic form) and records should be made of each issue that will be matched with the returned key. Keys damaged in the cutting process must be returned.

Inventories
Periodic inventories must be made of all key blanks, original keys, and duplicate keys issued. Merely telephoning or e-mailing employees, supervisors, or executives and asking them if they still have their keys will not suffice. Key control personnel must inspect each key personally.

Audits
In addition to the periodic inventory, a member of management should perform an unannounced audit of all key control records and procedures. During the course of this audit, a joint inventory of all keys should be conducted.

Perimeter Locking Devices
To meet life safety codes, perimeter legal exit doors require approved panic hardware such as cross bars or push pads. This hardware is installed on building exterior doors normally located at the ground level and exit doors in stairs that discharge to the exterior (where it is called fire exit hardware).

The push pad style has gained wide acceptance. One advantage to push pads is that electric latching and electronic monitoring features can be added (where permitted...
by the authority having jurisdiction). Doors equipped with panic bars or pads may be locked on the exterior side, and at all times the inside of the door must be operable, providing uninhibited egress.

Panic hardware and fire exit hardware function well but provide only a low level of security. A reason for this is that some doors can be compromised easily from the outside (using, for example, a simple device such as a coat hanger to pull a bar down to release the door). When these devices are installed on aluminum doors, particularly on large front entrance doors, the installation must be done in such a way as to make the device somewhat secure. One way to do this is to use an electromagnetic lock, which meets life safety requirements.

**Electromagnetic Locks**

Electromagnetic locks are very useful in high-rise buildings. “Devoid of moving parts—a characteristic that eliminates wear and binding—an electromagnetic lock possesses a holding power of from 1500 to 2700 lbs. [680 to 1225 kilograms] and consumes six to nine watts of power at 24 volts.”

Electromagnetic locks may be concealed (called shear electromagnetic locks) or exposed (called direct hold electromagnetic locks). They consist of an electromagnet, which is attached to the doorframe header, and a metal armature or plate, which is mounted on the door itself (Figure 5–34). The *New Webster Dictionary* (1980) defines

![FIGURE 5-34 A typical installation of a direct hold electromagnetic lock for a single door with request to exit push bar. The electromagnet is attached to the doorframe header, and a metal armature or plate is mounted on the door itself. Courtesy of Security Door Controls of Westlake Village, CA (for the Series 1500 EMLock), (www.sdcsecurity.com).](image)

an electromagnet as “a bar of soft iron rendered temporarily magnetic by a current of electricity having been caused to pass through a wire coiled round it.” When an electrical current is flowing through the electromagnet (usually at a low voltage of 12 or 24 volt DC), a magnetic field is created, and the armature is magnetically attracted to the magnet in the doorframe, thereby holding the door closed.

Electromagnetic locks can be installed on perimeter legal exit doors and main entrance doors. Through use of a time clock, these doors can be locked automatically at the end of the day when the building closes. The times of opening and closing these perimeter doors can vary according to the building’s needs. When the doors are secured, access from the outside of the building can be obtained by installing a card reader (normal egress is permitted using panic hardware or automatic unlocking devices such as motion detectors). Persons authorized to enter use their access card to open the door. In addition, the position of the door (whether it is open or closed) and its locking status (locked or unlocked) can be monitored at a remote location, such as the security command center, via sensors included on the electromagnetic lock.

Life safety codes mandate that the power source to all permitted locks restricting occupants’ means of egress must be supervised by the building’s fire life safety system. In the event of an emergency, such as a power failure or the activation of a fire alarm, electrical current to the electromagnet ceases, and the doors unlock (i.e., fail safe). Occupants can freely exit the building and responding emergency agencies, such as the fire department, can enter.

“The benefits of electromagnetic locks are that fire safety requirements can be easily met, security is attained and access is provided for select personnel. Electromagnetic locks take the place of illegal or other unapproved methods of security by eliminating the need for chains, padlocks, and other mechanical devices.”

Stairwell Locking Devices

Stairwell door security is a lot more complicated than perimeter door security. The stringent code requirements and specifications for stairwell locks and locking systems are essential because stairwells are a critical means of egress for occupants during building emergencies. For example, during a fire, elevators generally are not considered a safe means of general population evacuation (although under special circumstances, such as when the elevators have been fire protected or the fire department directs, they might be used for evacuation of the disabled/physically impaired and others). This leaves the stairwells as the primary means of egress.

\*Fail safe is “a safety feature of a security device that is designed to release or disconnect during a power loss” (ASIS Glossary of Terms. January 4, 2008. <www.asisonline.org/library/glossary/b.pdf>.; ASIS International; October 22, 2008).

To understand the importance of critical stairwell specifications, it is worthwhile to examine NFPA 101, *Life Safety Code* (which itself, or a modification thereof, has been adopted by many authorities having jurisdiction):

Section 7.2.1.5.1 Doors shall be arranged to be opened readily from the egress side whenever the building is occupied.

Section 7.2.1.5.2 Locks, if provided, shall not require the use of a key, a tool, or special knowledge or effort for operation from the egress side.

Section 7.2.1.5.7 Every door in a stair enclosure serving more than four stories, unless permitted* ... shall meet one of the following:

1. Re-entry from the stair enclosure to the interior of the building shall be provided.
2. An automatic release that is actuated with the initiation of the building fire alarm system shall be provided to unlock all stair enclosure doors to allow re-entry.
3. Selected re-entry shall be provided in accordance with 7.2.1.5.7.1. [The Life Safety Code allows for some exceptions, particularly in older high-rise buildings where automatic release systems are not installed.]

Section 7.2.1.5.7.1 Doors on stair enclosures to be equipped with hardware that prevents re-entry into the interior of the building provided that the following criteria are met:

1. There shall be at not less than two levels where it is possible to leave the stair enclosure to access another exit.
2. There shall not be more than four stories intervening between stories where it is possible to leave the stair enclosure to access another exit.
3. Re-entry shall be possible on the top story or next-to-top story served by the stair enclosure, and such story shall allow access to another exit.
4. Doors allowing re-entry shall be identified as such on the stair side of the door.
5. Doors not allowing re-entry shall be provided with a sign on the stair side indicating the location of the nearest door, in each direction of travel, that allows re-entry or exit.53

As Geringer pointed out,

*The inherent problem is that building tenants may need to lock these exits on the stair side for obvious security concerns, such as transient pedestrian traffic. To ensure life safety [i.e., fire door integrity], all stairwell doors require a ... mechanism that maintains a closed and latched door position, even when the door is unlocked, to prevent smoke and fire from entering the stairwell. One solution is to install high-tower-function electrified mortise locksets on*

*There are exceptions listed in the NFPA 101 *Life Safety Code*. For more details, one should examine the code itself or the code requirements of the authority having jurisdiction for a specific building occupancy.

appropriate stairwell doors [Figure 5–35]. These locks are equipped with
door-position sensors as well as locked/unlocked status sensors. When ener-
gized, only the stair side is secured.... Generally, high-tower-function mortise
locks are energized and locked at all times. Access control is accomplished
by either a mechanical key, [a] digital keypad, or a card reader.... The power
source for these locks is controlled by the building life safety system so that
in an emergency, doors immediately unlock yet remain closed and latched,
protecting the stairwell from smoke and fire.

The obvious benefits of this type of lock are the following:

- Life safety is provided.
- Authorized personnel have controlled access.
- Building tenants have supervised security.  

**Balancing Security and Fire Life Safety**

The fact that security and fire life safety are different disciplines, and that their priorities
are sometimes in conflict with each other, is nowhere better demonstrated than at the stair-
well exits. “The conflict lies between the need to have immediate, unobstructed, one-step* exit from a building that may be on fire and the need to prevent unauthorized ingress or egress.”  

---

54 Geringer RG. High-rises look to lock out problems. *Access Control Reprint.* Atlanta, GA; June 1991:2.

*One-step* refers to the requirement that only a single action is needed to unlatch the door.

9th printing. (Used with permission of POA Publishing, LLC, Los Angeles, CA. Original copyright from the
Merritt Company, July 1993:5).
Stairwell Exits at Ground Level

Fire exit hardware is installed on fire doors within a high-rise building, including stairwell exit doors that normally exit at the ground level. These doors must remain closed and latched at all times for fire compartmentation purposes.

The stairwell exit doors that normally exit at the ground level may be locked on the exterior side as long as, at all times, the inside of the door is operable, providing uninhibited egress. When an exiting occupant applies pressure to the fire exit hardware, the door will immediately unlock (although, under special circumstances a delayed egress lock may be incorporated into the emergency exit system). One way to deter unauthorized entry from the outside of the building is to install a powerful electromagnetic lock. This maintains a high degree of security and has no impact on life safety. However, only under specific conditions can fire exit doors be locked from the inside of the stairwell at the point of exit from the building. NFPA 101, *Life Safety Code*, states,

Section 7.2.1.5.1 Doors shall be arranged to be opened readily from the egress side whenever the building is occupied.

Section 7.2.1.5.2 Locks, if provided, shall not require the use of a key, a tool, or special knowledge or effort for operation from the egress side.

Section 7.2.1.5.11 Devices shall not be installed in connection with any door on which panic hardware or fire exit hardware is required where such devices prevent or are intended to prevent the free use of the door for purposes of egress, unless otherwise provided in 7.2.1.6 [Special Locking Arrangements*].

Section 7.2.1.5.11 Examples of devices prohibited by this requirement include locks, padlocks, hasps, bars, chains, or combinations thereof.56

These life safety requirements present a security problem—the need to maintain immediate, unobstructed exit from the stairwell exit door that discharges to the exterior at the ground level provides an opportunity for a person who has perpetrated a crime within the building to make a rapid escape. The NFPA addresses the need to maintain a degree of security on these emergency exit doors in NFPA 101, *Life Safety Code:*

Section 7.2.1.6.1 Delayed-Egress Locks. Approved, listed, delayed-egress locks shall be permitted to be installed on doors serving low and ordinary hazard contents in buildings [such as those hazards most likely found in office buildings, hotels, and residential and apartment buildings] protected throughout by an approved, supervised automatic fire detection system in accordance with Section 9.6 [Fire Detection, Alarm, and Communication Systems], or an approved, supervised automatic sprinkler system in accordance with Section 9.7 [Automatic Sprinklers and Other Extinguishing Equipment], and where permitted in Chapters 12 through 42, provided that the following criteria are met.

1. The provisions of 7.2.1.6.2 [Access-Controlled Egress Doors] for access-controlled egress doors shall not apply to doors with delayed-egress locks.

---

*These special locking arrangements include delayed-egress locks and access-controlled egress doors.

2. The doors shall unlock upon actuation of one of the following:
   a. Approved, supervised automatic sprinkler system in accordance with Section 9.7
   b. Not more than one heat detector of an approved, supervised automatic fire detection system in accordance with Section 9.6.
   c. Not more than two smoke detectors of an approved, supervised automatic fire detection system in accordance with Section 9.6.
3. The doors shall unlock upon loss of power controlling the lock or locking mechanism.
4. An irreversible process shall release the lock within 15 seconds, or 30 seconds where approved by the authority having jurisdiction, upon application of a force to the release device required in 7.2.1.5.9 under the following conditions:
   a. The force shall not be required to exceed 15 lbf (67 N).
   b. The force shall not be required to be continuously applied for more than 3 seconds.
   c. The initiation of the release process shall activate an audible signal in the vicinity of the door.
   d. Once the door lock has been released by the application of force to the releasing device, relocking shall be by manual means only….
5. A readily visible, durable sign in letters not less than 1 inch (25 mm) high and not less than 1/8 inch (3.2 mm) in stroke width on a contrasting background that reads as follows shall be located on the door adjacent to the release device:

   PUSH UNTIL ALARM SOUNDS.
   DOOR CAN BE OPENED IN 15 SECONDS.  

   “If the exit doors are designed as part of an integrated system, the time delay can be a substantial crime prevention tool” (Figure 5–36).

Sequence of Events
If a person uses a stairwell to escape a building at the ground level after committing a crime on an upper floor, the following sequence of events could be designed to occur when he or she pushes on the emergency exit release bar:

- An alarm on the door will sound at the door but the door will not immediately open.
- Activation of the door alarm will trigger an alarm signal to the security command center to alert security staff of the situation. Building security using an intercom that communicates with this area could challenge the person, and security officers could be immediately dispatched to the inside or the outside of the stairwell to intercept the person in question.
- A CCTV camera at the emergency exit door could be used to view and record the event.

57 ibid., pp. 144, 145.
Thus, this 15-second egress delay (or 30-second egress delay, where permitted by the authority having jurisdiction) may allow enough time for security staff to take action and to obtain a recorded image that may be helpful in identifying the individual and any property they may be carrying. The delayed-egress lock thus provides an opportunity to implement basic security measures without a substantial impact on life safety. Some delayed-egress locking systems are even designed with features such as verbal exiting instructions and a lighted digital countdown display to indicate how many seconds remain before the door will release. Of course, the authority having jurisdiction must always be consulted when installing such locks.

**Stairwell Exits to Building Roof**

There is a conflict between security and fire life safety when a stairwell provides access to a building’s roof. There may be a need to maintain immediate, unobstructed access
from the stairwell door at the roof for use by first responders. This access needs to be balanced with the security concern that an unauthorized person (including, for example, possibly a suicidal person) may use this same opening to reach the roof. Whether or not the stairwell door(s) leading to the roof can be locked depends on the local authority having jurisdiction. Some jurisdictions permit it to be locked if certain criteria are met—such as requiring the door(s) leading to the roof to automatically unlock or fail-safe when activation of the building’s fire life safety system occurs. An intercom and a CCTV camera, both constantly monitored in the security command center, can be installed at the door. A person (other than those who carry a key or an access card to unlock the door) can use the intercom to request access and can be viewed by the security staff via the camera. If the person is granted permission to proceed, security staff can then remotely unlock the door leading to the roof.

Other Locking Devices

Doors within a tenant or an apartment that do not lead to a legal exit, such as a perimeter or a stairwell door, are permitted to use a variety of electric and combination locks (in addition to key-, card-, token, and biometric system–operated locks), depending on their application.

Electric Locks

The three main types of electric locks are electromagnetic locks (previously addressed), electric strikes, and electric bolt locks. They are available in two operating modes: fail safe—unlocked when deenergized, locked when energized, and fails into safe (unlocked) mode; and fail secure—locked when deenergized, unlocked when energized, and fails into secure (locked) mode. The exception to this is the electromagnetic lock, which is fail safe only.

The following description of electric strikes and electric bolt locks was obtained from *Electronic Locking Devices* by John L. Schum:59

- Electric strikes (also called electric door openers or electric releases) use either an electromagnet or a solenoid to control a movable keeper (Figure 5–37). The *New Webster Dictionary* defines a solenoid as “a coil of wire wound in the form of a helix, which, when traversed by an electric current, acts like a magnet.”60 The keeper interfaces with the bolt of the lock device on the door. Electrical actuation of the strike allows the door to open even though the bolt of the lock device still is extended. Electric strikes usually are installed in the doorframe in place of the conventional lock strike plate. They also are available for mounting on the doorframe. They are used in conjunction with various door locksets to provide additional security features, including convenience and remote operation to lock or

---

unlock doors electrically to control the egress and ingress of persons. Receptionists often use these devices to open entrance doors without the inconvenience of physically going to the door itself.

- Electric bolt locks (or electric locks, electric deadbolts, or power bolts) consist of a spring-loaded bolt that is activated by an electric solenoid and moves into or out of a mounting strike. These generally are mounted in or on the doorframe (Figure 5–38). They are not for use on doors used as points of egress. These devices can provide a range from low to high security and are used in traffic control situations, especially mantraps. An interlock is a system of multiple doors with controlled interaction. A mantrap is “a double-door booth or chamber that allows a person to enter at one end, undergo an access identification routine inside the booth, and if the routine is satisfied, the lock on the booth door at other end is released.”\(^6\) Mantraps are also known as interlocks or sally ports. Mantraps are popular in high-security areas such as computer rooms and data centers. Unlike electric strikes, electric bolt locks require no other mechanical lock device to provide security.

**Combination Locks**
Combination locks operate mechanically or electrically (and are not to be confused with the dial-type combination locking mechanisms used on safes, etc.).

A mechanical push-button combination lock has an alphanumeric keypad that is part of the locking mechanism. The keypad is used to enter a series of letters or numbers in a particular predetermined sequence. If the correct sequence of letters or numbers is entered, the bolt in the lock is released mechanically. Some mechanical push-button combination locks are combined with a key that will only operate when the correct sequence of letters or numbers has been entered (Figure 5–39).
Figure 5-38: A mortise-mount right-angle electric bolt. Courtesy of Security Door Controls (www.sdcsecurity.com).

Figure 5-39: A Simplex 5000 mechanical push-button combination lock. Courtesy of Kaba (www.saflok.com).
An electrical push-button combination lock is different in that the alphanumeric keypad assembly is remote to the locking mechanism. When the correct sequence of letters or numbers is entered, an electrical signal is generated to operate the lock.

**Limitations of Combination Locks**

A problem with combination locks is that denying access to a person who has the lock combination requires erasing the codes from the lock itself. Also, someone can surreptitiously obtain the correct sequence of letters or numbers required for operating the lock by looking over the shoulder of a person as he or she enters the appropriate letters or numbers.

A modern electronic numeric keypad manufactured by Hirsch Electronics Corporation has addressed this problem. The Hirsch ScramblePad Secure Electronic Keypad (Figure 5–40) has a scrambler that automatically changes the position of the numbers on the keypad after each use and can only be read by a person standing directly in front of the keypad. This makes it much more difficult for anyone other than the person using the device to observe the numbers being entered.

A safety feature incorporated into some combination locks is a duress code that when a particular letter or a number or a sequence of letters or numbers is entered will automatically notify a monitoring area that the person is signaling that there is a duress or emergency situation.

Push-button combination locks should never be installed on doors used as points of egress. Instead they are commonly installed within already-secured areas on doors leading to isolated areas such as a door leading to a computer room. Electrical push-button combination locks should be equipped with standby power so that in the event of the loss of normal power the lock will continue to operate. If locks are not equipped with this feature, they often are designed, for security reasons, to fail secure. Also, combinations on push-button locks always should be able to be changed rapidly and without difficulty.

**Electromagnetic Hold-Open Devices**

Before proceeding to card-operated locks, we will briefly discuss the use of electromagnetic hold-open devices on elevator lobby doors. Elevator lobby doors normally are held in an...
open position. On activation of the building fire life safety system, electrical current to the electromagnetic hold-open device ceases and the device releases the lobby doors, which swing shut (Figure 5–41). This action results in compartmentation of the elevator lobby and assists in preventing fire and products of combustion from entering into the lobby.

**Code Acceptance**
The code acceptance of electromagnetic locks, delayed-egress locks, electric strikes, electric bolt locks, or combination locks always should be checked with the local authority having jurisdiction, a registered locksmith, a certified door consultant, or an architectural hardware consultant.*

**Credential-Operated Locks**

Credential-operated locks are part of electronic access control systems commonly found in modern high-rise buildings. In general, access control systems consist of the following:

- Access control credential device (whether it be an access card or a keycard [as it is sometimes called], a token, or a biological characteristic of the person requesting access)


***A credential is something that entitles a person to certain rights or privileges.

****An access card is a device that is presented to a card reader to operate an access control system. Sometimes it is called an electronic access card or a keycard.
Access control credential reader (whether it be a card reader, a token reader, or a biometric reader)
- Central processing unit (CPU) controlling the access control system
- Wiring or wireless communication system from the access control reader to the microprocessor
- Locking device or, in elevator installations, the elevator control system itself
- Closing mechanism of the door and the barrier itself or, in the case of elevator installations, the elevator operating system itself
- Security command center, or similar location, where the microprocessor, the keyboard, the monitor display screen, and the printer are located

According to Cumming,

The various categories of the system all act under the same principle—that recognition of a binary [or, in large systems, hexadecimal] code generated electronically, activates a checking procedure within the system. If, after checking, the code is verified, a second signal activates a locking device [or, in elevator installations, the elevator control system itself], allowing entry. The choice of a particular access system is a matter of trying to match the product to the environment in which it will operate, the level of security required, and the needs of the users.  

In the case of a card-operated lock, the unique card of the building user is presented to a card reader at the location where access is being controlled. Within the card reader a sensor deduces information from the card. The information is translated into a binary code that is transmitted electronically to the CPU controlling the system. Access information of the cardholder has previously been programmed into the computer memory. This information, which will include the identification of the cardholder and the time period in which to grant access, is then compared by the CPU with the code number it has received from the reader. The CPU will then communicate back to the locking device to unlock and facilitate access, or it will remain locked and thereby deny access. The time the card was used and the identity of the cardholder will be recorded in the memory of the CPU and may also be printed out for future reference. If a communication failure occurs, modern systems are designed to perform, at the card reader location, limited functions of the CPU such as allowing or denying access. (Some card-operated locks, such as those on many hotel guest room doors, only operate at the door itself; more modern lock systems are hardwire or wireless systems communicating back to a central computer at the front reception desk.)

Card-operated locks use various types of cards. Because the card is the key to the system, the system is only as secure as the security afforded to the card itself. The following sections describe cards used with card-operated locks.

---


*For example, the Saflok Messenger Wireless Lock Access Network has the capability for the Messenger module in each lock to report to the central computer all keys used in the lock. Also, it can notify the central computer when a door has not been fully closed for a specified period of time and when the battery power operating the lock is low (Saflok™ Messenger® Wireless Lock Access Network brochure [Saflok, a member of the Kaba Group. <www.saflok.com>]).
Magnetic Slug Cards
Previously the magnetic slug card was widely used, but it has now been superseded by magnetic stripe cards and barium ferrite cards. The magnetic slug card consisted of magnetic bits embedded in an opaque plastic card in a particular row-and-column pattern. A row of magnetic-sensing heads then read the presence or absence of a magnetic slug to determine the appropriate code.

Magnetic Stripe Cards
The magnetic stripe, or mag-stripe (or strip), card is the most inexpensive and frequently used low-security access system card. It has the appearance of a standard credit card. It consists of a magnetic stripe fused onto the card’s surface. Information, in the form of a binary code, is recorded on the magnetic stripe. Because the stripe is visible and accessible and the technology involved is well known, the codes are susceptible to being duplicated, changed, or obliterated (low-strength magnetic fields may cause distortion of the coded information). To address this issue, some manufacturers have recorded on the magnetic stripe a unique code that cannot be changed or removed and can be read only by using specialized equipment. The cards themselves are prone to normal wear and tear such as cracking and scratching. They are very reliable, producing few false readings, and have particular application where a large number of cards are required. Using a keypad in conjunction with the card reader raises the level of security of such card-operated locks.

Magnetic Sandwich or Barium Ferrite Cards
In these cards, a sheet of magnetic material, usually barium ferrite, is laminated in sandwich fashion between two plastic layers. Spots in the magnetic material are magnetized in a particular row-and-column pattern. The presence or absence of a magnetic spot is then read by a row of magnetic-sensing heads to determine the appropriate code. These cards stand up to normal wear and tear very well with the recorded code being protected by the two outer layers of plastic material.

Wiegand Effect Cards
Wiegand cards, also known as embedded wire cards, are used for high-security applications where limited numbers of cards are required. The card has short lengths of special wire embedded within it. A magnetic field is generated within a card reader, causing the wires to carry electronic signals when the card is passed through the reader. These electronic signals determine whether or not a card user is authorized for access. These cards are relatively expensive and are difficult to reproduce, but they do stand up well to a considerable amount of wear and tear.

Insertion- and Swipe-Type Readers
Before examining other types of cards, it is appropriate to state that one of the following types of card readers is used to read the aforementioned cards:

- The insertion-type, where the card is held by its end and inserted into a slot in the card reader (Figure 5–42). With this type, clips or chains attached to the card may interfere with the insertion of the card.
- The swipe-type, whereby magnetic stripe cards are held along the top edge of the card and are “swiped” through a slot in the card reader allowing the magnetic
FIGURE 5–43  Swipe-type electronic card reader in an office building. An access card is “swiped” through the slot in the card reader. Photograph by Stephen Lo.

stripe to be read (Figure 5–43). This type of reader is preferred because clips or chains attached to the card are not a problem, it has no moving parts requiring maintenance, and its design makes it less susceptible to card jamming in the reader and the effects of the weather.
Proximity Cards

These low-security cards are usually of the standard credit-card type with three laminated layers, the center layer containing the coding information. They operate locks in a similar fashion to the aforementioned cards but are not required to come into contact with the card reader.

Proximity cards, when brought in relatively close proximity to the reader (Figure 5-44), can communicate with the sensor by electromagnetic, ultrasound, or optical transmissions. Because these user-friendly cards do not need to be inserted into or swiped through the reader, there is less wear and tear on the cards themselves. Because proximity card readers contain no moving parts, maintenance is seldom required. Also, persons carrying items such as books, a briefcase, a laptop computer, or an umbrella can use proximity cards more conveniently than the previously mentioned insert- or swipe-type cards. Proximity cards are often more convenient for disabled/physically disabled persons to use. Also, large-sized proximity readers are convenient for all drivers when presenting their access card to exit a parking garage. A feature of proximity readers is that they can be mounted behind glass or a digital keypad or otherwise made inaccessible to acts of vandalism.

(Sometimes, a key fob is used. It is a small device that people often carry with their keys on a ring or a chain. It usually contains a passive radio frequency identification [RFID] tag that operates in much the same manner as a proximity card to communicate via a [reader] pad) with a central server.)

Dual Technology Card

Sometimes, access cards have dual technology. Examples would be a magnetic stripe/proximity card and an RFID/proximity card.

Magnetic Stripe/Proximity Card

A magnetic stripe card may be used for a building tenant or resident to access a building garage, the building itself, and its elevators. In addition, the tenant or resident may have

---

a proximity card to access his or her office or apartment. By providing a dual technology card—a proximity card with a magnetic stripe on it—tenants or residents need carry only one card.

**RFID/Proximity Card**

An RFID/proximity card has an RFID tag inside the proximity card. “The proximity card allows access into a building and/or particular parts of the building in the normal manner. Within the building, there are strategically placed antennae which note movement of card holders past them. The associated software logs all these movements, but can also be programmed to alarm at a security post when an RFID tag enters a part of the building* that it should not.”  

(See Figure 5–45 for a residential door lock that incorporates RFID technology.)

**Smart Cards**

Smart cards are similar to a credit card with information stored on an integrated circuit chip embedded in the plastic card itself. “The card has both a coded memory and microprocessor intelligence. It can record card transactions [events] and store data.”  

It can be used to store large amounts of information about the cardholder. According to Harwood, “the intelligence of the integrated circuit chip ... allows [a smart card] to protect the information being stored from damage or theft. For this reason, smart cards are much more secure than magnetic swipe cards, which carry information on the outside of the card and can be easily copied. Smart cards are an effective way of ensuring secure access to open interactive systems, such as encryption key mobility, secure single sign-ons and electronic digital signatures.... The smart card is ideal for IT security applications.”

“The smart card differs from the card typically called a proximity card in that the microchip in the proximity card has only one function: to provide the reader with the card's identification number. The processor on the smart card has an operating system and can handle multiple applications such as a cash card, a pre-paid membership card, and even an access control card.”

There are both contact and contactless smart cards. “The difference between the two types of smart cards is found in the manner with which the microprocessor on the card communicates with the outside world. A contact smart card has eight contacts, which must physically touch contacts on the reader to convey information between them. A contactless smart card uses the same radio-based technology as the proximity card with the exception of the frequency band used. Smart cards allow the access control system to save user information on a credential carried by the user rather than requiring more memory on each [lock] controller.”

Smart cards can be used to control access to and within buildings. An “emerging use of smart cards allows service providers such as newspaper delivery carriers and

---

*For example, in a corporate headquarters office building, alarmed antennae could be installed in the area of the chief executive officer's office and the corporate boardroom.


ibid.
elevator repairmen to enter residential buildings to perform work or make deliveries. Cards can be programmed to allow certain people access to facilities at certain times. This application could also work well for particular people, such as couriers and delivery persons, who need to access multiple buildings at particular times.

While other types of cards, such as proximity cards, can also be programmed for time-specific access, an advantage that smart cards have over other technologies is that a single chip can carry multiple codes for different kinds of

---

69 Gips MA. The name’s the game. Security Management. Alexandria, VA; September 1999:106.
High-rise security and fire life safety systems, explains Bordes. Also, the date and the access period are authenticated by a cryptographic algorithm— contained in the smart card’s chip—a feature not shared by mag stripe or other technologies. This setup eliminates the burden of carrying multiple mechanical keys for multiple buildings. It also authenticates the user and tracks his or her movement. Of course, all the buildings must have appropriate ... technology installed for the system to work.\(^{70}\)

Card Reader Applications
Card readers can be used for the various ingress and egress points to and within high-rise buildings (lobbies, loading docks, parking areas, stairwells, elevators, roofs, elevator machine rooms, fan rooms, central plant, mechanical and engineering facilities, and electrical closets) and various other areas that will vary according to the type of building occupancy. In some office and apartment buildings, tenants and residents use the same access card to enter the parking garage, the building itself, the elevator, and their tenant space or apartment (and in some facilities, to enter recreational areas, business centers, and other areas provided for the tenants/residents).

Antipassback Feature
“A feature of an access control system which prevents successive use of one card to pass through any portal in the same direction. To attain this protection, a separate reader is required at each entrance and exit. Antipassback prevents a card [that has been] passed back to another person [from being used] for the purpose of gaining entry.”\(^{71}\) The antipassback feature often is used to control access to parking garages.

Piggybacking and Tailgating
As with all card readers, the designed level of security can be compromised when the card user permits “tailgating” or “piggybacking.” Tailgating occurs when a person who is authorized to enter at the location where access is being controlled permits, willingly or unconsciously, another individual to enter without being subject to the verification procedure. This phenomenon is particularly prevalent at card readers located at building and tenant entrance doors, and in elevator cars. After the card has granted access, the authorized tenant holds the building or elevator door open so that the person immediately behind can gain access. Such activity can also happen at an access-controlled door when the person seeking entry without authorization waits outside the door until someone exits and then enters while the door remains open.

Identification Cards
Cards, in addition to facilitating access, may also be used as company identification cards. In this case, a photograph of the cardholder, a panel requiring the signature of the authorized cardholder, and possibly a company logo and text, can be added to the card itself. The first two features help ensure that the card is being used by the person authorized to do so. To enhance security, the badges may be numbered and issued in sequence. These

---

\(^{70}\) Gips MA. The name’s the game. *Security Management*. Alexandria, VA; September 1999:106.


---
permanent badges are either photographic-based, laminated identification badges, or, the now prevalent, high-quality color photo ID cards produced quickly and easily using computer-based, video imaging systems. As Goldfeld says, the former “are not capable of efficient badge verification or authentication, because photos and other ID information must be stored in hard copy form and are not readily retrievable. These types of systems also have no safeguards against fraudulent badge production. On the other hand, computer-based, video imaging systems store and retrieve all pertinent verification and authentication information electronically, keep track of IDs that have been produced, as well as who produced them, and often have a number of security features to combat fraud.”

The integration of photo ID badges with access control can be very useful in heightening the level of security for a particular area. “The best benefit, and the one that increases both the security level and the system’s usefulness, is that, in a truly integrated system, any access control system CRT [computer display] screen can display the person’s original digital photo. The display can be initiated automatically by the presentation of an ID badge at a card reader or by operator manual selection via a keyboard, or [a] mouse. The operator can then visually compare the retrieved digital photo with the face, either directly or remotely via a CCTV image, of the cardholder.”

Temporary Access Cards and Identification Badges
Temporary access cards or temporary identification badges are used in some buildings to control the entry of visitors, including vendors and contractors.

Access cards can be programmed to permit a visitor to access certain areas of a building (for example, a particular floor) during a particular time frame. After the authorized time period has passed, the card cannot be used again to gain access.

Temporary identification badges can vary from self-adhesive or clip-on paper badges to more sophisticated light-sensitive badges that expire automatically in one day, one week, or one month and thereby prevent unauthorized reuse. The latter change color to alert that the badge’s authorized time frame has expired.

Biometric ID System–Operated Locks
In modern high-rise buildings, biometric ID system–operated locks may be part of electronic access control systems in very specialized areas (and in some major buildings, to control access to the building itself). Biometric ID system–operated locks work on the principle that people have certain biological characteristics unique to each individual. These characteristics may include fingerprints, hand geometry, signatures, voice patterns, facial recognition, and iris and retina patterns. The biometric ID system checks this physical characteristic and if, after checking, the specific characteristic is verified within the system, a second signal activates a locked device, allowing entry.

At present, biometric ID systems may be susceptible to errors such as rejecting a person authorized to have full access and permitting access to a person whose access is not authorized. Part of the problem lies in the fact that over time, human biological characteristics change. These changes may be due to weight loss and gain, physical

injuries, extended periods of prolonged usage, tiredness, and stress. A possible solution to this problem may be the development of biometric ID systems that operate on more than one personal characteristic. Also, biometric ID systems are presently more expensive than the conventional card access systems and do not have the ease of user operation that the simple presenting, inserting, or swiping of a card affords. A possible solution for use as a conventional door/gate access reader for a high-security application is a station that integrates multiple technologies (Figure 5–46).

Building Telephone or Voice-Over Internet Protocol Door Entry Systems

A building telephone entry system (Figure 5–47) or a voice-over Internet protocol (VoIP) entry system can allow communication by a person seeking entry outside a residential or apartment building to building management, building security, or directly to an individual apartment using a telephone line or a VoIP. The person receiving the request can then remotely operate the building entry door to allow the guest to enter the building.

Turnstiles

Turnstiles are used to prevent or control pedestrian traffic, particularly in office building lobby areas. As O'Leary wrote, 75

> Because waist-high turnstiles do not actually create a total physical barrier, they generally are considered as low- to medium-security devices.... There are three types of turnstiles [Figure 5–48] currently used in facility security: tripod,

---


---


**Turnstiles are usually used in buildings to limit pedestrian travel in one direction and may also be used to collect admission fees.
FIGURE 5-47 Building telephone entry system. A person can directly dial a resident’s code and request entry. Such a system has two extra relay outputs that can be used in a variety of ways, including turning on a lobby light or unlocking an interior door by tone commands from the resident’s location or based on an access granted decision. Courtesy of Keri Systems EntraGuard Telephone Entry System (www.kerisys.com).

proprietary barrier and optical. Tripod types come in a wide variety of shapes and sizes to suit virtually any application. Tripod turnstiles all use a three-pronged barrier wheel, which rotates as the user’s leg presses against it to allow passage. Proprietary barrier turnstiles include gates [and “pop up” barrier arms] and the devices which are generically referred to as turnstiles, but which may not turn at all. Optical turnstiles offer no physical barrier, but offer a route for pedestrian traffic and may be used for monitoring traffic flow, to provide signaling or may be part of a facility’s management system which provides metal detection and loss prevention, [and] reads access cards.

Any waist-high turnstile can perform in a high-security application depending on the system designed around it and the personnel operating the facility. The turnstile can be used in a variety of modes: controlled entry/no exit, controlled entry/free exit or controlled entry/controlled exit.

Turnstiles typically are connected to access control, remote release and remote monitoring equipment to cause them to control access, control egress or report traffic flow rates. Options include: time-out relay, red and green indicator lights, extended arms, remote release button, out-of-use lock and electronic key bypass.

The most common type of turnstile deployed inside high-rise office building lobbies is waist high. In these building lobbies with high pedestrian traffic and the need for controlled access, multiple optical turnstiles located near building elevators can be very effective. Authorized tenants can effortlessly pass through the turnstile using a proximity access card. If an invalid card is used or a person attempts to pass through the turnstile without an authorized card, an audible signal will sound and supervising security staff can stop the individual concerned and question them as to their right to enter (or, additionally, CCTV cameras can be programmed to signal if someone jumps over the waist-high turnstile). Once the person has passed through the turnstile, he or she can then proceed to an access card-controlled elevator for travel to the authorized floor. Using a turnstile as a primary means of access control helps alleviate the problem of an unauthorized person proceeding directly to a building elevator car and then tailgating behind an authorized person to gain access to upper floors.

Rapid Entry Systems

Before leaving the subject of access control systems, it is important to discuss the availability of building and elevator keys for fire department use during an emergency situation. Having to force entry to locked buildings slows down emergency personnel response time, and doors may be unsecurable after the incident due to damage caused at entry. Essential building keys should therefore be readily available to a responding unit when arriving on site. If building staffs, such as security or engineering personnel, are not available to meet the responding agency, it is necessary to provide an alternative means to access the site and building and move freely through it. One possible solution

*Full-height turnstiles are usually used to control pedestrian traffic in areas where security personnel do not directly monitor their operation.

**Much of the information in this section was provided by Knox System, a supplier of rapid entry systems (Knox System. A Guide to Professional Rapid Entry. Newport Beach, CA: The Knox Company; 1998).
is for the fire department to be in possession of the essential keys for buildings to which they may be required to respond. For most city fire departments, however, it is virtually impossible to manage and control effectively the thousands of keys that could be involved.

In buildings across the United States, this critical issue of key control is accomplished by way of a fire department rapid entry system, namely a rapid entry key vault or fire department lock box (Figure 5–49). Selected building keys, access control cards, and, depending on the size of the selected container, the building emergency procedures manual, a list of key building personnel contacts, building floor plans, and hazardous material safety data sheets may be stored in these specially designed, weatherproof, fixed steel encased boxes and vaults. They are usually installed in a conspicuous location on the exterior vertical wall of the building.
To help prevent tampering, the lock box usually will be situated more than six feet (1.8 meters) above the ground and securely mounted on the surface or recessed into the building wall. In some buildings, the rapid entry box or vault will be equipped with an alarm tamper switch connected to the building intrusion detection system. These boxes and vaults are all fitted with the same specially designed master key, supplied free ahead of time to the local fire department. The key is secured to fire department primary response vehicles and ambulance or paramedic units, and its use is strictly controlled. Such an arrangement can also reduce liability on the part of building owners and managers because building keys that are only needed during a fire are well secured and do not need to be left in the custody of building personnel.

Property Control Systems

There are various security systems and equipment that can be used to store and protect property.

Safe Rooms

Safe rooms are “shelters that may be constructed outside or within dwellings or public buildings. These safe rooms will protect occupants from a variety of hazards, including debris impact, accidental or intentional explosive detonation, and the accidental or intentional release of a toxic substance into the air. Safe rooms may also be designed to protect individuals from assaults and attempted kidnapping, which requires design features to resist forced entry and ballistic impact. This covers a range of protective options, from low-cost expedient protection (what is commonly referred to as sheltering-in-place) to safe rooms ventilated and pressurized with air purified by ultra-high-efficiency filters. These safe rooms protect against toxic gases, vapors, and aerosols (finely divided solid or liquid particles).” Safe rooms may also be used to protect occupants against natural disasters such as tornadoes, cyclones, hurricanes, and typhoons.

According to Knowles and Levy,

While details of safe room construction are usually private, safe rooms typically include:

- Independent phone line(s).
- A back-up generator.
- Independent, isolated ventilation and drainage.
- Oxygen scrubbers to replenish the air supply.
- Closed-circuit television monitors.
- Computer(s) with independent Internet connection.

Information on the design of safe rooms can be found in FEMA 453, Design Guidance for Shelters and Safe Rooms. (FEMA Risk Management Series, Washington, DC, May 2006) and other shelter publications such as the American Red Cross (ARC) 4496: Standards for Hurricane Evacuation Shelter Selection, FEMA 320. Taking Shelter from the Storm: Building a Safe Room inside Your House, and FEMA 361. Design and Construction Guidance for Community Shelters. Information on nuclear explosions and shelters that protect against radiological fallout may be found in FEMA TR-87, Standards for Fallout Shelters.

A control panel (or computer terminal) that allows operation of all security systems and electronic locks.

Access doors with electronic locks and mechanical back-ups.\textsuperscript{77}

**Filing Cabinets, Key Cabinets, Safes, Safe Deposit Boxes, and Vaults**

Office, hotel, and apartment buildings may contain various filing cabinets, key cabinets, safes, safe deposit boxes, and vaults used to store and protect papers, files, documents, and computer software; facility keys; cash, checks, bonds, precious metals, and jewelry; and other items of high value or sensitivity. The protection afforded may not only be against security threats, such as burglary, but also against safety threats, such as fire.

It is important to realize that burglar-resistant containers are not necessarily fire resistant, and vice versa. On occasions, irreplaceable documents have been stored in safes that offer strong resistance to a would-be thief, only to have the items perish in a fire. Similarly, valuable items such as cash and jewelry have been stored in safes that were designed to resist the high temperatures of fire but that offered no resistance to an enterprising burglar. The ideal solution may be a container that is burglar resistant and built into a fire-resistant receptacle. The degree of protection depends largely on the value of the planned contents of the filing cabinets, key cabinets, safes, safe deposit boxes, and vaults. This section is not an in-depth of these storage containers. However, mention is made of a common storage container found in many hotel guest rooms (i.e., in-room safes).

**Hotel Guest In-Room Safes**

Some hotel guest in-room safes use a digital keypad system, needing a unique combination\textsuperscript{*} to open and close it (Figure 5–50), or a security key,\textsuperscript{**} which can only be removed from the safe after the door is closed and locked. Others are opened with a keycard or a credit card. Some safes have an interrogation feature that permits tracking of historical usage,\textsuperscript{78} including some whose locks can be accessed remotely by hotel staff using an online system.

**Metal Detectors and X-Ray Systems**

**Screening People and Property**

Metal detectors and X-ray systems, although not commonly used in high-rise buildings, are deployed in sensitive facilities such as high-profile building complexes, signature buildings, courts and other government facilities, and for special events requiring screening people and property (mainly for guns, knives, and explosives concealed on people and contained in packages and other containers).


\textsuperscript{*}"Establish a policy for changing the master code in a timely fashion when an employee with access to the master leaves the company for any reason, or any other time the confidentiality of the master code could have been compromised" (Barth S. The value proposition of in-room safes. Lodging Hospitality. Cleveland, OH; November 2004;60(15):40).

\textsuperscript{**}"If using mechanical key safes, use a high-level security key that can’t be duplicated and that has an infinite number of keyways" (Barth S. The value proposition of in-room safes. Lodging Hospitality. Cleveland, OH; November 2004;60(15):40).

\textsuperscript{78}Barth S. The value proposition of in-room safes. Lodging Hospitality. Cleveland, OH; November 2004;60(15):40.
“Metal detectors [or magnetometers] work by generating an electromagnetic field and then measuring changes in that field caused by the presence of metal objects. Newer metal detectors can direct operators to the area of the body where a gun or knife might be hidden.” 79 Metal detectors can be hand-held wands or walk-through types.

“X-ray machines work by applying controlled voltage and current to the X-ray tube, which results in a beam of X-rays. The beam is projected on matter. Some of the X-ray beam will pass through the object, while some are absorbed.” 80 X-ray machines can be used to examine hand-carried items, pallet-sized ones, or entire vehicles.

The type of tenancy and pattern of use of a building influence whether such security measures are appropriate. For example, the 25-story-high New York Municipal Building in Manhattan houses 5000 employees, including prominent city officials and city agencies. Due to the threat of violence,

Visitors entering the main lobby of the building must pass through a Metorex walk-through metal detector that incorporates LEDs that indicate an area of a person’s body that may conceal a weapon. “The use of the walk-through has minimized the use of metal detecting wands because they can pinpoint an area in question. Now, wands are used only to confirm the presence of metal,” says director of security, James J. Darmos. Items carried by visitors are put through Heimann Systems High Scan x-ray equipment.

79 Alonso-Zaldivar R. Metal detectors will take center stage in new era. Los Angeles Times. Los Angeles, CA; June 14, 2002:A20.
X-ray machines are also used in the mailroom. The machines can zoom in on an object within a package and exhibit densities in black-and-white and color.\textsuperscript{81}

An added layer of protection is to combine a metal detector with an access control system. According to Scott Dennison, director of CEIA USA, “This allows for metal detection and hands free access control in a single unit, enabling the user to have an extremely high flow rate while dealing with the threat of workplace violence.”\textsuperscript{82} “We’ve developed a technology that will read an access control card as the person is walking through the metal detector,” he said. “It verifies that not only does the person not have a weapon, but they are also authorized to be in that facility.”\textsuperscript{83}

In planning the installation of metal detectors and X-ray machines, it is important to analyze traffic patterns and select equipment that can accommodate the expected traffic and avoid compromising the security objectives or creating traffic jams. According to Scott Dennison,

\begin{quote}
Security should begin by calculating the number of persons expected to enter during each half-hour increment and reviewing the type of personal articles that entrants will bring with them. Then, security should determine how many metal detectors and x-ray machines will be required to handle this traffic flow, factoring in a cushion of about 25 percent. (The processing rate of a single-lane, walk-through metal detector and x-ray machine ranges from 300 to 600 persons per hour.)

The number of metal detectors and x-ray machines should be based on the estimated flow rate of entrants and the established acceptable waiting time.

The correct number of security screening personnel required to operate the equipment can be ascertained at this point. [A walk-through metal detector and X-ray machine requires four-persons: one for the metal detector, one for the X-ray machine, one to carry out inspections with a hand-held wand, and one to carry out physical bag inspections, when required.] It is also important to develop a floor plan that accommodates entrants who will need a place to line up for processing.\textsuperscript{84}

Training and periodic checks of the efficiency of the screening personnel in detecting certain objects are critical. “Detection equipment is only as good as the employees who operate it. Personnel must be trained properly, and equipment stations must be staffed with sufficient personnel. Poor training or understaffing will undermine the effectiveness of the screening process.”\textsuperscript{85}
\end{quote}


\textsuperscript{82}Metal detectors meet multiple need. Access Control & Security Systems. Atlanta, GA; December 2000:27. Comments by Scott Dennison, director of CEIA USA, Twinsburg, OH.

\textsuperscript{83}Metal detectors add shapes, sizes, features, and functions. Security. Highlands Ranch, CO; August 1998:26. Comments by Scott Dennison, director of CEIA USA, Twinsburg, OH.

\textsuperscript{84}Dennison S. Developing the right sensitivity to weapons. Security Management. Alexandria, VA; August 1998:38.

\textsuperscript{85}ibid, p. 43.
Screening Vehicles and Containers
Entire vehicles, including large trucks and containers, can be X-rayed to reveal any hidden explosives, plastic weapons, or drugs. AS&E’s cargo and vehicle inspection system is noninvasive and uses an X-ray source mounted in a truck. Such a device can be effective in providing photo-like X-ray images for detecting explosives and weapons before a vehicle is permitted entry to an under-building parking garage and loading dock/shipping and receiving area.86

Asset Tracking Systems
Small radio frequency identification (RFID) asset tags—some being embedded into desktop and laptop computers at the time of manufacture—can be assigned to an asset that is authorized to leave a high-rise building. Integrated with a building’s access control system, asset tracking can be utilized to control the movement of primary assets from a building. “Prime assets tend to be IT [information technology] assets because they tend to be portable and have intrinsic high value for themselves and for the information they contain.”87

The following describes an asset tracking/access control system in the lobby of a prominent 39-story Manhattan high-rise office building.

An access card is assigned to tenants of the facility with normal access levels and work shifts. The card is encoded with the tenant or employee name and other information. Also assigned are small tags for assets permitted to be removed from the building. These asset tags are encoded with a serial number and the owner’s name, department and telephone number.

Initially, all asset tags are assigned a zero access code, with no privilege for egress. When assigned, the tags are programmed into the system along with the cardholder or escort who is permitted to remove the asset from the facility. The loop [RF (radio frequency) signal] readers read card and tag at the same time, and the system checks to see if the two tags have been linked, records the movement and triggers an alarm at the security desk if the removal of property is unauthorized. The name of the person carrying the asset, the serial number of the asset and owner’s name and extension appear on the PC screen at the security desk.

All movements through the glass doors [in the main lobby] are recorded on the software system, by time and by employee and asset codes. The CCTV system keeps a visual record that is also date- and time-stamped.

87 Comments by Don Small in Asset management, tracking are access issues. Security. Highlands Ranch, CO; July 2000:27.
A security or facility manager can also keep track of assets throughout the building’s interior. By installing the loops at selected doors, assets can be tracked by department, user’s name or asset serial number.\textsuperscript{88}

Such a “hands-free” asset tagging and tracking system “allows free egress when authorized assets are removed, but prevents unauthorized removal of property. Without electronic tracking, assets can be removed by concealing them in a briefcase, package or gym bag.”\textsuperscript{89} This system can also be adapted to screen assets being mailed out of a building through a central shipping area such as the loading dock.

**Intrusion Detection Systems**

Various types of intrusion detection systems (IDSs) are available to enhance the quality of security provided for a building’s perimeter, public access or common areas, maintenance spaces, and other interior areas.

An IDS is designed to deter (intruders may be deterred by posted warning signs), detect (an imminent or actual security violation), delay (by activating physical security measures such as locks and barriers), and respond (by indicating where an intrusion has taken place).\textsuperscript{90}

Basically an intrusion detection system detects when an unauthorized intrusion has occurred in an area and transmits an alarm signal. (A signal may also be sent when the person setting an alarm system fails to do so correctly or inputs a predetermined code that indicates he or she is under duress and needs assistance.) The signal may be transmitted to sound a local alarm—such as a bell, a horn, a siren, or a whooper—at or near the protected area. It may be transmitted to an onsite monitoring location staffed with operators trained to carry out a predetermined alarm response procedure, or to an offsite central station\textsuperscript{H17004} likewise staffed with personnel trained to notify the appropriate agencies.

**Onsite Monitoring**

In the high-rise building, the onsite monitoring location may be the local annunciator and control panels built into an open-style desk arrangement or a more complex and sophisticated security command center, both of which often will be located in the building’s main lobby. In the case of onsite monitoring, when an intrusion alarm is activated, security staff will either investigate the reason for the alarm themselves or notify the appropriate law enforcement agencies. If the intrusion alarm involves a tenant space or apartment, a prearranged notification procedure should be carried out.

---


Offsite Monitoring

In the case of offsite monitoring, once notified of an intrusion alarm, the central station staff will either notify security staff at the building, dispatch a responding agent such as a patrol officer, or notify the appropriate law enforcement agency and request a response to investigate the alarm. In addition, the central station staff may also directly notify building management or the appropriate building representative of the incident. The specific response procedures should be preplanned and documented.

Intrusion Detection Components

An intrusion detection system consists of three basic components: a sensor, a control unit, and an annunciation device.

Sensors

Sensors are installed in the area being protected. The types of sensors that may be found in high-rise buildings are described in the following sections.

Pressure Mat or Pad Detector

Pressure mat or pad detectors are, in effect, simple switches that either react to pressure when it is applied to them or react when normally applied pressure is released. They may be in the form of a strip or a mat. In some locations—for example, inside tenant offices and apartments—they may be secreted under carpeting with the associated electrical wiring concealed from view.

Magnetic Contact Switch

Magnetic contacts are reliable, simple devices consisting of a permanent magnet attached to a door (and, in some applications, to openable windows) and a magnetically operated switch attached to the frame. The magnet may be surface mounted and visible or flush mounted and concealed. The switch operates by means of a magnetic field generated when the door or window is closed. If the door or window is opened, the magnetic field is interrupted and an alarm is initiated. Magnetic contact switches are effective devices, but bridging or jumping the circuit can defeat surface-mounted ones. These switches are commonly used in high-rise buildings for exterior doors (particularly stairwell exit doors leading outside of a building), interior doors (particularly stairwell doors and doors leading to maintenance areas), and interior doors leading to offices, apartments, and other sensitive areas. These devices are useful for monitoring intrusions into building stairwells.

Electrical Switch

Electrical switches are installed in a similar fashion to magnetic contact switches. However, in this case, they consist of electrical contacts. They operate on the principle that an electrical circuit is completed when a door or window is closed and the contacts come together. If the door or window is opened, the electrical current is interrupted and

an alarm is initiated. As with magnetic contacts, electrical switches can be defeated by bridging or jumping the circuit.

**Break-Wire System**

Very fine, electrically conductive wire configured in the form of a screen or a criss-cross arrangement across an opening can be used to detect intrusion. When the wire is broken, the electrical circuit is severed and an alarm is initiated. Such an arrangement can be useful in protecting building exterior openings such as those leading to HVAC air intakes. The wiring system also can be modified, using magnetic contact switches to detect movement of the wiring assembly without the wire actually breaking. Accordingly, an alarm will be initiated to notify monitoring staff of the intrusion.

**Vibration Detector**

A vibration detector utilizes microphones to detect audio noise. The sensitivity of the detector can be adjusted to initiate an alarm when it detects vibrations such as those resulting from forced entry. It can be installed on surfaces—walls, ceilings, floors, and doors—and objects such as works of art, files, safes, cabinets, and vaults. Although vibrations of the building and equipment contained within it can lead to false alarms, these false alarms can be reduced by adjusting the sensitivity of the vibration detector system.

**Capacitance Detector**

Capacitance detectors operate using an electromagnetic “barrier.” On application of a small electrical charge to a metal object, an invisible electromagnetic field is set up around the object such as a file, a safe, a cabinet, or a vault. If something intrudes into the field, an alarm will be initiated. When this device is in use, it is vital to properly ground the object being protected.

**Passive Infrared Detector**

Instead of emitting a signal or a field that can be disturbed by an intruder, passive infrared (PIR) detectors are passive or inert and operate on the principle that human beings emit heat, in the form of infrared radiation, from their bodies. When an intruder moves within the range of the detector, an alarm is triggered by the very small, but detectable, variations in heat caused by the intruder’s presence.

The proper location of the passive infrared detector is critical because false alarms can be caused by sunlight and heating, ventilation, and air-conditioning (HVAC) systems. In high-rise buildings, PIR detectors are also commonly used as automatic door openers, particularly in heavily traveled public access or common areas such as building lobbies.

**Ultrasonic Motion Detector**

Ultrasonic motion detectors operate on the principle that a space can be filled with inaudible sound waves. Using a transmitter, the device both sends and receives ultrasonic waves. If an intruder enters the protected space, the standing-wave pattern is disturbed and an alarm is initiated. Ultrasonic motion detectors can false alarm because HVAC systems discharge air into the protected space. In addition, noises (such as telephones ringing) within or outside the protected area can cause false alarms by disturbing the wave patterns.

---

*A false alarm occurs when a system detector indicates in error that there is an incident.*
Microwave Motion Detector
Microwave motion detectors have an operating principle similar to ultrasonic motion detectors, with the exception that high-frequency electromagnetic microwaves are transmitted into an area. If an intruder enters the protected space, the standing-wave pattern is disturbed and an alarm is initiated. Because microwaves can penetrate building walls, they may be used to detect movement outside of areas where the device is operating, but this feature can also lead to movements being detected that are not of consequence to the space being protected. Some tuning devices can circumvent these problems by restricting the area covered by the detector. Electric motors, fluorescent lights, or other devices that interfere with the detector by emitting electromagnetic waves can cause false alarms.

Video Motion Detector
Video motion detection allows a CCTV camera to be used as an alarm device. The underlying principle of operation is that the contrast change in a specific area of the image causes an alarm output. If motion occurs and the particular scene changes, the sensing device initiates an alarm to draw the viewer's attention to this fact, or it switches on a video-recording device to record the activity. "A video motion detector (VMD) is a device that analyzes the video signal at its input and determines whether its contents have changed and consequently, produces an alarm output." Video motion detection is an important tool when deployed in building stairwells and other sensitive areas.

Acoustic Detector
Acoustic detectors use a sensitive and accurate hi-fi microphone to detect noise created by an intruder attempting to gain entry to a particular area or moving within the protected space. Their use is usually restricted to vaults and other high-security applications.

Photoelectric Detector
When an invisible beam of light projected from the transmitter of a photoelectric detector to its receiver is interrupted, an alarm is initiated. Various patterns of the photoelectric beam can be devised, and mirrors can be used to deflect the beam around corners. An obvious method an intruder can use to circumvent the system is to climb over the beam or crawl under it. Photoelectric detectors tend to be used more frequently in outdoor applications.

Dual-Technology Motion Detector
A dual-technology motion detector combines the use of two technologies in a single device. The initiation of both technologies is required before an intrusion is signaled. Such a device can help eliminate false alarms.

Control Unit
The sensors are linked, usually electrically, to the control unit. The control unit normally consists of circuitry installed in a metal enclosure. The cover of the unit often contains a key-operated switch that permits one to alter the signal(s) sent to the annunciation device and deactivate the sensor, thus permitting access to the protected area without an alarm signal being activated. A standby battery source normally is provided to furnish power in

---

case the primary electrical power source fails. Also, a tamper switch usually will be pro-
vided so that if the unit is interfered with, a signal is sent to the annunciation device.

Annunciation Device
On activation of a sensor, a signal is sent to the control unit, which in turn transmits a
signal to sound a local, audible alarm (such as a bell, a horn, or a siren) at or near the
protected area; transmits a signal to an onsite monitoring location (such as an open-style
desk arrangement or the security command center); or transmits to an offsite central sta-
tion. A combination of these signals is also possible.

Often in high-rise buildings, tenants and residents have their own intrusion detect-
ion systems, separate from the building’s systems. Usually offsite central stations moni-
tor tenant and resident’s systems. Sometimes, building owners and managers monitor
tenant and residence alarm systems within a building.

Duress Alarm Systems
A duress alarm (sometimes called a panic alarm) is “a device that enables a person
placed under duress to call for help without arousing suspicion.”\(^{92}\) These alarms come
in the form of switches and kickbars mounted underneath or on the side of a desk or
counter or on the floor. The assistance may be requested for security reasons such as
when the person feels threatened, is under attack, or has just been attacked, or for safety
reasons such as a medical emergency.

The switches operate through an electric current continuously running through a
circuit. When the duress alarm switch is activated, the current stops, resulting in the
initiation of an alarm at a remote location. The remote location may be another area
within the facility, the security command center, an offsite central station, or some other
location that is constantly monitored when the switch is operational.

In the security application, it is generally considered safer to transmit a signal that
does not sound a local alarm (such as a bell, a horn, or a whooper) at or near the pro-
tected area. Sudden noise around a person committing a robbery, for example, may lead
that individual to react violently.

In high-rise buildings, duress alarms may be found in reception areas (particularly
where executive offices are located) and cashier’s booths at entrances to parking garages
and lots. As with all security systems and equipment, the operation of duress alarms
should be regularly tested and this activity documented. Duress alarms are particularly
important because their activation usually indicates an emergency situation. It is criti-
cal that they operate as designed. Their construction should always include protective
guards or other design features to avoid accidental activation.

Security Mirrors
Although not security equipment per se, a convex mirror is a reflecting device commonly
found in parking garages and other areas where there are “blind corners.” Such a device

International; October 24, 2008.
extends the range of observation for a person looking into the mirror so that they can see around a corner and observe oncoming people or vehicles. These mirrors can also be installed immediately inside entrances to parking garages so that the driver of a vehicle entering the garage can observe any person who enters the garage on foot directly behind his or her vehicle (this is of particular value when vehicles enter garages with roller doors or gates that only open when authorized vehicles are entering and exiting).

**Lighting**

“Adequate lighting not only helps people recognize and avoid dangers, but also in many cases deters criminals by creating in them the fear of detection, identification and apprehension.”

If an attack should occur, it makes apprehension by security and law enforcement personnel more likely. It helps create a more secure atmosphere. It serves the purposes of safety by illuminating slip-and-fall hazards such as water puddles, pot-holes, and difficult-to-see steps.

Security lighting can complement and enhance other security measures such as physical barriers, stationary posts or mobile patrols, CCTV, and intrusion detection systems. (Super tall buildings, particularly those located near airports and in the path of approaching aircraft, may have red emergency lights installed on the roof and sides of the building to alert aircraft. For example, Burj Dubai in the United Arab Emirates has the “glass edges of the tower lined with red emergency lights to warn off aircraft.”) It also can be used for traffic signals and signs.

**Factors to Consider**

Consider these factors when selecting an appropriate lighting system:

1. Numbers and positions of light fixtures
2. Direction of light beams (often light will be directed toward walls, barriers, and the building itself)
3. Extent of illumination of particular areas (for example, security-risk locations such as parking garages will often require total rather than partial illumination)

---


*As suggested by Ralph Witherspoon, CPP, CSC, in “Parking lot and garage security.”

For safety and security, I recommend interior garage lighting should be a minimum of six foot-candles (measured both vertically and horizontally) throughout the garage, 24 hours per day. Sunlight seldom enters garage interiors, and cannot be relied upon for lighting. A minimum of 10 foot-candles is recommended at pedestrian entry/exit points, over driving lanes, stairs and elevator lobbies (out to a 30’ [9.1 meters] radius from the elevator doors). If the facility or its immediately surrounding area has a significant history of crime, or a recent history of violent crime, higher levels of illumination may be needed. Energy-efficient metal-halide lighting provides reasonable color rendition for CCTV and direct viewing. Interior walls and ceilings should be painted with a glossy or semi-glossy white paint to increase light reflection. This also increases the ability of parkers to observe movement and potential threats. Pillars and ramp corners should be painted in contrasting colors for driving safety. Lighting at the vehicle entry/exit points should usually be at least 30 to 50 foot-candles for safe transition from the garage to the exterior lighting. Garage owners/operators should discuss this with a lighting engineer.

Rooftop parking open to the sky should be illuminated to at least three foot-candles, as specified below for surface parking lots. Where possible, interior and exterior stairwells should be visible,
4. Type of lighting sources—incandescent, mercury vapor, metal halide, fluorescent and high- or low-pressure sodium vapor

5. Type of lighting equipment (continuous lighting is continuously applied to an outside area during periods of darkness; standby lighting is continuous lighting intended for reserve or for standby use or to augment continuous lighting; portable lighting is movable and manually operated and can be used to augment continuous or standby lighting; and emergency lighting duplicates any or all of the previous three types and generally operates during power failures)

6. Method of activation of the light fixtures (manual or automatic using a timer or photoelectric cell system)

7. Recommended minimum illumination levels for areas such as pedestrian walkways, building and vehicle entrances, and inside parking garages, as may be required by local ordinances

For exterior lighting, consideration also must be given to protecting the light fixture from weather and vandalism. When making recommendations regarding lighting, a qualified lighting engineer should be consulted.

**General Types of Lighting**

The descriptions of the general types of lighting sources that follow were adapted from the chapter titled “Security Lighting” in the *Handbook of Loss Prevention and Crime*. 95

**Incandescent**

Incandescent lamps are common and relatively inexpensive; glass light bulbs become luminous (i.e., emit light) through the action of an electric current on a material called a filament. They produce very good to excellent color rendition (color rendition affects one's ability to discriminate, grade, or select colors and to determine whether colors will appear

---

316

HIGH-RISE SECURITY AND FIRE LIFE SAFETY

natural), providing warm, white light. They are relatively short in rated life (500 to 4000
hours) and low in lamp efficiency as compared with other lighting sources. These lights are
generally for interior use and have largely been replaced by fluorescent lights in buildings.

Mercury Vapor
Mercury vapor lamps emit a purplish white color because of the action of an electric
current passing through a tube of conducting and luminous gas. They are considered
more efficient than incandescent lamps of similar wattage, have widespread application
for exterior lighting, and produce good color rendition. They are used for street lighting and are commonly used as security lighting in parking lots. They have a long life
(24,000 hours) and are used where long burning hours are required. The time needed
to light these lamps once they are switched on is considerable. However, once illuminated they can tolerate substantial dips in electrical power.

Metal Halide
Metal halide lamps are similar in physical appearance to mercury vapor but provide a
light source of higher luminous efficiency and better color rendition. Therefore, fewer
fixtures are required to light the same area as mercury vapor lamps. The rated life
(6000 hours) is short when compared with mercury vapor lamps. They are used where
the burning hours per year are low and color rendition is of utmost importance. As with
mercury vapor, the time to light these lamps once they are switched on is considerable.
However, once illuminated they can tolerate substantial dips in electrical power.

Fluorescent
Fluorescent lamps are large, elongated bulbs that have a long rated life (9000 to 17,000
hours) and high lamp efficiency, and they produce good color rendition. They cannot project light over large areas and may have a decreased efficiency at low ambient
temperatures. Because of the latter, they have limited value in colder climates for outdoor use. Compared with incandescent lamps, their initial cost is higher, but they have
a lower operating cost because they require less electrical power to emit an equivalent
amount of light. Fluorescent lights provide ample illumination for safe working conditions. They are commonly used as interior lights in modern buildings.

High-Pressure Sodium Vapor
High-pressure sodium vapor lamps are discharge lamps that are similar in construction
to mercury vapor lamps but emit a golden-white to light pink color. The cost of the
light fixture is high, but the cost of operation is low. They have a long life (up to 24,000
hours), produce relatively good color rendition, and are used for the exterior lighting of
parking areas, roadways, and buildings.

Low-Pressure Sodium Vapor
Low-pressure sodium vapor lamps are discharge lamps that are similar in operation to
mercury vapor lamps but produce poor color rendition. They emit a light yellow color,
and their maintenance of light output is good throughout their rated life. Their expected
life is good (up to 20,000 hours), and they operate at a low cost (equivalent to that of
high-pressure sodium vapor lamps). Previously they were widely used in urban centers.
They are now most common on major highways.

safetymessage.com


Light-Emitting Diodes (LEDs)
A light-emitting diode (LED) is “a semiconductor diode that emits light when an electrical current is applied in the forward direction of the device, as in the simple LED circuit. The effect is a form of electroluminescence where incoherent and narrow-spectrum light is emitted.”96 It can be used for traffic signals and exit signs. “Exit signs that employ LEDs (light-emitting diodes) as a light source have a significantly longer lifespan than conventional lights and present less chance of failing at a critical time. In addition, the use of LEDs provides uniform illumination—which testing has shown increases visibility and readability.”97

Appropriate Light Selection
“The important thing to remember is to make the light selected best fit the need or purpose.... If a parking lot is very large, and many fixtures are required, the priority should be a long lasting bulb with good maintenance (higher mean time between failures) and low replacement costs.”98 Also, if the light is to be used for CCTV cameras, the lower the available minimum ambient lighting level is, the more expensive will be the camera required to produce images of reasonable clarity and definition. The extra cost invested in the lighting system can result in an overall cost reduction because a less expensive camera may be able to be used.

When used in public restrooms (particularly those in parking garages), “lights should be permanently wired on, or they should be tied to motion detectors to give light whenever people are inside the rest rooms.”99

Communication Systems
Various forms of communication systems are available for use in high-rise buildings and interior areas, as described in the following sections.

Telephones
Telephones (fixed position and mobile) are an essential communication tool within a high-rise complex. Telephones located in the security command center should be sufficient to handle daily operations plus the extra demands placed on them when building emergencies occur. Important telephone numbers, particularly those of emergency services (fire department, police department, emergency medical services, etc.), may be programmed into many telephone systems for speed dialing. In selecting a telephone system, it is important to consider whether the system can operate in the event of an electrical power failure.

Mobile cellular telephones have application in large high-rise complexes because by their very nature they afford mobility to the user. However, losing phone connections in under-building parking garages and elevators is a problem.

As with most systems, telephones are subject to misuse. The primary misuse is unauthorized calls, including those to pay-per-minute services. Arrangements can be made with the telephone company to screen out and block certain numbers so they cannot be dialed without an authorized code.

**Portable Two-Way Radio Systems**

Portable two-way radios (sometimes called hand-held radios or walkie-talkies) are another essential communication tool within a high-rise complex. All two-way radios have two major components: the transmitter that converts sound waves into inaudible RF energy that is broadcast over the air and the receiver that converts the inaudible RF energy into sound that can be detected by the human ear. The following information was obtained from the American Protective Services *Tools for Security Training Course* and Motorola.

**Transmitter and Receiver**

For transmitter control, most radios have a “mic key,” or “press-to-talk switch,” used to turn off the receiver and activate the transmitter. Receiver controls are more diverse. A “volume knob” is used to adjust the level of sound that is heard but has no effect on the loudness of transmissions. The “squelch knob” is used to adjust the sensitivity of the receiver to incoming signals and acts like a filter. A common way of adjusting it is to turn it down until a rushing noise is audible and then to turn it up just until the noise stops. The “PL,” or “private line switch,” is used to limit a signal received to only that from radios that have the same crystal. The “channel selector” is used to select the frequency the radio will use to transmit and receive the radio frequency energy. In some buildings, radios with multiple channels are provided—one for the exclusive use of security staff; one for engineering staff; other ones for staff that may include janitorial, housekeeping, and parking personnel; and one designated for use during emergencies only.

**Base Station**

A base station, often located in the security command center, should be able to broadcast to all frequencies. The specific controls and their location on the radio will vary from manufacturer to manufacturer and model to model.

**Use of a Repeater**

Because of the large amounts of concrete in high-rise structures, it is vital that the radio communication system selected has adequate power and quality to facilitate audible and clear communication to all normally occupied areas of a building. Usually in high-rise buildings a repeater is added to the radio system to enhance radio coverage. A repeater is “a radio device that retransmits received signals for the purpose of extending transmission distance or overcoming obstacles.” The repeater consists of several basic components—a receiver, a transmitter, circuitry linking the transmitter and receiver, and

---


either one antenna or two antennas and a duplexer (a duplexer permits a single antenna to transmit and receive at the same time). An antenna is a conductor used for transmitting or receiving electromagnetic radio waves. The repeater’s antenna is usually located on the roof of a building and permits inexpensive, low-powered radios to communicate with each other over greater distances.

**Pagers**

A pager or a beeper is a pocket-sized electronic device useful for notifying the person carrying it of a telephone message. Notification is by way of a high-pitched audible signal or by vibration. Particularly useful are pagers that display alphanumeric text messages.

Paging systems can be effectively integrated with security and fire life safety systems. For example, the access control system at a facility can be set up so that “when an alarm comes in, it can be simultaneously sent over pagers carried by security personnel.”

Paging of groups of people can be an effective means of communication when many individuals need to be simultaneously informed of an event, particularly of an emergency situation.

**Public Address Systems**

A public address system (PA) is a one-way system for communicating from the fire command center to the occupants of a building. It should have adequate power and speaker quality so that, in all normally occupied areas of the building (including elevator cars), voice messages can be clearly and distinctly heard. Each PA system is different, depending on the manufacturer and system models. Usually the system functions with the operator manually selecting the required zones (ordinarily, separate paging zones will be designated for each floor and for stairwells and elevators) and speaking loudly and clearly into a microphone that connects to these areas. The capability for communication to individual floors or the whole building at once is often provided.

**Intercom Systems**

An intercom is a two-way communication device that enables communication from the security command center or other constantly monitored area to specified locations throughout a building. These locations may include elevators, stairwells (for occupants who are inside the stairwell), passenger elevator lobbies, at the stairwell door(s) leading to the roof, at certain access card readers, and at various outside locations and in parking structures and lots.

Intercoms usually are mounted on walls, columns, or bollards and may be operated by the occupant simply pressing a button and speaking while the button is depressed or speaking hands-free after the button has been pressed to activate communication. This action initiates a signal at the monitoring location and should identify the station from which the call originated. If the button is pressed and no answer is received from the originating station, security operations often require staff to be dispatched immediately.

---

to that location. The intercoms should be clearly visible, particularly those in parking areas, and should have their number and location distinctly marked on them, along with written instructions as to how to operate them.

Intercoms in parking structures are primarily used to help those requesting emergency assistance due to a security problem or a medical condition and, possibly, lost persons.

Many facilities include phrases such as “SECURITY ASSISTANCE,” “EMERGENCY INTERCOM,” or “EMERGENCY CALL STATION” printed in bold letters on signs at each intercom location. For safety and identification purposes, some intercom systems have distinctive flashing lights that activate at the station that is in use. Others are integrated with the CCTV system so that, on activation of an intercom station, the appropriate camera will be automatically called up for the operator who is monitoring the system. (See also Chapter 6, “Emergency Call and Assistance Stations”).

Intercom systems may be hard wired, use a telephone line, or a voice-over Internet protocol (VoIP).

Megaphones or Bullhorns
Megaphones or bullhorns can be important communication tools, particularly if the public communication system in a building fails to operate. They can also be of great value in communicating with large groups of people inside, or congregated together outside, the building.

Speakers and Microphones
A two-way voice communications system from the security command center to speakers and microphones located at sensitive areas, such as stairwells, can be a valuable tool for security and life safety. If there is a problem in a remote area, security staff can handle it immediately by communicating to that location. Used in conjunction with CCTV, speakers, and microphones (although the use of microphones and listening devices is prohibited in some cities) can be an effective part of the total security system. If, for example, security staff members observe a crime in progress while monitoring camera images, they can use the speaker system to communicate to that area and possibly thwart the crime. This combination of CCTV and speaker systems has been effective in exterior parking areas where potential car thieves were successfully warned off before they had the opportunity to carry out their intentions.

Personal Data Assistants
Personal data assistants (PDAs) provide a compact, portable means of maintaining and organizing information, as well as a mobile means for monitoring security systems.

Mass Notification Systems
Mass notification systems (MNSs) are used during emergencies to supply real-time information and instructions to occupants or emergency personnel within a building or multiple buildings. Such systems may be integrated with security and fire systems and can deliver

---

104 Adapted from *Unified Facilities Criteria (UFC) DoD Minimum Antiterrorism Standards for Buildings* (UFC 4-010-01, July 31, 2002:A-3, B-12).
voice or text messages through devices that include telephones, radios, pagers, PA systems, intercoms, speakers, mobile phones, computers, and PDAs. In addition to these communication systems, there may be fire department voice communication systems, scanners, and other like devices. It is critical that all essential communication systems are provided with backup power to ensure their continued operation during an electrical power failure.

Closed-Circuit Television Video Systems

Closed-circuit television video system, abbreviated as CCTV and sometimes called closed-circuit video, involves the transmission of scenes or moving pictures from a video source, such as a camera, by conversion of light rays to electronic signals, which are transmitted via coaxial cable, fiber-optic cable, or twisted pair wire (hence the terminology “closed-circuit”) or by microwave links, infrared wireless transmission, radio frequency (RF) wireless transmission, telephone lines, networks, and a host of other methods to specific receiving equipment such as a video display monitor or a video-recording device.

“Modern camera systems are not always a true closed-circuit system, although they are still referred to as such. Many new devices, such as wireless transmitters, Web cameras, and camera servers, are being added to camera systems now. These devices allow people with the proper knowledge and/or equipment to receive the video images from the camera without being directly connected to it. Although theoretically this is not a closed-circuit system, it has drastically expanded the applications and usefulness of video surveillance systems.”

As more and more equipment was invented to enhance the CCTC system, the system’s role gradually changed. Today video is used in virtually every type of facility, and in many cases has become a necessity. With all of these changes and advances in the video industry, it is still important to keep the primary purpose of the camera system in perspective. A camera system cannot protect people from crime. Cameras cannot protect property from theft or vandalism. The camera is merely the silent observer, watching what it has been set up to watch. The recording device is there to gather and store information, primarily for future use as evidence if needed—evidence for a court of law if necessary or company evidence for confronting dishonest employees or patrons should that need arise. Camera systems are merely a tool that,
when set up properly, can detect activities. These activities must still be interpreted by a human being, who can then take whatever actions may be necessary as a means of response.\textsuperscript{106}

CCTV systems are used extensively in high-rise buildings. As with other security systems and equipment—such as physical barriers and locking systems and lighting and intrusion detection systems—CCTV is part of the basic security measures that make up the total security program. CCTV can amplify the range of observation of security staff. It can alert them to incidents that need a response and provide a permanent record of incidents for later evaluation and possible use as evidence. CCTV systems can be interfaced with other equipment such as intercoms and intrusion detection devices.

The following sections address some of the basics of video systems.

Area Observed and Ambient Lighting Levels

Illumination is a critical factor in the quality of the CCTV picture. For exterior- and interior-mounted cameras, it is essential that adequate levels of useful light be available (whether it be sunlight, moonlight, starlight, or an artificial source of illumination such as various types of lamps). For nighttime viewing, infrared lighting may be more cost-effective than traditional security lighting. For all cameras, it is essential that not only adequate levels of useful light be available, but also that the light be compatible with the type of image sensor contained in the camera.

Camera and Lens

The camera is the device that facilitates the conversion of the image, produced by the lens, to an electronic signal for transmission via coaxial cable, fiber-optic cable, or other means, to the remote video monitor or video recording device. The lens is an “optical device for focusing a desired scene onto the imaging device”\textsuperscript{107} in a camera.

Lenses come in different sizes that allow choices for the area view. Each lens has a specified focal length (FL). FL is “the distance from the lens center, or second principal plane to a location (plane) in space where the image of a distant scene or object is focused. FL is expressed in millimeters or inches.”\textsuperscript{108} For use in remote control applications, fixed FL lenses are usually obtainable in an auto or motorized iris form. By varying the diameter of the aperture, the iris controls the amount of light reaching the image sensor.

Types of Lenses

The various types of lenses available are as follows:

1. Standard, wide-angle, and telephoto lenses are lenses with a fixed focal length. A standard lens produces an image that is the same as what the eye sees at the same distance; a wide-angle lens is designed to view a wide area up close; and a telephoto lens is designed to view distant areas and produce images larger than what the naked eye sees.

\textsuperscript{106}ibid., pp. 2, 3.
2. A zoom lens has a variable focal length. It is “a camera lens that can vary the focal length while keeping the object in focus, giving an impression of coming close to or going away from an object.”\textsuperscript{109} It can be manually operated or motorized and can be used as a standard, wide-angle, or telephoto lens. “A motorized zoom lens (in the CCTV industry) is distinguished by its full ratio of zoom from wide angle to telephoto ... usually in a 10 to 1 (10:1) or higher format. Additionally, the zoom and focus functions are physically connected so that a zoom lens may be focused in the full telephoto mode and then ‘zoomed out’ to the wide-angle view while maintaining perfect focus.”\textsuperscript{110}

3. “A vari-focal lens is a form of limited zoom lens. Usually in a manual format, the vari-focal lens has a limited zoom ratio of usually less than 2:1 ... i.e., 8.5 mm – 12.5 mm. Additionally, the vari-focal lens has no physical attachment between the zoom and focus functions and so requires refocusing each time the scene perspective is changed.”\textsuperscript{111}

4. A split lens or bifocal lens is a system consisting of two separate lenses that view two scenes with identical or different magnifications and then combines them on the camera imager.

5. A pinhole lens and a right-angle lens can be used for covert surveillance purposes. The pinhole lens “can be mounted onto virtually all shapes and sizes of surveillance cameras. The resulting camera assemblies are either mounted in walls or in ceilings with just a small viewing aperture protruding from these locations. One of the main disadvantages of this type of covert surveillance is the light lost by these lens configurations and limited viewing angles they produce.”\textsuperscript{112} The right-angle lens can be used with the camera mounted inside a thin wall or above the ceiling.

An essential key in properly designing any CCTV system is to select the most appropriate lens for the application at hand. Doing so maximizes the value of the resultant video images.

**Analog and Digital Cameras**

In addressing CCTV systems, it is important to realize that presently two types of CCTV—analog and digital—are available. Analog (the older video format) is rapidly being replaced by digital (the new video format).

Analog systems use chip cameras—also called charge-coupled device (CCD) cameras—that were introduced in the early 1980s and caused tube cameras to become effectively obsolete for security applications\textsuperscript{113} by the late 1990s. CCD cameras “are integrated circuit devices that utilize an array of solid state, light sensitive elements (picture elements or pixels) arranged on a silicon chip to sense light passed from the scene


\textsuperscript{110} Pierce CR. comments made in review of this section, “Closed-Circuit Television Systems,” for the 2nd ed. of High-Rise Security and Fire Life Safety; April 2002.

\textsuperscript{111} Ibid.

\textsuperscript{112} Wimmer R. Modern video covert surveillance options. Security Technology & Design; October 2003:46.

through the lens. The pixels, the smallest sensing elements in the sensor, are arrayed in horizontal rows and vertical columns of varying size.” 114 As Pierce wrote,

*The strongest advantages of chip cameras are that they require less energy and take up less space (because of the lack of high-voltage image tubes), require less maintenance (average image chip life expectancy is five years, compared to the average image tube life of one to two years), and are more flexible, coming with more standard features than tube cameras…. Vidicon [tube] cameras have a high propensity to burn or retain images, meaning the pickup tube shows the scene it has been staring at even after the lens is capped…. Chip cameras, on the other hand, cannot burn or retain images, and are even warranted against such problems.* 115

Digital systems use CCD and complementary metal oxide semiconductor (CMOS) cameras. CCD cameras require a digital signal processor to change the signal from analog to digital, whereas CMOS cameras always transmit digital signals. 116 “For now, CCD is the camera of choice in digital systems. But some engineers and consultants predict that CCDs will be challenged by CMOS technology, in part because it is much cheaper to manufacture than CCD cameras.” 117

Monochrome (black and white) cameras have been largely replaced by color cameras, except for a few specialist applications. 118 “While the performance of color cameras for outdoor applications in artificial light is still inferior to monochrome, most indoor applications, particularly when identification and recognition of people are the primary purpose, benefit considerably from the use of color.” 119 “Color offers valuable additional information on the objects being monitored. More important, the human eye captures color information quicker than the fine details of an object. The drawback is not so good performance in low light levels.” 120 As buildings upgrade their camera systems, color is increasingly becoming the camera of choice.

**Camera Mounting and Housing**

A camera can be mounted in several ways: on a support bracket; recessed into a ceiling or wall; or housed in a dome (containing either a fixed position or a pan, tilt, and zoom camera*), a box, or a custom-shaped protective container made of metal or strong plastic material (housings can be high impact and vandal resistant and even ballistic rated). In interior locations such as reception areas, the camera housing needs to be inconspicuous and fit in with the décor of the facility. Some housing can even be designed to look like track lighting.

---

114 ibid.
117 ibid., p. 79.
119 ibid., p. 38-15.

*A fixed dome camera is housed in a dome enclosure and stays in one fixed position. Pan, tilt, and zoom capabilities are addressed in the next section.*
The electrical power supply to a camera should not be a simple plug-in, as is often the case, but should have the greater degree of security afforded by hard wiring extending from the camera into conduit, plastic channels, or directly into the wall. The camera should be mounted so that it is out of the normal reach of people and cannot be approached without the person doing so being within the camera’s field of view. If it is not mounted at a sufficient height, a person who reaches the camera may sabotage it by pulling the plug, cutting the power supply, or covering the camera lens with an object to obstruct its view.

Exterior-mounted cameras in particular need to be protected with a heavy-duty housing (Figure 5–51) against weather, vandalism, and intentional interference with a camera to make it inoperative. An environmental housing can provide protection against wind, snow, rain, moisture, dirt, or, in some cases, explosions. Sometimes, the housing is equipped with a windshield wiper and heater.

Camera Pan, Tilt, and Zoom Capabilities

Pan or pan/tilt mechanisms are peripheral devices that allow the camera or the housing to move along a horizontal plane (pan) or vertical plane (tilt). Pan moves the camera mounted to it from side to side. Pan/tilt moves the camera mounted to it from side to side and up and down. These mechanisms can be designed to operate automatically or

---

*All conduit should be securely fastened to walls or ceilings with no openings or compartments between the two ends. If a separate connection or junction box needs to be added, then security measures should be taken to prevent access to that box. One method would be to use nonconventional screw heads that require special tools to remove. All conduit used for security wiring should be dedicated only to security. No other type of wiring should be allowed to run through the same tubing” (Beaudry MH, Skip Brandt H. Suite security. Security Management. Alexandria, VA; January 1998:75).
manually. A controller is a device that controls the pan, pan/tilt, or automatic lens functions. Controller types include a zoom lens controller, a pan or pan/tilt controller, or an operations controller, which is a combination of the first two in a single unit.

Most pan, tilt, and zoom (PTZ) cameras are housed in domes (Figures 5–52 and 5–53). As Damjanovski wrote,

They are usually enclosed in a transparent or semitransparent dome, so they make an acceptable appearance in aesthetically demanding interiors or exterior.... Transparent domes usually have an inner mask, with an optical slot in front of the lens, while the rest of the mask is a non-transparent black plastic. By keeping the interior dark (black zoom lenses and camera bodies), they offer a very discreet and concealed surveillance. Very often it is impossible to judge where the camera is pointing, which is one of the very important features of dome cameras. Tinted domes usually have no mask and so the whole dome is transparent but tinted.... Almost all PTZ domes of the newer design have preset positioning.121

---

Preset positioning is “a function of a pan and tilt unit, including the zoom lens, where a number of certain viewing positions can be stored in the system’s memory ... and recalled when required, either upon an alarm trigger, programmed or manual recall.”  

For example, a particularly sensitive door can be equipped with a magnetic contact. When the door is opened “we can force the camera to automatically turn in that direction, zooming and focusing on the previously stored view of the door.”

**Dummy Cameras**

In the past, some buildings, particularly in areas such as parking garages and lots, used dummy cameras. A dummy camera looked like a camera but was not one. It consisted of an opaque camera housing with an apparent power supply connected to it. It may have contained a camera, but was not hooked up to any monitor, or did not contain a camera at all. These devices can provide people with a false sense of security because they believe they are in an area monitored by personnel or recorded by a CCTV system. In the case of a security-related incident such as robbery or assault, the presence of such devices can result in liability exposure for the owner or manager of the facility.

**Closed-Circuit Transmission**

The most common system for transmission of the closed-circuit video signal, whether from a digital or analog camera, is coaxial cable or fiber-optic (also called optical fiber) cable. The CCTV camera manufacturer generally specifies the maximum distance between the camera and the monitor over which the CCTV will perform efficiently. Coaxial cable remains the typical method for transmission over distances up to 2500 feet (762 meters), without the need for video signal amplification. “The actual distance depends on the type of coaxial cable used.”

It is ordinarily reliable and often the upfront lowest-cost method.

If there are difficulties with the installation of coaxial cable, the video signal can be transmitted via several other transmission means: fiber optic, two wire, wireless, infrared, microwave, radio frequency, and satellite. “Fiber optic cable is gaining acceptance because of its better picture quality (particularly with color) and lower risk factor with respect to ground loops and electrical interference.”

**Network Transmission**

There is a growing demand for remote monitoring and playback capability of cameras. For example, a security manager who is traveling may be notified of a serious incident that is occurring, or has occurred, at a particular facility. Using the appropriate technology, it is now possible to remotely access a building’s networked video surveillance system to view live video or a recording of the incident. A network camera, commonly

---

called an Internet protocol (IP) camera, can connect directly to a computer network. According to Matchett,

_The camera is actually a self-contained video server with its own node or address on the network, as if it were a computer. The video from a network camera can be viewed from any computer on the network, provided that the camera is equipped with the proper software. Most network cameras can be viewed with a standard Web browser, the same program used to view Web sites on the Internet. Because the cameras are self-contained servers, many can actually be connected and configured to transmit and view the images over the Internet. Many can also be accessed directly from a computer by dial-up modem connecting straight from the viewing computer to the camera._

One of the advantages is that special cabling is no longer required. The camera can plug into any computer jack on the local area network (LAN) or wide area network (WAN) or [global area network (GAN)]. Most facilities with a computer network will have one or more connection points in each room.

One disadvantage is the ability to tie the camera into an existing camera system. Most control equipment is only equipped with connectors for a traditional camera system. Recording the images from the network camera is more complicated than simply connecting to a recorder and pressing the record button. A [security manager] who is considering using network cameras should fully evaluate the capabilities and limitations of this system before making a decision.127

However, it is noted that “the security of the video information being sent via the network—both internal [within a building] and external [outside a building]—is an important consideration when planning an IP video system.”128

**Video Monitor**

The video monitor is “a device for converting a video signal into an image.”129 The image can be shown in black and white (B/W) or color depending on the particular camera and monitor equipment. As mentioned previously, color has become increasingly popular, particularly where enhanced imaging is vital to the scene being viewed. In certain applications, particularly identification, it is far better to have the camera image

---


---
displayed in color. For example, a camera may be viewing a dark-colored floor area to monitor property removal. If a person carrying property close to her or his body is wearing dark-colored clothing and walks across the area, the property itself may not be discernible on a B/W monitor. However, the same image displayed in color may clearly reveal the property being removed.

Before proceeding, it is appropriate to address a common belief—that CCTV video monitors are nothing more than overpriced television sets. “The video monitor is designed to work with the industrial closed-circuit video system, and will outlast—and out-perform—the consumer television at a lower overall cost, provided that it is installed in a proper environment.”

Pierce further elaborated, “The average television is designed to operate eight hours a day for five years. The monitor is designed to run continuously for 24 hours per day for five years.” In other words, the actual life of the CCTV video monitor is three times that of the consumer television. Pierce also stated that the life of the monitor is reduced when the following situations are present:

1. Dust levels are high (dust gets inside the monitor and leads to heat buildup and premature breakdown of the solid state electronics).
2. Papers are stacked on top of and around the monitor (not permitting proper dissipation of heat and thereby resulting in premature failure of the cathode ray tube, or CRT).
3. Brightness and contrast controls are turned to the maximum.

**Controls**
The controls on the monitor are similar to domestic television sets, with power on and off, contrast, brightness, horizontal, and vertical hold (and color controls, if the monitor is color).

**Size**
Video monitors can be procured with various screen sizes, including large flat screens.

**Onscreen Displays**
Several types of displays and onscreen character generation can be used to assist the performance of an operator viewing a monitor. Displays using graphic floor plans and maps with flashing, colored icons symbolizing event locations and definitive text can be used to decrease the operator’s response time and increase adherence to, for example, established procedures for responding to alarms.

Onscreen character generation varies from camera system to camera system. It may show the camera number, camera title (brief description of the camera location), date, and time. Also, if alarms are part of the CCTV system, it may show the alarm status of each camera being displayed at that time. The date and time information is generated either by an exterior unit or the camera microprocessor unit. The unit producing this information should have battery backup to accommodate limited power failures.

---

131 ibid.
Mounting

Monitors may be tabletop, rack, or wall mounted depending on their size and the number being viewed. “There have been several studies of operator effectiveness regarding the most effective angle of the monitors to the operator. Design the console or viewing area in such a way that the monitors that will be viewed by the operator will be aimed straight at wherever the operator is sitting.” 132 Figure 5–54 displays a two-operator security console configuration.

Rack mounting, particularly where large numbers of monitors are involved, permits the monitors to be mounted in a functional way that takes into account the camera scenes that are being monitored. For example, if there are a series of cameras in a corridor, the monitors displaying those images should be programmed together in a horizontal or vertical pattern where one monitored scene leads immediately to the adjacent monitored scene. Other examples in the high-rise setting may be a series of cameras monitoring the loading dock area, various levels of the parking structure, building lobbies, elevator cars, or ground floor exits from building stairwells. Rack mounting also saves space and the clutter that ensues when multiple monitors are mounted on a tabletop.

Operator Viewing Effectiveness

Before proceeding, it is appropriate to mention a problem that occurs with monitoring large numbers of cameras. There does come a point when the person cannot keep pace with the demands of the viewing operation. “There have been several studies of operator effectiveness regarding the number of monitors an operator can watch. Effectively the average person cannot watch more than four pictures simultaneously with any comprehension of what is happening.” 133 The operator will view multiple monitors by repeatedly scanning back and forth across them. To monitor effectively, additional operators may be needed. However, because of the financial impact such a move would have, this issue is often not addressed. As a result, the effectiveness of the security operation suffers and the operators themselves are subjected to stress and fatigue. “To combat this

---

132 ibid.
133 ibid.
problem, CCTV systems should be designed to be as ‘hands free’ or automated as possible. This provides the operator the ability to respond to the situation versus watching the screen and concentrating on the controls.”

A split screen unit is “equipment that simultaneously displays parts or more than one image on a single monitor.” Two, 4, 9, 16, or 32 scenes can be simultaneously displayed on a single monitor. The problem with this technique is that the resolution of the scenes is decreased proportionately and it becomes more difficult for the operator to distinguish what is being viewed.

Video switchers (see next section) can also be used to amplify a person’s ability to view multiple video cameras.

Another possible solution to monitoring large video installations is to continuously display a few cameras that have security importance, continuously record all cameras, and automatically call up cameras on alarm (using alarm devices such as a magnetic door contact, a motion detector, or video motion detection). Some video systems are programmed to automatically perform video tours of sensitive locations viewed by the cameras. This helps ensure that particularly sensitive locations receive appropriate attention. (See the next section on video analysis, which discusses technology that can lead to more effective monitoring of large video systems.)

An important factor in the monitoring of video systems is the total time an operator is able to stay alert and work effectively while viewing single or multiple monitors. The studies mentioned earlier have addressed this vital but often neglected factor. “After approximately one hour (less time for people of below average intelligence) the average operator’s mind has mentally shut off the monitor to the point that an object or objects of identifiable size can be moved into and consequently through the scene at a rate of six inches [0.15 meters] per minute.” One obvious solution to this problem is to rotate the video operators. However, in many high-rise building operations, training multiple operators and frequently rotating them may not be a viable option because of the limited staff. Where little change is occurring, providing color monitors and alarm interfacing can help to break the monotony of monochrome images. The more that is happening, the more likely it is that the operator will stay active and alert and more effectively monitor the CCTV system.

**Video Analysis or Video Analytics**

Video analysis or video analytics (or sometimes known as image analysis or intelligent video) “involves the extraction of information from digital images by a method known as digital image processing. Image analysis can include simple tasks like barcode reading to the much more complicated processes of facial recognition.” According to Harwood,

> Intelligence video refers to the analysis and extraction of video information with specific reasoning attached for specific applications.... The intelligent video system can be programmed for an endless variety of uses. For example, a particular problem [at a bus station or possibly a parking lot] is the gathering of loiterers.

---


This problem is alleviated by system alarms that are instigated by the video itself when the presence of persons where they should not be is indicated. Personnel who have been alerted to the scene can view the area and determine the cause for the alarm, then dispatch someone to disperse the loiterers if necessary. A similar feature is used to eliminate illegally parked cars from sensitive areas or abandoned vehicles. Automatic detection and alert for vehicles parked in restricted areas gives security personnel immediate notice of a breach that could eliminate a potential car bomb threat or simply result in a parking ticket.\textsuperscript{138}

Video analytics can also be used for applications such as alerting security staff of vehicles speeding or traveling in the wrong direction or a package left unattended in an area.

**Video Switchers**

The simplest CCTV system involves a single camera with its image displayed on a single video monitor. Larger high-rises often have an extensive camera system covering multiple locations within a building, with camera images being displayed on multiple monitors. A person viewing the monitors is restricted because he or she can comfortably view only a certain number of monitors at any given time.

A video switcher is “a device for switching more than one camera to one or more monitors manually, automatically or upon receipt of an alarm condition.”\textsuperscript{139} It allows multiple cameras to be viewed on a single monitor or multiple monitors, either in sequence or one at a time. “Video switchers enhance a video system, allowing it to save costs while remaining effective through multiple camera monitoring through a single source of view.”\textsuperscript{140} There are various types of manually and automatically operated video switchers. “Manual switchers, sequential switchers, and alarming switchers have been replaced by various multiplexers, matrix switchers, and the newer digital control/manipulation systems. They are still in use but are of no consequence to modern design.”\textsuperscript{141}

**Matrix Switcher**

A matrix switcher is “a device for switching more than one camera, VCR, DVR, video printer, and the like, to more than one monitor, VCR, DVR, video printer and so on.”\textsuperscript{142} Such a device can be of use in large high-rise buildings, which contain vast numbers of CCTV cameras and monitors (and in multibuilding complexes where multiple systems are being monitored in a centralized location).

Matrix switching uses microcomputer control circuits and permits the display of any camera view on any monitor. Available systems can include hundreds of cameras and scores of monitors. The camera views are inputs to the central processor that can match camera views to monitor manually via an

\textsuperscript{138}ibid.


\textsuperscript{141}Pierce CR. Comments made in review of this section, “Closed-Circuit Television Systems,” for the 2nd ed. of High-Rise Security and Fire Life Safety; April 2002.

\textsuperscript{142}A video printer is “a device for converting a video signal to a hard-copy printout” (Damjanovski V. CCTV. 2nd ed. Burlington, MA: Elsevier Butterworth-Heinemann; 2005:528).

\textsuperscript{143}ibid., p. 514.
operator keyboard, automatically through video motion detection• or alarm activation [by a magnetic door contact or a motion detector], or in accordance with programmed sequence patterns via the keyboard and CPU [central processing unit] or developed off-line and loaded into the CPU.143

Multiplexer

A multiplexer is a powerful, high-speed video switcher that has largely replaced the aforementioned switchers.144 It is a device that can input the video signals from multiple cameras (up to 16) and produce two kinds of video outputs: one for viewing and one for recording. “The multiplexer operates by selecting a frame from each camera in sequence, digitizing it, and displaying it in a predefined location on the [video monitor] screen”145 or sending it to the recorder.

Multiplex Video Recording

A problem in reviewing VHS tape recordings was when multiple camera images were sequentially displayed on a single monitor and then recorded on the videocassette recorder (VCR). When the video was played back, the images from all the cameras were displayed sequentially. The frequent image switching made it difficult for the reviewer to follow clearly what was occurring on any one particular camera. The situation was chaotic when up to 16 camera images were being viewed. This difficulty has been removed by multiplex video recording.

A major advance in video recording has been the development of multiplex recording which digitizes the camera input, processes or enhances the signal in various ways and then records it in real-time or time lapse. Multiplexing allows multiple cameras (up to 16 at present) to be recorded on a single recorder (DVRs, typically have built-in multiplexers). Instead of switching from camera to camera to select the image, the multiplexer merely selects or “grabs” a frame from each camera in series, processes or enhances the signal and passes it to the recorder, until all cameras have been selected. It then starts the cycle over again…. When grabbing frames the multiplexer electronically identifies each with its source camera. When the tape is played back, utilizing the multiplex unit as a playback control, only the successive images from the selected camera are displayed. The net effect is as though the tape was made from a single camera.146

•Video motion detection allows a CCTV camera to be used as an alarm device. “A video motion detector (VMD) is a device that analyzes the video signal at its input and determines whether its contents have changed and consequently, produces an alarm output” (Damjanovoski V. CCTV. Woburn, MA: Butterworth-Heinemann; 2000:190). “For each camera involved, a detection pattern is selected and stored in the processor. The detection pattern may be all or some of the camera image. Video Motion Detection is only used with fixed position and fixed focus cameras” (Television in security. In: Williams TL, ed. Protection of Assets Manual. Vol. IV (used with permission of POA Publishing, LLC, Los Angeles, CA. 2000:38–61).


Because there is a small time lapse between camera images, when the recording is played back motion may appear slightly jumpy. Despite this consequence, the quality of the image is acceptable for most applications in the high-rise setting.

Video Recording and Storage

A video-recording device records camera images. These images can be used to examine past incidents, for investigations, as evidence in civil litigation or criminal actions (although the admissibility of digital recordings in judicial proceedings has still to be determined), and to defend against insurance claims.

Video recording can be in either real time or time-lapse mode. (Real time means that all images the camera captures are recorded; time lapse means that the images are recorded intermittently.) “The prime reason for including time-lapse capability in the CCTV recorder is to conserve the storage medium.”

Previously in the security field, reel-to-reel videotape recorders (VTRs) were the standard, followed by videocassette recorders (VCRs) and then digital video recorders (DVRs) and network video recorders (NVRs).

Digital Video and Network Video Recorders

Digital video recorders (DVRs) and network video recorders (NVRs) offer a number of advantages over VCRs. For an existing analog system, DVRs can provide digital recording and playback capabilities. DVRs have “the ability to record and play back video from the same storage space at the same time … DVRs differ in terms of disk space, resolution, compression, frame rates, motion detection, archiving ability, searchability/retrieval, playback, image authentication, and operating systems. Advances are being made in all these areas.” As Kruegle stated,

Both magnetic and optical disk systems have an advantage over VCRs with respect to storage and retrieval time of a particular video frame, which leads to the advantages of using a digital recording system. The biggest return on investment is the amount of time saved while investigating a particular event. The other benefits include:

Fast retrieval, transport and enhancement of images
Storage capacity
Able to record multiple times without image degradation
To increase storage capacity, hard drives are often used simultaneously. For long-term storage, images are archived and stored on a removable memory device.

With regard to the amount of time saved while investigating a particular event, rather than manually winding and rewinding through endless videotape, “to review recorded images, users simply type into a PC keyboard the time and date the images were captured.”

147 Ibid., pp. 38–63.
Chapter 5  •  Building Security Systems and Equipment  335

recorded; the computer calls them up instantly.”150 Also, when required, digital versions of a particular image can be easily printed out or stored on a portable memory device.

In large high-rise complexes deploying huge numbers of cameras, digital video recording means that the archiving and storage of vast numbers of videotapes is now no longer necessary.

And, as Damjanovoski noted,

The other important advantage of digital video signals is the possibility for digital processing and storage. This includes image enhancement, compression, transmission, various connections, and storage. Also, an important feature is that there is no difference in image quality between the copies and the original. Whether we make one, two, or ten copies of the image captured in a digital format, the quality is exactly the same as the original no matter what generation copy it is. And last, but not the least important feature with video captured in digital format is the possibility of checking the originality of a copy. This feature is often referred to as “water-marking,” and it enables the protection of digital signals against deliberate tampering, a very important aspect for CCTV security applications.”151

A network video recorder (NVR) is “a software or computer that records video on a hard disk." Like a DVR, it records digitally so the user can instantly search by time, date, and camera. It collects video from network cameras, network video servers, or a DVR over the network.”152

Rapid Technological Change

Since the 1980s, an accelerating change in the technology that supports CCTV systems has occurred. CCTV specialists, consultants, manufacturers, dealers, and suppliers can be an invaluable source of information for determining exactly which state-of-the-art systems and equipment are available at any one point of time. However, one needs to be aware that advice may be given with the specific intention of promoting one particular product or system. Charlie Pierce, a leading authority on CCTV, advised that it is best to “design the application first and fit the equipment to it.”153

Camera Applications

CCTV can enhance the security of a high-rise building’s perimeter, the building itself, public access or common areas, maintenance spaces, and tenant areas. Perimeter entrances and exits, hallways and corridors, elevators and elevator lobbies, parking areas, and other sensitive locations can be monitored and kept under surveillance.


Cameras in Buildings

CCTV cameras might be installed in high-rise buildings in locations such as the following:

- **Building access points where occupants enter on foot.** All building entrances, particularly when an entrance door is remotely controlled. With a remotely controlled door, it is vital that persons requesting entry can be seen on camera to help determine whether they are to be granted or denied access by security staff monitoring the system. If the door is equipped with an electronic card reader to control access, a camera is also useful to view when tailgating or piggybacking of persons occurs.
- **Public lobbies with potentially slippery floors** (such as marble surfaces) where slip-and-falls might occur.
- **Pedestrian egress points such as ground floor exits from building stairwells.** A camera in conjunction with a video motion detector can, when movement is detected in the stairwell, draw the attention of security staff monitoring the system, and also trip a video recorder to record the images in real time. This setup is useful for detecting unauthorized removal of property from a building stairwell. The provision of a two-way voice communications system with a speaker and microphone at the camera location can be effective for communications between the security command center and such a location.
- **Inside passenger and service/freight elevator cars.** A camera installed in a visible location inside an elevator car may deter threats against persons (such as lewd behavior, assault, or robbery) and threats against property (such as vandalism of the elevator car itself). With vandalism, particularly graffiti, if no action is taken against this type of activity, it may escalate. Installing a CCTV camera covertly in the affected elevator car(s) might lead to identification of the persons responsible.
- **Crucial entry and exit points within the building.** These include main lobby and lobby console/reception/front desk areas, security checkpoints where building workers (such as engineering, security, janitorial, and housekeeping staff) enter the facility, and cross-over floors between elevator banks (for example, cross-over floors between the passenger elevators that serve the building tower and the passenger elevators that serve an under-building parking garage, or between low- and mid-rise elevator banks, or between the mid- and high-rise elevator banks).
- **Walkways and corridor routes leading to public areas such as day-care facilities, laundry rooms, vending machines, fitness centers, saunas, swimming pools, spas/hot tubs, and other recreational areas.***

---

*The design of the CCTV system (including selection of camera locations, types, and monitoring arrangements) for a particular building should only be done after a risk assessment (as described in Chapter 4) has been completed.

**The use of microphones and listening devices is prohibited in some jurisdictions.

Video surveillance inside a recreational area might be considered an infringement of the user’s privacy. As with all sensitive locations, legal counsel should be sought before proceeding to install cameras in such areas. Even if a camera in a sensitive area is not being monitored but is only being used to record images for later use if an incident warrants it, the mere fact of having a camera in an area, such as a swimming pool, could generate an expectation that the area is being monitored. If an incident were to occur, this expectation could lead to liability exposure for the building owner, manager, or facility operator who required such equipment.*
• **Other sensitive areas.** These include the building perimeter; neighboring streets; passenger and service/freight elevator lobbies; stairwell exits to the building roof; dumpster and trash compactor areas; openings to outdoor air intakes and ducts for HVAC systems and air handling units; strategic locations on mechanical floors or floors that have restricted access, including entrances to elevator machine rooms, elevator pits, and main utility areas such as the power transformer room* and central plant; and high-value item storage areas, including safe and vault areas. Again, video motion detection can be used to warn the operator monitoring the system of movement within a certain area, and recording can provide evidence for later review.

• **Locations where covert surveillance is required.** A concealed camera can be an important tool for observing activities, particularly illegal ones such as theft. Cameras can be cleverly concealed in emergency lighting systems, in emergency exit signs, behind clocks, behind works of art, behind one-way mirrors, in ceiling-mounted sprinkler heads, in portable radios, in air fresheners, in hollowed-out books, and in other items that can be openly displayed. A hidden camera can be used to observe events where it would be impossible to conceal the presence of a person. Modern technology has reduced the size of surveillance equipment and aids such as a pinhole and a right angle lens. In conjunction with a video-recording device, concealed cameras can be used to view areas for extended periods of time and provide a permanent record of the events. In some applications, the portable unit of CCTV and VCR/DVR may need to be equipped with a self-contained power source—for example, on top of elevator cars where the camera, equipped with a pinhole lens, and the VCR/DVR may be installed as a self-contained unit. Note that such installations must always be carried out in conjunction with a certified elevator technician.

Of course, not all public access or common areas may be monitored by any CCTV system, covert or otherwise. For example, cameras are not permitted in restrooms, changing areas, and locker rooms, or in any other areas where users have a reasonable expectation of privacy.

### Cameras in Parking Garages and Lots

CCTV cameras might be installed in high-rise parking garages in locations such as the following:*•

- **Garage access points where occupants enter on foot.**
- **Pedestrian egress points such as ground floor exits from garage stairwells.** A camera in conjunction with a video motion detector can, when movement is detected in the stairwell, draw the attention of security staff monitoring the system and also trip a video recorder to record the images in real time. This setup is useful for detecting unauthorized persons in a garage’s stairwell(s). The provision of a two-way voice communications system with a speaker and microphone at

---

*The power transformer room is the space, usually located underground, where a utility company brings its high-voltage lines into a building for step-down transformers to convert high voltage to low voltage for use by the building.

**The design of the CCTV system (including selection of camera locations, types, and monitoring arrangements) for a particular building should only be done after a risk assessment (as described in Chapter 4) has been completed.
the camera location can be effective for communications between the security command center and such a location.

- **Inside passenger and service/freight elevator cars.** Cameras within elevator cars can be an effective deterrent to threats against persons (such as lewd behavior, assault, or robbery) and threats against property (such as vandalism of the elevator car itself). As noted earlier, with vandalism, particularly graffiti, if no action is taken against this type of activity, it may escalate. Installing a CCTV camera, either openly or covertly, in the affected elevator car(s) may help deter or identify the persons responsible for the vandalism.

- **Crucial entry and exit points for an under-building garage.** These include cross-over floors between elevator banks that serve the building tower and the passenger elevators that serve the under-building parking garage.

- **Access points for vehicles to parking garages (and lots).** If a vehicle gate or traffic arm is remotely controlled, it is vital that vehicles, and possibly drivers, be viewed on camera to determine if they are to be granted access. Many parking garages—particularly under-building ones—have cameras installed at all ingress/egress points that, in conjunction with a video-recording device, record the license plates of all vehicles entering and exiting the property as well as closeup images of the vehicle drivers (if an incident occurs, this helps to identify vehicles that may have been involved; also, optical recognition software can be used for real-time recognition of license plates).

- **Other sensitive areas.** These include the garage perimeter; neighboring streets; parking attendant’s booth, an automatic pay station, or the entrance to a room where cash is stored on site; emergency call stations and intercoms located inside a garage; in passenger elevator lobbies or pointing outward from these lobbies to view pedestrians coming from the parking areas and vehicles traveling by these areas; stairwell ground floor exits; openings to outdoor air intakes and ducts for HVAC systems and air handling units; entrances to elevator machine rooms\(^*\) and elevator pits; and entrances to other utility areas. Again, the use of video motion detection can be used to warn the operator monitoring the system of movement within a certain area.

- **Locations where covert surveillance is required.** See the previous section for information on concealed cameras.

The installation of cameras in parking garages is somewhat restricted because many facilities have a labyrinth-style design with low ceilings and structural columns and have hiding places that can limit the field of view. According to Bowers,

_Pipes, girders, and signs can make coverage even more difficult to arrange. If the cameras are hung beneath these obstructions, they are likely to be knocked off by a tall vehicle, such as a van. Corners, cross-ramps, and dead ends where it is difficult to justify the cost of a camera may create other blind spots._

_Several good ways around these obstacles to good CCTV coverage do exist, however. In a garage designed in the row-and-column array or_
perpendicular roadways array, cameras can be placed to cover each driving lane. For short lanes, a single camera mounted on the wall will suffice, and in long lanes the cameras can be arranged in facing pairs. In this arrangement, all persons or vehicles must ultimately pass close to one camera or another.\textsuperscript{154}

In open parking lots, cameras can be mounted on light poles or on adjacent buildings.

The actual design, configuration, and location of any CCTV system in a high-rise building and a parking garage or parking lot depends largely on the security and life safety needs of the building and the parking garage or parking lot itself. It is of note that some garage operators do not locate cameras in parking garages and lots due to the concern that doing so may expose the company to liability unless there is adequate staff to monitor the images.

Undervehicle Viewing Cameras and Scanning Systems

A small, weather-resistant, battery-operated video camera fitted with an ultra-wide angle lens can be used for viewing the undercarriage of vehicles for suspicious objects such as improvised explosive devices. The camera with illumination using LEDs is mounted on a swivel wheelbase that can be moved under a vehicle. The image can be viewed using a head-mounted, antiglare LCD video monitor.\textsuperscript{155}

Another device utilizes a camera for inspecting the undercarriage of vehicles. “The Under Vehicle Monitoring System SecuScan essentially comprises a scanning unit, a workstation, traffic lights and a light barrier…. Through a small slit in the scanning unit, the camera captures the entire underside of a vehicle in moving traffic…. To simplify the correlation between the underside images and the corresponding vehicles, an optional front-end capture camera as well as automatic license plate recognition can be integrated…. All the data collected or manually entered can be stored in a database under the vehicle license plate number. In case of recurring vehicles, the software provides the possibility to compare the current underside image with an already archived one of the same vehicle in order to identify potential deviations at a glance.”\textsuperscript{156}

Patrol Management Devices

Security staff activities, such as mobile (or beat) patrols or rounds, can also be supervised using portable patrol management devices. These devices may be mechanical clocks fitted with a graduated paper roll or disk or electronic guard tour systems. Both systems generate a record of patrol activity and can be used to evaluate and control the performance of the patrolling officer. “They provide the security manager with a consistent record of rounds and occurrences at a facility without the need for human supervision

\textsuperscript{154}Bowers DM. Assigning a place for parking security. Security Management. Alexandria, VA; December 1999:64.
\textsuperscript{156}Signalbau Huber Under Vehicle Monitoring System. Signalbau Huber, Munich, Germany. <www.secuscan.com/content/prospekt/prospekt_e.pdf>; July 4, 2008.
to ensure that rounds are completed as assigned.”¹⁵⁷ A description of these two patrol management devices follows.

**Mechanical Clock**

Patrol officers may carry the mechanical clock (commonly called a watchman’s clock or watch clock) around on patrol. At certain locations, preinstalled keys are inserted into an opening in the clock. This causes the date, time, and key number to be recorded on paper housed within the clock. Supervisors are provided a master key that enables the clock to be opened to review records of tours, to wind the clock or to add batteries, to reset the date and time, and to replace the paper roll or disk.

Unfortunately, an unscrupulous security officer working alone in an area can fabricate a patrol. This is done by removing keys from the designated stations at the beginning of the shift, taking them (lined up in their original order) to a central location, and then turning them in the clock at the required times (for instance, every hour), thereby simulating the tour. The keys are then returned to their original locations at the end of the shift. Supervisors can defeat this scam by visiting a patrol officer at unannounced times during a shift and inspecting key stations, by securing the keys to their stations using screw flanges and requisite screw head “seals” to prevent tampering, or by reviewing CCTV recordings of aspects of the officer’s patrol.

Patrol personnel should not be issued the master key to the clock (although provisions might be made to provide supervised access to the master key in the event that the clock malfunctions). As an added precaution, the tape or disk is automatically marked each time the clock is opened so supervisors can inspect for nonauthorized access.

The mechanical clock can sometimes be cumbersome to carry and made inoperable by being dropped or impacted with a heavy object.

**Electronic Guard Tour System**

An electronic guard tour system functions either alone or with software. It consists of a reader that may be of various shapes and sizes and includes either a contact wand or a noncontact laser scanner. The officer carries around the reader or data acquisition unit during the patrol, and at certain stations the reader “reads” preinstalled data strips or disks, recording information such as date, time, station number, and location. The stations may be barcodes, magnet strips, chips, or metal disks. Data can be transferred from the reader to a computer or printer by placing the reader in a cradle or data transfer unit or by connecting the reader directly to a printer.

**Advantages of Electronic Guard Tour Systems**

Some advantages of electronic guard tour systems over mechanical clocks are as follows:

- Readers are smaller and lighter than traditional mechanical clocks.
- The data strips are small, unobtrusive, and easy to install, and they can be colored to match their surroundings.

- The printout of information is easier to read than that generated by traditional mechanical clocks. Some systems have the additional advantage of being able to print the data out in various ways, showing the name of the patrolling officer, the length of the tour, the tour stations completed, and exceptions to the tour (including stations missed or duplicated). Data also can be saved to a computer file for later reference.

- Most systems are virtually tamperproof.

“Guard tour management systems not only provide the security officer with a sense of added responsibility and feeling of self-worth, but generate accurate reports that verify the effectiveness of each tour or patrol.”

Patrol monitoring devices not only provide a documented means to monitor the patrol activity of security staff, but they also can provide valuable evidence to explain, for example, why there was a delay in an officer observing an incident (if the officer is shown to have been at another location). They also can be used to determine the approximate time of an occurrence (for example, if an officer is seriously injured while on patrol, the last station visited will assist in determining the time the incident occurred).

In addition to the two systems just described, electronic card access systems can be used to monitor patrol activities. Each patrol officer can be issued a card to access certain areas while on patrol. The records obtained from the card access system can then be used to review patrol activities.

Patrol Vehicles

Patrols may be conducted on foot or using a motor vehicle, an electric cart, a bicycle, a tricycle, or a personal transporter.* The decision as to what vehicles, if any, will be used depends on factors such as the use of the facility, its size, the areas to be patrolled (including whether public roads and footpaths will be involved and what vehicles are authorized to travel along such routes), the actual patrol duties to be performed, the average distances that security staff will be expected to travel, anticipated increases in staff productivity gained with the increased mobility of a vehicle, and the expected travel times for staff to respond to security incidents occurring in any part of the facility.

Virtual Guard Tour

Video technology such as a virtual guard tour can be deployed in a security command center to assist in patrolling certain building areas at certain times without security

---

*An example of a personal transporter is the Segway PT, “a two-wheeled, self-balancing electric vehicle invented by Dean Kamen. It is produced by Segway Inc. of New Hampshire, USA. The name ‘Segway’ is a homophone of ‘segue’ (a smooth transition, literally Italian for ‘follows’). PT is an initialism for personal transporter while the old suffix HT was an initialism for human transporter. Computers and motors in the base of the device keep the Segway PT upright when powered on with balancing enabled. Users lean forward to go forward, lean back to go backward, and turn by using a ‘Lean Steer’ handlebar, leaning it left or right. Segway PTs are driven by electric motors at up to 20 kilometres per hour (12 mph). Gyroscopic sensors are used to detect tilting of the device which indicates a departure from perfect balance. Motors driving the wheels are commanded as needed to bring the PT back into balance” (Segway PT. Wikipedia. October 17, 2008. <http://en.wikipedia.org/wiki/Segway>; October 25, 2008).
personnel needing to physically visit these areas. According to a report from the Security Industry Association, “A virtual guard tour eliminates the need for a security guard to do the traditional facility walk-through at scheduled times. A digital video recorder can be programmed to flash in sequence to each of any number of cameras linked at any interval a user chooses. The video can be recorded, physically monitored, or both. Virtual guard tours reduce the need for expensive capacity on recording equipment because not every camera has to be recorded all the time. And it allows the guard more time flexibility to monitor the access points deemed most critical.”

Security Monitoring Center

The focal point for an entire building’s security operations may be local annunciator and control panels built into an open-style desk arrangement or a complex and sophisticated security command center. In either case, “The security manager must consider such issues as the noise level in the control center, the appearance of the control center, the chair the operator uses, work station height, lighting, air conditioning, and equipment layout.” The systems should be readily accessible to the operator and ergonomically designed so that monitoring does not contribute to operator stress and fatigue. The design should bear in mind the comfort of the operators who will spend considerable periods of time performing routine and, at times, monotonous tasks within its confines. Adequate ventilation, heating, and air-conditioning are essential. (“Dust is a major hazard in surveillance rooms. Regular cleaning and a good air purifier machine within the room will help keep the dust down.”)

The organization and appearance of the open-style desk arrangement or the security command center often reflect a building’s commitment to security. If the area is attractive and well laid out; if equipment is up-to-date, well maintained, and sufficient for the needs of the security staff to carry out their duties and responsibilities; if the room is clean and the work surface of the operators is clean and free of clutter, then it is likely that building security is taken seriously and the program is being professionally managed.

If the security command center is located in a separate room, it should meet the following standards:

- Be of adequate size to accommodate the operation and future expansion needs.
- Be highly secure with access doors to it kept locked at all times. (Some command centers use mantraps to control entry.) High-security doors should have a door viewer so that security staff members have a clear view of the other side of the door and can see the person requesting entry before access is granted or denied.
- Have interior windows be constructed using burglar-resistant (and possibly bullet-resistant) glass, and windows facing the exterior of the building should be kept to a minimum. (Some buildings, for security purposes, prefer to house the

---


security command center in a windowless room so that an outsider is not even aware of its presence.)

- Have other security elements, such as dip trays if a window that is accessible to the public exists. (A dip tray is a small opening at the base of a window through which keys, access cards, and other small items can be passed.)

Security Convergence

This chapter generally addresses security systems and equipment as stand-alone systems. However, “technologies are emerging that overlap physical and IT [information technology] security. Most of this overlap is coming from the application of Internet protocol technologies to traditional technologies, ranging from perimeter controls, to surveillance and tracking technologies, access management and integrated communications systems.”

“The incorporation of computer intelligence and network connectivity into devices and systems—the basic convergence influence—allows systems to be of greater and greater real-time benefit to their users.” When “security technology shares an infrastructure backbone with the building’s IT network[,] it may no longer be necessary to run cable for a new surveillance camera—often, it can be plugged into an Ethernet* port and assigned an IP address. Some equipment may even reside on the wireless network, allowing it to be reconfigured and repositioned easily and cheaply as the facility’s needs change.”

As this convergence trend continues, the interoperability** of building security systems and equipment, particularly with building automation systems, will become of increasing importance.

Security System Maintenance and Replacement

An important function of the security department is to ensure that building security systems and equipment continue to work properly. Depending on the building, this responsibility may vary from simply communicating problems to building management, to calling for maintenance service from system vendors, to actually having a systems specialist on staff who is responsible for the entire security system. It is important to keep equipment manufacturer’s operation and service manuals onsite and to keep a record of work performed on the systems and equipment.

When systems and equipment become unreliable and outdated, the responsibility for upgrading or replacing them may reside with the security department. Because

---


* Ethernet is “a local area network used for connecting computers, printers, workstations, terminals, and so on, within the same building. Ethernet operates over twisted wire and coaxial cable” (Damjanovoski V. CCTV. 2nd ed. Burlington, MA: Elsevier Butterworth-Heinemann; 2005:507).


** Interoperability is “the ability of a system or a product to work with other systems or products without special effort on the part of the customer” (SearchSOA.com Definitions. <http://searchsoa.techtarget.com/sDefinition0,,sid26_gcl212372,00.html>); December 28, 2008).
the security requirements of a building may have changed since the original system was installed, a system upgrade presents an opportunity to reevaluate needs and acquire a system that will more comprehensively and efficiently address those needs.

Summary

- The security systems and equipment of high-rise buildings vary according to the specific needs of each facility.
- Buildings can use a combination of physical barriers, locks, locking systems, property control systems, intrusion detection systems, duress alarms, lighting systems, communication systems, closed-circuit television video systems, and other security devices integrated into a total security system.

Key Terms

Access card. A device that is presented to a card reader to operate an access control system. Sometimes it is called an electronic access card or a keycard.

Active vehicle barrier. “An impediment placed at an access control point that may be manually or automatically deployed in response to detection of a threat.”

Algorithm. “A series of steps that are carried out in a specific order to provide a solution to a problem or execute a task.”

Antipassback. “A feature of an access control system which prevents successive use of one card to pass through any portal in the same direction. To attain this protection, a separate reader is required at each entrance and exit. Anti-passback prevents a card [that has been] passed back to another person [from being used] for the purpose of gaining entry.”

Atrium (plural atria). A large open space within a structure that is two or more floors high. Some buildings, particularly “larger-scale hotel building configurations often have atria two or three stories high and sometimes up to sixty stories high, which are often the focal point of building design. Atrium areas themselves may include several occupancies or mixed functions associated with hotel operations.”

Barrier. “A natural or man-made obstacle to the movement of persons, animals, vehicles, or materials.”

Berm. A mound of earth usually covered in grass.

Blast curtains. “Heavy curtains made of blast-resistant materials that could protect the occupants of a room from flying debris.”

---


Bollard. A cylindrical post firmly anchored to the ground and usually constructed of heavy steel.

Building envelope. “The separation between the interior and the exterior environments of a building. It serves as the outer shell to protect the indoor environment as well as to facilitate its climate control…. The physical components of the envelope include the foundation, roof, walls, doors and windows.”

Central station. “A business approved to monitor subscribers’ alarm systems from a central location rather than on site.”

Charge-coupled device (CCD). Imaging device used in cameras. “Integrated circuit devices that utilize an array of solid state, light sensitive elements (picture elements or pixels) arranged on a silicon chip to sense light passed from the scene through the lens. The pixels, the smallest sensing elements in the sensor, are arrayed in horizontal rows and vertical columns of varying size.”

Closed-circuit television (CCTV). The transmission of scenes or moving pictures from a video source, such as a camera, by conversion of light rays to electronic signals, which are transmitted via coaxial cable, fiber-optic cable, twisted pair wire (hence the terminology “closed-circuit”), or infrared beams, microwave, radio waves, satellite, or a host of other methods to specific receiving equipment such as a video display monitor or a video (recording device. Also sometimes known as closed-circuit video.

Coaxial cable. “The most common type of cable for copper transmission of video signals. It has a coaxial cross section, where the center core is the signal conductor, while the outer shield protects it from external electromagnetic interference.”

Credential. Something that entitles a person to certain rights or privileges.

Dip tray. A small opening at the base of a window through which keys, access cards, and other small items can be passed.

Door viewer. A small device installed in an opaque door to provide a clear view of the other side of the door (using a hollow end or peephole to look through and a lens at the other end to give a wide viewing angle). See view port.

Dumbwaiter. “A hoisting and lowering mechanism, used exclusively for carrying materials, with a limited size car that moves in guides in a substantially vertical direction.”

Duress alarm. “A device that enables a person placed under duress to call for help without arousing suspicion.” Sometimes called a panic alarm.

Duress code. “A special code that reports an ambush, duress, or emergency situation. The code can be given verbally, for example, as part of what would appear to be a routine conversation, or entered on a digital keypad during what would appear to be a routine disarming sequence or call-in.”

---

177 ibid.
Ethernet. “A local area network used for connecting computers, printers, workstations, terminals, and so on, within the same building. Ethernet operates over twisted wire and coaxial cable.”\(^{178}\)

Fail safe. “A safety feature of a security device that is designed to release or disconnect during a power loss.”\(^{179}\)

Fail safe lock. “A type of lock that automatically opens when a power failure occurs.”\(^{180}\)

Fail secure lock. “A type of lock that automatically locks when a power failure occurs.”\(^{181}\)

False alarm. Occurs when a system detector indicates in error that there is an incident.

Fiber optics. “A technology designed to transmit signals in the form of pulses of light. Fiber optic cable is noted for its properties of electrical isolation and resistance to electrostatic and electromagnetic interference.”\(^{182}\)

Fire barrier. “A continuous vertical or horizontal construction assembly designed and constructed to limit the spread of heat and fire and to restrict the movement of smoke.... A continuous membrane, either vertical or horizontal, such as a wall or floor assembly that is designed and constructed with a specified fire resistance rating to limit the spread of fire and that also will restrict the movement of smoke. Such barriers might have protected openings.”\(^{183}\)

Fire escape. A steel stairway attached to the exterior of a building for occupant evacuation and fire department access.

Fire exit hardware. “A door-latching assembly incorporating an actuating member or bar that releases the latch bolt upon the application of a force in the direction of egress travel and that additionally provides fire protection where used as part of a fire door assembly.”\(^{184}\)

GAN (global area network). “A network that (a) is composed of different interconnected computer networks and (b) covers an unlimited geographical area.”\(^{185}\)

Gurney. “A metal stretcher with wheeled legs, used for transporting patients.”\(^{186}\)

Hard disk. A magnetic disk onto which data is written to or read from. The terms hard disk and hard drive are used interchangeably.

Internet protocol (IP). “The method by which data is sent from one computer to another over the Internet. Each computer [or other network device such as an IP camera], known as a host on the Internet has one address that uniquely identifies it from all other computers on the Internet. A Web page or an e-mail [or other digital data] is sent or received by dividing it into blocks called packets. Each packet contains both the sender’s Internet address and the receiver’s address. Each of these packets can arrive in an order different from the order [in] which they were sent. The IP just delivers them and the Transmission Control Protocol TCP puts them in the correct order.”\(^{187}\)


\(^{180}\)ibid.

\(^{181}\)ibid.


Interoperability. “The ability of a system or a product to work with other systems or products without special effort on the part of the customer.”

Iris. “A means of controlling the size of the lens aperture and therefore the amount of light passing through the [camera] lens.”

Key fob. A small device that people often carry with their keys on a ring or a chain. It usually contains a passive radio frequency identification (RFID) tag that operates in much the same manner as a proximity card to communicate (via a reader pad) with a central server.

LAN (Local area network). “A short-distance data communications network (typically within a building or a campus) used to link together computers and peripheral devices.”

Latch. A mechanical device for keeping a door or a gate closed.

LCD (liquid crystal display). “An electro-optical amplitude modulator realized as a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. It is often utilized in battery-powered electronic devices because it uses very small amounts of electric power.”

LED (light-emitting diode). “A semiconductor diode that emits light when an electrical current is applied in the forward direction of the device, as in the simple LED circuit. The effect is a form of electroluminescence where incoherent and narrow-spectrum light is emitted.”

Lens. An “optical device for focusing a desired scene onto the imaging device” in a camera.

Mantrap. “A double-door booth or chamber that allows a person to enter at one end, undergo an access identification routine inside the booth, and if the routine is satisfied, the lock on the booth door at other end is released.” Also known as a sallyport or an interlock.

Masonry. “The building of structures from individual units laid in and bound together by mortar, and the term ‘masonry’ can also refer to the units themselves.”

Mass notification systems. Used during emergencies to supply real-time information and instructions to occupants or emergency personnel within a building or multiple buildings.

Master keying. “A method of keying locks which allows a single key to operate multiple locks, each of which will also operate with an individual change key. Master key systems are used primarily with pin and disc tumbler locks.”

---

Matrix switcher. “A device for switching more than one camera, VCR, DVR, video printer, and the like, to more than one monitor, VCR, DVR, video printer and so on.”199

Mobile phone (also known as a wireless phone, cell phone, or cellular telephone). “A short-range, electronic device used for mobile voice or data communication over a network of specialised base stations known as cell sites…. A satellite phone communicates directly with an artificial satellite, which in turn relays calls to a base station or another satellite phone.”200

Multiplexer. A device that can input the video signals from multiple cameras (up to 16) and produce two kinds of video outputs: one for viewing and one for recording. “The multiplexer operates by selecting a frame from each camera in sequence, digitizing it, and displaying it in a predefined location on the [video monitor] screen”201 or sending it to the recorder.

Pan or pan/tilt mechanisms. Peripheral devices that allow the camera or the housing to move along a horizontal plane (pan) or vertical plane (tilt). Pan moves the camera mounted to it from side to side. Pan/tilt moves the camera mounted to it from side to side and up and down.

Panic hardware. “A door-latching assembly incorporating an actuating member or bar that releases the latch bolt upon the application of a force in the direction of egress travel.”202

Passive vehicle barrier. “A vehicle barrier that is permanently deployed and does not require response to be effective.”203

Piggybacking. A security breach that occurs when a person who is authorized to access an area where access is being controlled permits, willingly or unconsciously, another individual to also access it without being subject to the verification procedure. Also known as tailgating.

Pinhole lens. “A fixed focal-length lens, for viewing through a very small aperture, used in discrete surveillance situations.”204

Pin tumbler lock cylinder. “A lock cylinder employing metal pins (tumblers) to prevent the rotation of the core until the correct key is inserted into the keyway. Small coil compression springs hold the pins in the locked position until the key is inserted.”205


Portal. An opening such as a gate, door, or entranceway.

Power transformer room. The room usually located underground where a utility company brings its high-voltage lines into a building for step-down transformers to convert high voltage to low voltage for use by the building.

Preset positioning. “A function of a pan and tilt unit, including the zoom lens, where a number of certain viewing positions can be stored in the system’s memory and recalled when required, either upon an alarm trigger, programmed or manual recall.” 207

Raised floor. As the names suggests, an underfloor space that can house electrical, plumbing, and air-conditioning systems, as well as cables, telephone wiring conduits, and computer wiring.

Rebar or reinforcing bar. “A common steel bar that is commonly used in reinforced concrete and reinforced masonry structures. It is usually formed from carbon steel, and is given ridges for better mechanical anchoring into the concrete. It can also be described as reinforcement or reinforcing steel.” 208

Repeater. “A radio device that retransmits received signals for the purpose of extending transmission distance or overcoming obstacles.” 209

Safe room. A shelter located inside or outside of a building, designed and constructed to protect against specific security and fire life safety threats.

Scissor stairs. Two stairways that are located close together in the same stair shaft. “The stairways are disposed adjacent to each other in parallel vertical planes and configured in an X shape. A fire wall separates each stairway.” 210

Security barrier. An obstruction designed to deter, detect, delay, and deny movement of persons, animals, vehicles, or materials into and out of an area. It may also obstruct audio or visual surveillance of an area.

Security command center. Focal point for a building’s security operations and communications. Also known as the security monitoring center and the security control center.

Sidelight panel. The section immediately adjacent to a door.

Smart card. Similar to a credit card with information stored on a microprocessor-type integrated-circuit chip embedded in the plastic card itself. “The card has both a coded memory and microprocessor intelligence. It can record card transactions [events] and store data.” 211

Split screen unit. “Equipment that simultaneously displays parts or more than one image on a single monitor.” 212

Stairs. “A series of steps leading from one level of floor to another, or leading to platforms, pits, boiler rooms, crossovers, or around machinery tanks and other equipment.” 213

Stairway. “A series of steps and landing having three or more rises constitutes stairs or a [a] stairway.” 214

Stairwell. “A compartment extending vertically through a building in which stairs are placed.” 215

214 ibid.
215 ibid.
Stand-off distance. “A distance maintained between a building or portion thereof and the potential location for an explosive detonation or other threat.”

Token. A physical security device required to operate a lock (for example, see key fob).

Transom. The section immediately above a door.

Transponder. “A wireless communications, monitoring, or control device that picks up and automatically responds to an incoming signal. The term is a contraction of the words transmitter and responder. Transponders can be either passive or active.”

Video analysis. “Involves the extraction of information from digital images by a method known as digital image processing.” Also known as video analytics or image analysis.

Video printer. “A device for converting a video signal into an image.”

Video switcher. “A device for switching more than one camera to one or more monitors manually, automatically or upon receipt of an alarm condition.”

View port. A small device installed in an opaque door to provide a clear view of the other side of the door (using a hollow end or peephole to look through and a lens at the other end to give a wide viewing angle). See door viewer.

Voice-over Internet protocol (VoIP). “A general term for a family of transmission technologies for the delivery of voice communications over the Internet or other packet-switched networks.”

WAN (wide area network). “A network of computers that are widely separated by distance.”

Won doors. Special accordion-style doors found in the elevator lobbies of some high-rise buildings.

Zoom lens. “A camera lens that can vary the focal length while keeping the object in focus, giving an impression of coming close to or going away from an object.”

Additional Reading


---


220 ibid.

221 ibid.


This page intentionally left blank
High-rise buildings have many types of fire life safety systems and equipment that can be deployed to address specific fire life safety threats. Their primary purpose is to help ensure that a building is safe to use, that occupants are able to escape safely and quickly in the event of a fire or other emergency, that first responders are able to gain access to all areas within and on the structure, and that appropriate control measures are rapidly initiated.

This chapter outlines the systems and equipment that may be found in a typical modern high-rise building. It is important to note that this outline is generic in nature. Because of the number of different model codes and standards, the chapter does not focus on the statutory requirements of any one code or standard; however, extensive reference is made to the National Fire Protection Association (NFPA*) National Fire Codes. To determine what is actually required at a specific site, one must review the laws, codes, and standards that have been specifically adopted by the authority that has jurisdiction.

Monitoring of Fire Life Safety Systems

The focal point for the fire life safety operations and communications of a building may be a simple local annunciator and control panel or a more complex and sophisticated fire command center, both of which will usually be located in the main floor lobby or in an adjoining room. The latter may be known as the fire control room, the central control station, the command center, the control center, the fire command station, or the fire control center (Figure 6–1).

In the event of a fire, the fire department will usually designate this area as its command post. If the fire command center is located in a separate room, it should be identified as such by a conspicuous sign on its door. (Some authorities discourage this for security reasons—in that case, the local fire department must be consulted and a nonpublic identifier established.) The door should be kept locked at all times. The fire command center (or the local annunciator and control panel) will usually be located near or adjacent to the main entrance to the building; the fire authority that has jurisdiction will oversee its actual location and accessibility.

The fire command center is separated from the remainder of the building by fire-resistant construction, with all openings protected by assemblies with a fire-resistant rating specified by the local authority that has jurisdiction. The fire command center

*All NFPA information in this chapter is used with permission of the National Fire Protection Association, Quincy, MA.
should not be used for any other purpose than that for which it is designed. It usually will contain the following as a minimum:

- Voice communication and building public address (PA) system.
- Fire department voice communication systems.
- Public telephone for fire department use.
- Stairwell intercom systems.
- Fire detection and alarm system annunciator and control panels.
- Sprinkler control valve, airflow detector, and fire pump status panels.
- Other fire protection equipment and system annunciator or status indicators.
- Air-handling system controls and status indicators.
- Elevator status panel displaying elevator operations.
- Emergency and standby power systems status indicators.
- Controls for simultaneously unlocking stairwell doors locked from stairwell side
- Building and elevator keys.
- A copy of the Building Emergency Procedures Manual (as described in Chapter 9).
- A computer terminal and printer are often provided for the fire life safety systems.

All fire life safety systems should be listed or certified by the appropriate agencies as having met minimum standards.
Voice Communication and Building Public Address System

The voice communication and building PA system is a one-way system providing a means of communication from the fire command center to the occupants of the building. Each system will vary depending on the manufacturer and system models. However, it should have adequate power and speaker quality so that audio messages can be clearly and distinctly heard in all normally occupied areas of the building (including elevator cars and stairwells).

Usually, the operator manually selects the required zones (ordinarily, separate paging zones will be designated for each floor and for stairwells and elevators) and speaks loudly and clearly into a microphone that connects to these areas (Figure 6–2).

The system almost always allows communication to individual floors or the whole building at once. (This feature has sometimes led to problems in high-rise buildings. By mistake, operators have activated the “ALL CALL” feature of the panel, thereby causing the audible fire signal to sound on all floors. To reduce the chance of accidentally activating this feature, some buildings, with the approval of the local fire authority that has jurisdiction, install a molded polycarbonate cover over the “ALL CALL” button or switch. This cover is hinged to the panel and if the “ALL CALL” feature needs to be used, the operator swings the cover open to access the appropriate button or switch.) Systems usually are designed so that the sounding of a fire alarm signal in any particular area or floor will not prevent voice communication to other floors or areas; also, when the voice communication system is selected for a zone in which a fire alarm is already sounding, the audible alarm will automatically discontinue when the microphone is activated in order for the operator to speak.

FIGURE 6–2 A building fire safety director identifies the type of fire detection device in alarm and its location before making a public address announcement to the occupants of a modern high-rise building. Courtesy of SimplexGrinnell, a Tyco Company (www.simplexgrinnell.com).
Fire Department Voice Communication Systems

The fire department voice communication system is provided for fire department use. It enables two-way telephone communication between the fire command center and specified locations throughout the building where telephone jacks (refer to Figure 6–3, presented later) or handsets are installed. These locations include entries into stairwells on each floor, standby and emergency power rooms, elevator cars, elevator machine rooms, and passenger and service/freight elevator lobbies. In some cities, the systems permit simultaneous voice communication between six locations. If telephone jacks rather than fixed handsets are installed, the hand-held telephone sets normally will be kept in the fire command center, one being permanently installed with a cord of sufficient length to reach all areas. Some authorities that have jurisdiction permit the use of an approved fire department radio communication system operable to all locations within the structure.

Public Telephone for Fire Department Use

A public telephone designated for fire department use allows controlled access to the public telephone system. Its callback number should be clearly marked on the handset. Often this telephone is red in color to indicate that it is to be used for emergency purposes only.

Stairwell Intercom Systems

An intercom is a two-way device enabling communication between the fire command center, or other constantly monitored location, and other specified locations throughout the building. From a life safety standpoint, intercoms are often installed in stairwells for the use of occupants who are inside the stairwell and need assistance. They are usually mounted on the wall just inside the stairwell entrance and are operated by pressing a button and speaking while the button is depressed.

The intercom should have its floor number and location marked on it, along with written instructions on how to operate it. Some jurisdictions require that older high-rise buildings that do not have stairwell door automatic unlocking systems that activate (i.e., unlock the stairwell doors) when a fire alarm occurs provide two-way intercoms inside the stairwells at every fifth floor. This is to ensure that any occupant trapped inside the stairwell would have a means of communicating with building staff to notify them of the situation. Someone could then come and open a stairwell door near the location, thus eliminating the need for the occupant to walk all the way down the stairwell to exit the building.

Fire Detection and Alarm System Annunciator and Control Panels

Annunciator and control panels monitor and control the fire detection and fire alarm system devices located throughout the building. According to Wilson,

Fire alarm systems are classified according to the functions they are expected to perform.... The basic components of each system are:

A system control unit.
A primary, or main, power supply.
A secondary, or standby, power supply.

One or more initiating device circuits or signaling line circuits to which manual fire alarm boxes, sprinkler waterflow alarm initiating devices, automatic fire detectors, and other fire alarm initiating devices are connected.

One or more fire alarm notification appliance circuits to which audible and visible fire alarm notification appliances, such as bells, horns, [sirens and whoopers], stroboscopic lamps, and speakers, are connected.

Many systems also have an off-premises connection to a central station, proprietary supervising station, remote supervising station, or public service fire serve communication center by means of an auxiliary fire alarm system.¹

The secondary power supply, mentioned earlier, is an emergency power system from which power is automatically transferred. Examples of emergency power supplies include a storage battery or group of batteries, a generator driven by a fuel-supplied prime mover, or an uninterruptible power supply (UPS);¹ also, there may be other means sanctioned by the authority that has jurisdiction. (Emergency power systems will be elaborated on later in this chapter.) The secondary power supply may also energize trouble signals in the fire detection and fire alarm system. A trouble signal initiated by the system will occur due to either a problem with the fire protective signaling system equipment itself (such as a device or the wiring associated with the system) or the failure of the system’s primary power supply.

According to Bryan, “The primary purpose of a fire detection system is to respond to a fire, and to transform this response into a visual-audible signal which should alert the building’s occupants and the fire department that a fire has been initiated. The fire detection system is intended to respond to the initial signs, signals, or stimuli which indicates that a fire has begun.”² When a fire detection device is activated, a signal immediately will be sent to the fire command center. The signal may also be sent to the security command center, depending on the onsite monitoring arrangements, or to an offsite central station.

In some modern high-rises, alarm signals are graphically displayed on a video monitor with operator input using a touch screen, a mouse, or keyboard commands, or displayed on a screen located on the fire annunciator panel itself. Screen information, such as floor plans and graphic maps with flashing icons symbolizing event locations, fire safety symbols, and programmable step-by-step emergency instructions, can be customized for a specific building. Using graphic systems can help train operators quickly and thoroughly decrease an operator’s response time and increase adherence to established alarm response procedures.

¹ Moore WD. Fire alarm systems. In: Fire Protection Handbook. 20th ed. Quincy, MA: National Fire Protection Association; 2008:14–15. This quote has been slightly modified. The words “sirens and whoopers” have been added.

¹ Uninterruptible power supply (UPS), “a system that provides continuous power to an alternating current (AC) line within prescribed plus or minus tolerances. A UPS protects against over-voltage conditions and brownouts. Also called uninterruptible power source” (ASIS Glossary of Terms. December 19, 2007. <www.asisonline.org/library/glossary/b.pdf>); ASIS International; November 19, 2008). “It differs from an auxiliary power supply or standby generator, which does not provide instant protection from a momentary power interruption. A UPS, however, can be used to provide uninterrupted power to equipment, typically for 5-15 minutes until a generator can be turned on or utility power is restored.” (Uninterruptible power supply. Wikipedia. November 16, 2008. <http://en.wikipedia.org/wiki/Uninterruptible_power_supply>); November 19, 2008.)

The annunciator and control panels that monitor and control the fire protection systems will take various forms depending on the designer and manufacturer of the equipment and on the requirements of the authority that has jurisdiction.

Manual Fire Alarm Stations

A manual fire alarm station (i.e., manually activated fire alarm station), sometimes called a manual fire alarm box, manual pull station, or manual pull alarm, is “a manually operated device used to initiate an alarm signal.” According to NFPA 101, *Life Safety Code*,

Section 9.6.2.3 Manual fire alarm boxes shall be provided in the natural exit access path near each required exit from an area, unless modified by another section of this Code.

Section 9.6.2.4 Additional manual fire alarm boxes shall be located so that, from any part of the building, no horizontal distance on the same floor exceeding 200 feet (60 m.) shall be traversed to reach a manual fire alarm box.

Section 9.6.2.6 Each manual fire alarm box on a system shall be accessible, unobstructed, and visible.4

However, according to Bill Webb, former chief engineer of Rolf Jensen and Associates, some authorities discourage or prohibit the use of manual fire alarm stations.5

In a typical modern high-rise, manual fire alarm stations (Figure 6–3) are mounted on walls located in the common area corridors adjacent to the stairwells, in passenger and service/freight elevator lobbies, and at the roof adjacent to the exterior door of each stairwell.

Sequence of Operations

A manual fire alarm station may be activated by depressing, lifting, or pulling a lever or a switch or by breaking a thin glass plate and pulling a lever or a switch. In modern high-rise buildings, this usually will cause the following sequence of operations:

- An audible signal, and a visual signal—usually a strobe (electronic device producing flashing lights) (Figure 6–4)—on the floor on which it is initiated (in some buildings a signal will simultaneously occur on the floor where the alarm initiated, on one or two floors above this floor, and on one or two floors below this floor)
- An audible and visual signal at an offsite central monitoring station
- A live voice or prerecorded evacuation message to the occupants (some fire departments do not allow an automatically activated prerecorded message, as it may not be appropriate for every alarm situation)
• Shutdown of the air-handling—heating, ventilation, and air-conditioning (HVAC)—system on the floor in alarm, and in other areas as designated by the system
• Activation of the smoke control system on the floor in alarm
• Activation of building stairwell and elevator shaft pressurization fans
• Release of hold-open devices for doors (usually elevator lobby doors) on the floor in alarm
• Release of all stairwell door locks in the building

Municipal Fire Alarm Box

Some municipalities provide a means for a fire alarm to be manually sent directly to the local public fire service from a municipal fire alarm box (street box) housed in an enclosure in the street outside of the building. Many city fire departments have eliminated these boxes because people have transmitted alarms when no fire conditions existed. The need for these public reporting stations has been largely eliminated by the widespread use of local emergency telephone services using the public telephone network emergency telephone number* if this service is available.

Automatic Detection Systems

“The automatic fire detector is designed to respond and transmit a signal via a pneumatic, electric, hydraulic, or mechanical communications system. The automatic fire detector is programmed to respond when the appropriate physical-chemical condition exceeds certain response thresholds.”

A variety of detectors exist to sense the presence of smoke, heat, flame, and gas. The selection of the appropriate detector depends on such factors as the type of combustion or gaseous buildup that may be anticipated, the intended location and purpose of the detector, the architectural configuration, and the presence of air currents caused by HVAC systems.

The selection, installation, and maintenance of the appropriate detector are all critical factors in avoiding false alarms. A false alarm occurs when a detector indicates that there is a fire but in reality there is none. Causes of false alarms include a lack of detector maintenance, short-term electrical interference in the communications systems sending the signal back to the fire command center (such interference typically can be eliminated by initiating an alarm verification feature), and, to a much lesser degree, faults in the detector itself. A false alarm may also be caused by conditions that appear to indicate a fire but actually are caused by the occupants themselves, such as an occupant smoking a pipe, a cigar, or a cigarette and blowing the smoke toward a smoke

*“Many countries’ public telephone networks have a single emergency telephone number, sometimes known as the universal emergency telephone number or occasionally the emergency services number, that allows a caller to contact local emergency services for assistance. The emergency telephone number may differ from country to country. It is typically a three-digit number so that it can be easily remembered and dialed quickly. Some countries have a different emergency number for each of the different emergency services; these often differ only by the last digit.” (Emergency telephone number. Wikipedia. October 21, 2008. <http://en.wikipedia.org/wiki/Emergency_call>; October 25, 2008.) “The ability to dial a single number to report emergencies was first used in Great Britain, in 1937. The British could dial 999 to call for police, medical or fire departments, from anywhere in the country. In 1958, the American Congress first investigated a universal emergency number for the United States and finally passed the legal mandate in 1967. The very first American 911 call was placed on February 16, 1968.” Bellis M. The History of 911 Emergency Calls. About.com: Inventors. <http://inventors.about.com/library/inventors/bl911.htm>; June 1, 2008.

detector. Closely aligned in meaning to a false alarm is a nuisance alarm. A nuisance alarm is “any alarm caused by mechanical failure, malfunction, improper installation, or lack of proper maintenance, or any alarm activated by a cause that cannot be determined.”

Smoke Detectors

A smoke detector is “a device that detects visible or invisible particles of combustion.” Smoke is often the first sign that a fire is occurring; therefore, an automatic detection system based on smoke detectors is a valuable tool in the early detection of fire. Smoke is “the total airborne effluent from heating or burning a material.” Smoke detectors are commonly classified by their mode of operation.

Ionization Smoke Detector

Ionization smoke detection (see an ionization smoke detector in Figure 6–5) is “the principle of using a small amount of radioactive material to ionize the air between two differentially charged electrodes to sense the presence of smoke particles. Smoke particles entering the ionization volume decrease the conductance of the air by reducing ion mobility. The reduced conductance signal is processed and used to convey an alarm condition when it meets preset criteria” (Figure 6–6).

“As a class, ionization smoke detectors are spot-type detectors, which provide somewhat faster response to high-energy (flaming) fires, since they respond to the number

---

8 ibid.
density of smoke particles, and such fires produce large numbers of relatively small particles.”

**Photoelectric Smoke Detector**

Photoelectric smoke detection (see the photoelectric smoke detector presented in Figure 6–7) uses light to detect visible smoke particles produced by burning material. It is designed to detect smoke when smoke either obscures a light beam (thereby reducing the amount of light received by a photosensitive device) (Figure 6–8) or the smoke scatters a light beam (thereby causing the light to fall on a photosensitive device that would not usually receive light when smoke was not present) (Figure 6–9). The former is known as photoelectric light obscuration smoke detection and the latter as photoelectric...

---

light-scattering smoke detection. \(^{12}\) “The light signal is processed and used to convey an alarm condition when it meets preset criteria.” \(^{13}\)

“Photoelectric smoke detectors, as a class, provide superior response to low-energy (smoldering) fires, since they respond to the optical density of smoke, and such fires produce a preponderance of visible size range smoke particles.” \(^{14}\)

**Placement of Smoke Detectors**

Smoke detectors generally are located in open areas, spaces above suspended ceilings, spaces under raised floors (particularly in computer rooms and data centers), cafeteria areas, air duct systems, passenger and service/freight elevator lobbies, elevator shafts, elevator machine rooms, enclosed stairways, dumbwaiter shafts, chutes, and electrical and mechanical equipment rooms. The specific locations and spacing of smoke detectors are determined by an assessment of local laws, codes, and standards, and engineering issues. Factors include “ceiling shape and surface, ceiling height, configuration of contents in the area to be protected, burning characteristics of the combustible materials present, ventilation, and the ambient environment.” \(^{15}\)

---


\(^{13}\) ibid.


Of course, all locations chosen for the installation of smoke detectors must be accessible for periodic device testing and maintenance. If the detectors are located in areas where they may be subject to mechanical damage, they should also be adequately protected; for example, some smoke detectors may have a protective wire-frame covering.

Addressable Devices
The use of multiple smoke detectors in high-rise buildings has been made practicable by the development of the addressable system. An addressable device is “a fire alarm system component with discrete identification that can have its status individually identified or that is used to individually control other functions.” When an alarm occurs, an addressable system can determine which particular device and its address or location that is causing an alarm. This permits new systems to be zoned by device rather than by floor. For instance, if an elevator lobby smoke detector is activated, all elevators are recalled in the manner described in the section titled “Controls in Elevator Lobbies,” presented later in this chapter. The sequence of smoke detector operation in a typical modern high-rise building is detailed in Table 6–1.

Heat Detectors
“Heat detectors are the oldest type of automatic fire detection device. They began with the development of automatic sprinklers in the 1860s.” According to Dungan,

Heat detectors are very reliable and have the lowest false alarm rate of all automatic fire detector devices. They are best suited for fire detection in small confined spaces where rapidly building high-heat-output fires are expected, in areas where ambient conditions would not allow the use of other fire protection devices, or where very early warning of fire is not required. Heat detectors are generally located on or near the ceiling and respond primarily to the convected thermal energy of a fire. They operate either when the detecting element reaches a predetermined fixed temperature or when a specified rate of temperature change occurs.

There are combination heat detectors that, for example, merge the features of both fixed-temperature and rate-of-rise devices. The fixed-temperature element senses a slow-developing fire when a predetermined temperature has been attained; the rate-of-rise element senses a rapidly developing fire (Figure 6–10). “Heat detectors can perform most of the same duties as smoke detectors but usually with a much longer time lag. An extended time lag is sometimes desirable, such as in the opening of a sprinkler, or the release of a special extinguishing agent.”

The sequence of heat detector system operation in a typical modern high-rise building is detailed in Table 6–1.

---

18 ibid.
<table>
<thead>
<tr>
<th>Manual Fire Alarm Station</th>
<th>Area Smoke Detector</th>
<th>Duct Smoke Detector</th>
<th>Elevator Lobby Smoke Detectors</th>
<th>Elevator Shaft Smoke Detector</th>
<th>Heat Detector</th>
<th>Sprinkler Waterflow Device</th>
<th>Sprinkler Valve Tamper Device</th>
<th>Special Extinguishing Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annunciate audible and visual signal at fire command center (alarm and trouble)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Annunciate signal at offsite monitoring station (alarm and trouble)</td>
<td>Depends on the system</td>
<td>Depends on the system</td>
<td>Depends on the system</td>
<td>Depends on the system</td>
<td>Depends on the system</td>
<td>Depends on the system</td>
<td>Depends on the system</td>
<td>Depends on the system</td>
</tr>
<tr>
<td>Activate audible and visual alarm on floor of alarm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Shutdown air-handling systems on floor of alarm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Activate smoke evacuation system on floor of alarm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Activate all stair shaft pressurization fans in building</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Release electromagnetic held-open doors on floor of alarm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Release all stairwell door locks in building</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Recall all elevators serving floor of alarm</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Open elevator shaft smoke damper</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Release approved elevator security door locks</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Gas Detectors

Gas detectors are automatic detection devices that monitor low-level concentrations of combustible gases such as methane, ethane, natural gas, and propane. When concentrations reach a predetermined level, an alarm is triggered to advise building occupants of the possible hazard. For example, methane gas seeps up out of the ground in some areas; as a result, methane gas detection systems have been installed as part of some high-rise life safety systems. If a certain concentration of methane gas is detected, an initial automatic alarm will notify security and engineering staff that further investigation is required. If the concentration continues to increase and reaches a predetermined level, the system automatically initiates another alarm indicating that the fire department and building occupants should be notified immediately of the potential hazard.

Automatic Sprinkler Systems

“In 1872, Philip Pratt of Massachusetts is credited with developing the first automatic sprinkler system in the United States.... [T]he first practical sprinkler was patented by Henry Parmelee of Connecticut in 1874. Parmelee improved on his device in 1875 and 1878 and it became the first sprinkler used extensively.”

An automatic sprinkler is “a device for automatically distributing water on a fire in sufficient quantity either to extinguish it entirely or to prevent its spread in the event that the initial fire is out of range, or is a type of fire that cannot be extinguished by water.” As Huggins explained,

A sprinkler system is defined as a combination of underground and overhead piping that is connected to an automatic water supply. The piping is specially sized or hydraulically designed with that portion of the piping within the building

---

generally located overhead. Sprinklers are attached to the overhead piping in a systematic pattern and a valve controlling each riser is located either directly on the system riser or in the supply piping. The system is usually activated by heat from a fire and discharges water over the fire area. A device actuating an alarm when the system operates is located on the system riser.\textsuperscript{22}

Automatic sprinklers not only are essential in new high-rise buildings, but in many cities it is mandated by code that existing high-rises be retrofitted with automatic sprinkler systems.

The prime motivational factor for the installation of sprinkler systems is that in the time that they have been in existence, they have proven to be a most effective means of controlling fires. The chance of death or extensive property damage is reduced substantially in a fully sprinklered building. “The NFPA has no record of a fire killing more than two people in a fully sprinklered public assembly, educational, institutional, or residential building in which the sprinkler system was operating properly, except in the case of explosions and flash fires and in instances in which fire brigade members or employees were killed during fire suppression operations.”\textsuperscript{23} In a later report, Dr. Hall, the NFPA’s assistant vice president for fire analysis and research, stated that “When sprinklers are present, the chances of dying in a fire and property loss per fire are cut by one-to two-thirds, compared to fires reported to fire departments where sprinklers are not present.”\textsuperscript{24}

The following description of automatic sprinkler systems was compiled using NFPA 13, Standard for the Installation of Sprinkler Systems, and the Fire Protection Handbook\textsuperscript{25} as references.

**Water Supply for Sprinklers**

For automatic sprinklers to operate, there must be a supply of water to the sprinkler that opens to extinguish or control fire and prevent it from spreading. This water may come from a variety of sources such as public water systems (usually considered the principal or primary water supply) and storage tanks of different types.

**Gravity Tanks**

Gravity tanks are tower- or roof-mounted water reservoirs that are not likely to be used for modern high-rise buildings.

---


Suction Tanks
Suction tanks, equipped with automatically operated fire pump(s), are increasingly used as a secondary water supply and sometimes, where the authority that has jurisdiction permits, as a principal water supply. These tanks are normally constructed of concrete, steel, or fiberglass and may be located directly beneath a fire pump(s).

Pressure Tanks
Pressure tanks are pressurized water reservoirs used to supply a limited amount of water for building sprinkler systems. Each tank is located above the highest sprinkler heads. When the public water pressure is too low to supply water to sprinklers on upper high-rise floors, the pressure tanks are used until water can be pumped into the sprinkler system through fire department connections (these connections are explained later).

The selection and location of these tanks and automatic fire pumps are based on the size and height of the building, its type of tenancy, and pattern of use.

Fire Pump
A fire pump is a mechanical device for improving the water supply pressure from public water systems and storage tanks. In modern high-rise buildings, centrifugal force is primarily responsible for developing fire pump pressure. The pumps are driven by electric motors (Figure 6–11) or by internal combustion engines fueled by diesel oil. Fire pumps usually are housed in areas protected from the possible effects of fires, freezing temperatures, explosions, and natural disasters such as floods and earthquakes.

Fire pumps usually are designed to start automatically when water pressure in the fire protection system drops to a predetermined level and shut down manually when their services are no longer needed.

In addition to automatic fire pumps, there are pressure maintenance jockey pumps. These small pumps automatically maintain the operating pressure in the fire protection system. To avoid starting the fire pump engine when there are small fluctuations in pressure, the jockey pump automatically starts, boosts the pressure to the correct level, and then shuts itself down.

Fire Department Connections
In addition to the aforementioned water sources, on the exterior of the building there are fire department connections that the fire department can access to pump water into the sprinkler system. These connections are required by NFPA 13, Standard for the Installation of Sprinkler Systems. They are used when the building water supply system is unable to provide water at sufficient pressure for the sprinkler system to discharge and disperse water effectively.

These fire department connections are easily accessed, usually being situated on the street side of the building, and are conspicuously marked with signs. Examples of the signs are “AUTOSPKR.,” “OPENSPKR.,” or “AUTOSPKR. and STAND-PIPE.” The connections often are fitted with protective caps that the fire department can easily remove to attach hoses (Figure 6–12).

*“Some [fire pumps] are called booster pumps because they ‘boost’ the pressure of the public supply”
FIGURE 6–11 Two electric fire pumps located alongside each other in the fire pump room of a high-rise building. Photograph by Roger Flores.

FIGURE 6–12 Fire department connections serving high, mid, and low zones of a high-rise building. Photograph by Roger Flores.
The fire department obtains water for these connections from water hydrants using fire department pumpers. A fire hydrant (Figure 6–13) is “a valved connection on a water supply system having one or more outlets and that is used to supply hose and fire department pumpers with water.”26 Fire hydrants generally are located along the street and often close to intersections to meet the needs of adjoining structures.

**Sprinkler Pipes**

In the typical modern high-rise, water is vertically transported upward in the building through a sprinkler system riser or vertical pipe located in each stairwell. A system of overhead piping on each floor horizontally connects the riser to the sprinklers that are located at regular intervals along the pipes. In steel-framed buildings, the horizontal pipes themselves are commonly located in the concealed space throughout the whole floor area. They are attached to the floor above using hangers and clamps (Figure 6–14).

**Sprinklers**

Various types of sprinklers are used in high-rise buildings.

*Standard Spray Sprinklers*

Standard spray sprinklers are installed in an upright or pendent position.27 This type of sprinkler may visibly protrude through the ceiling, be recessed with part or most of it

---

mounted in a recessed housing (Figure 6–15), or is concealed in the ceiling and hidden from view by a cover plate\(^\text{28}\) (Figure 6–16). (When a predetermined temperature is attained, the cover plate drops away leaving the sprinkler head exposed. The plate is often marked “Do Not Paint” to avoid the problem of the cap being painted over and thereby possibly adhering to the ceiling.)

**Quick-Response and Residential Sprinklers**

“A quick response sprinkler is a type of spray sprinkler that meets the fast response criteria of NFPA 13, *Standard for the Installation of Sprinkler Systems*, and that has special low-mass fusible links or bulbs that make the time of temperature actuation much

\(^{28}\)ibid., pp. 16–21.
less than that of a sprinkler with a conventional operating element. These sprinklers are specifically listed as a quick-response sprinkler for their intended use.  

“Residential sprinklers are sprinklers that have been specifically listed for use in residential occupancies. These fast-response sprinklers have special low-mass fusible links or bulbs that make the time of temperature actuation much less than that of a sprinkler with a conventional operating element. Residential sprinklers also have different discharge characteristics than spray sprinklers. They are required to throw water within 18 in. (457 mm) of the ceiling. This high-wall wetting pattern, along with the faster response, helps the residential sprinkler control or suppress typical residential fires with flows much lower than standard spray sprinklers.”

According to Madrzykowski and Fleming,

*It is important to recognize that, in addition to their fast-response characteristics, residential sprinklers have a special water distribution pattern. Because the effective control of residential fires often depends on a single sprinkler in the room of fire origin, the distribution of residential sprinklers must be more uniform than that of standard spray sprinklers, which in large areas can rely on the overlapping patterns of several sprinklers to make up for voids. Additionally, residential sprinklers must protect sofas, drapes, and similar furnishings at the periphery of the room. In their discharge patterns, therefore, sprinklers must not only be capable of delivering water to the walls of their assigned areas but also be high enough up on the walls to prevent the fire from getting “above” the sprinklers. The water delivered close to the ceiling not only protects the portion of the wall close to the ceiling but also enhances the capacity of the spray to cool gases at the ceiling level, thus reducing the likelihood of excessive sprinkler openings.*

**Sidewall Sprinklers**

“Sidewall sprinklers (Figure 6–17) have the components of standard sprinklers except for a special deflector, which discharges most of the water toward one side in a pattern

---

29 Comment by Robert E. Solomon, P.E., assistant vice president for building and life safety codes, NFPA International, Quincy, MA, when reviewing this chapter (January 2009).


somewhat resembling one quarter of a sphere. A small proportion of the discharge wets the wall behind the sprinkler. Located and mounted either vertically or horizontally along the junction between a ceiling and wall, sidewall sprinklers provide protection adequate for light-hazard occupancies, such as hotel lobbies, dining rooms, and executive offices. Sidewall sprinklers are generally used where pipe would be difficult to install in a ceiling. This concern might be the case with certain types of ceiling construction or in retrofit situations in which the building owner does not want to disturb asbestos above an existing ceiling.”

**Extended Coverage Sidewall Sprinklers**

“Extended coverage sidewall sprinklers are used in the horizontal position. They have larger areas of coverage than the areas of coverage allowed for standard sidewall sprinklers. They may be used in light-hazard occupancies, particularly in hotels and similar occupancies where a sprinkler system can be installed in an existing building without having piping exposed in living areas, which could be objectionable aesthetically.”

Some extended coverage quick response sidewall sprinklers are concealed (Figure 6–18). “The plate, while maintaining a fast response sensitivity, has been specifically designed without vent holes to increase its aesthetic appeal while helping to avoid objects from being hung from the sprinkler (i.e., garment bags, clothes hangers, etc.) that might otherwise cause an inadvertent operation. They are designed for installation along a wall or the side of a beam and beneath a smooth and level ceiling. Horizontal sidewall sprinklers are commonly used in lieu of pendent or upright sprinklers because

---


33 ibid.
of the aesthetics or building construction considerations where piping across the ceiling is not desirable.”

How Automatic Sprinklers Work

An automatic sprinkler is “a device consisting of a threaded orifice, a cap, supporting arms, a fusible element, and a deflector, which when attached to a sprinkler system branch line discharges water in a specific pattern onto a fire.” “Under normal conditions, the discharge of water from an automatic sprinkler is restrained by a cap or valve held tightly against the orifice by a system of levers and links or other releasing devices pressing down on the cap and anchored firmly by struts on the sprinkler.”

A common sprinkler, called a fusible sprinkler, contains a fusible metal that melts rapidly at a certain temperature and fuses, thereby permitting a cover over an opening in the sprinkler to drop away, water to flow, and a waterflow indicator to initiate a fire alarm. “A second style of operating element uses a frangible bulb. The small bulb, usually of glass, contains a liquid that does not completely fill the bulb, leaving a small air bubble trapped in it. As heat expands the liquid, the bubble is compressed and finally absorbed by the liquid. Once the bubble disappears, the pressure rises substantially, and the bulb shatters, releasing the valve cap. The exact operating temperature is regulated by adjusting the amount of liquid and the size of the bubble when the bulb is sealed.”

“Initiation of the alarm signal shall occur within 90 seconds of waterflow at the alarm-initiating device when flow occurs that is equal to or greater than that from a single sprinkler of the smallest orifice size installed in the system. Movement of water due to waste, surges, or variable pressure shall not be indicated.” The reason for the

---

37 ibid.
90-second delay is to avoid false alarms by allowing sufficient time to establish that a stable water flow has been achieved. The fire alarm is automatically transmitted to the fire command center and possibly to an offsite central monitoring station, sounds on the floor where the sprinkler water flow has occurred (and possibly on one or two floors above and below the alarm floor), and sounds a sprinkler fire-alarm bell located on the exterior of the building near ground level.

Types of Automatic Sprinkler Systems

Three types of sprinkler systems are found in commercial high-rise buildings: wet pipe, dry pipe, and preaction.

**Wet-Pipe System**

The wet-pipe system is the most common sprinkler system used in high-rise buildings. In the event of a fire, if the temperature exceeds a predetermined point, the sprinkler activates, and water contained in the pipe (which is connected to the water supply) is immediately discharged on the fire. A prerequisite of this system is that the area in which it is installed must be kept at temperatures above freezing.

**Dry-Pipe System**

In a dry-pipe system, in the event of a fire, if the temperature exceeds a predetermined point, the sprinkler activates, and pressurized air contained in the pipe escapes, permitting a dry-pipe valve to open; water then enters the sprinkler piping and flows out of the open sprinkler.

This type of system is used in unheated areas. If water were contained in a sprinkler pipe at low temperatures, it could freeze, thereby rendering the system ineffective. Because most commercial high-rise buildings are temperature-controlled, few of these more expensive dry-pipe systems are used in them, except possibly in garage or loading dock areas.

**Preaction System**

The preaction system works on the principle that, in the event of a fire, an automatic fire detection device (such as a smoke or a heat detector) located near the sprinkler will be activated. This in turn will allow water to enter the piping before the sprinkler is activated. Then, when the sprinkler opens after a predetermined high temperature is reached, water can immediately flow out of it.

---

*The other type, “deluge systems, as the name implies, deliver large quantities of water over specified areas in a relatively short period of time. These systems are used to protect against rapidly growing and spreading fires. Sprinklers used in a deluge system do not contain thermally sensitive operating elements and are referred to as open sprinklers. A deluge valve controls the system water supply and is activated by a supplemental fire detection system. Because open sprinklers are employed, system piping is at atmospheric pressure. As water reaches each sprinkler in the system, it is immediately discharged from the system. The nature of this system makes it appropriate for facilities in which significant amounts of highly combustible materials are present” (Huggins R. Automatic sprinkler systems. In: Fire Protection Handbook. 20th ed. Quincy, MA: National Fire Protection Association; 2008:16–37).*
This system is used in areas such as computer rooms and data centers where there is great concern for the accidental (and unlikely) discharge of water, which could damage, disable, or destroy computers or other valuable electronic equipment.

Supervision and Manual Operation of the Automatic Sprinkler System

A sprinkler control valve is provided on each floor in the stairwell(s) so that the automatic sprinkler system can be manually shut down for that floor. A looped sprinkler system means that the piping is continuous throughout a floor and a sprinkler control valve is located in each stairwell. To manually shut down the looped sprinkler system for a floor, the control valve in each stairwell must be shut down. Under normal conditions, the sprinkler control valve remains in the OPEN position. (To avoid malicious tampering with the sprinkler control valve, it is generally recommended that the valve be maintained in the open position using a chain and a padlock. An authorized person needing to shut the control valve can access it by unlocking the padlock. If this cannot be done in a timely manner, the chain can be cut.)

The sprinkler control valve is fitted with a supervisory signal-initiating device. Whenever the valve is moved from its normal position or moved back to its normal position, separate and distinct signals are initiated and immediately sent to the fire command center.

The supervisory signal-initiating device that monitors a sprinkler control valve, the waterflow switch, and the hose connection and valve for a combined sprinkler and standpipe riser are shown in Figure 6–19.

Standpipe and Hose Systems

Before proceeding further, it is appropriate to discuss standpipe and hose systems. A standpipe system is “an arrangement of piping, valves, hose connections, and allied equipment installed in a building or structure”39 designed to vertically transfer water to upper floors of the building so that the water can be used to fight fires manually using fire hoses (Figure 6–20). The standpipe system is another tool that can be used by trained building personnel or members of the fire department to combat fires. “Even in buildings that are protected by automatic sprinklers, standpipe systems can play an important role in building fire safety by serving as a backup for, and complement to, sprinklers.”40

Standpipe systems are subdivided into “classes” and “types.”

Classes of Standpipe Systems

“The process of designing a standpipe system begins with determining the intended use, that is, whether it is for (1) full scale fire fighting, (2) first-aid fire fighting or (3) both.”41

---

41ibid.
There are three classes of standpipe systems classified according to the service for which they are designed.

**Class I Systems**
Class I standpipe systems provide 21/2-in. (63.5-mm) hose connections for use by fire departments and those trained in handling heavy streams of water.

---


**A hose connection is the device used to connect a fire hose to the standpipe system.**
Use of a Class I system reduces the time and number of fire department personnel needed to attack a fire because hoses can be run within the building close to the fire rather than running extensive lines from exterior locations. Therefore, Class I systems are generally required in both sprinklered and non-sprinklered high-rise buildings.

**Class II Systems**
Class II standpipe systems provide 1 1/2-in. (38.1-mm) hose connections for use by trained building staff, occasionally by the fire department on arrival, and perhaps by building occupants before the fire department arrives. Typically each hose connection has a hose, a hose nozzle, and a hose rack installed on it.

The use of Class II systems with hoses preconnected to standpipe systems is becoming less prevalent because of two main concerns: whether untrained occupants can safely use a 100-ft (30.5-m) long hose providing water at a flow rate of 100 gal per min (378 liters per min), and whether it is a sound practice for occupants to be involved in fighting a fire instead of immediately evacuating an area. Many jurisdictions have entirely removed the requirement for occupant-use hose systems in facilities that are fully sprinklered.

**Class III Systems**
Class III standpipe systems provide both Class I and Class II hose connections for use by trained building staff and a larger volume of water for use by fire departments and those trained in handling heavy streams of water.
The use of Class III systems is becoming less prevalent because of the same concerns listed under “Class II Systems.”

Types of Standpipe Systems

Standpipe “types delineate the basic characteristics of systems: that is, whether the piping will be filled with water or not (wet versus dry), and whether the water supply for fire fighting will be automatically available or not (automatic, semiautomatic, or manual).”

In high-rise buildings there are three permissible standpipe systems. They are explained by Hague as follows,

**Automatic-wet systems** have piping that is filled with water at all times and have an automatically available water supply capable of supplying the water demand necessary for fire fighting. [A prerequisite of such a system is that the area in which it is installed be kept at temperatures above freezing.]

**Automatic-dry systems** have piping that is normally filled with pressurized air. These systems are arranged, through the use of devices such as a dry-pipe valve, to automatically admit water into system piping when a hose valve is opened, and they are connected to an automatically available water supply that is capable of supplying the water demand necessary for fire fighting.

**Semiautomatic-dry systems** have piping that is normally filled with air that may or may not be pressurized. These systems are arranged through the use of devices, such as a deluge valve, to admit water into system piping when a remote actuation device located at a hose station, such as a pull station, is operated. They also have a preconnected water supply that is capable of supplying the water demand necessary for fire fighting.

The automatic-wet standpipe system is most commonly installed in modern high-rise buildings with a fixed water supply not exposed to freezing. It is considered more effective in fighting fires than the other two systems.

Zoning in Tall Buildings

In tall buildings, to keep water pressures within a safety limit and, for example, to reduce the possibility of hoses attached to the standpipe system bursting or being too difficult to handle, standpipe systems are frequently separated into multiple zones that limit the maximum height of the water column. “The goal of zoning is to limit the pressure that can be developed in system piping and at hose connections to reduce the need for high-pressure fittings and pressure-reducing valves.”

---


44 ibid., pp. 16–197.
Sprinkler Control Valve, Waterflow Detector, and Fire Pump Status Panels

In the fire command center, annunciator panels monitor the sprinkler control valves and waterflow detection devices located throughout the building, and the status of the fire pump(s). NFPA 101, *Life Safety Code*, requires that “High rise buildings shall be protected throughout by an approved, supervised automatic sprinkler system installed in accordance with Section 9.7 [Automatic Sprinklers and other Extinguishing Equipment]. A sprinkler control valve and a waterflow device shall be provided for each floor.”

Fire Department Connections

As with automatic sprinkler systems, on the exterior of the building there are connections that the fire department can access to pump water into the standpipe system. This may be required if the building water supply system is unable to provide water at sufficient pressure for the standpipe system to disperse water effectively, or if the standpipe system is a dry standpipe, one without a permanent water supply capable of sending water to the system on demand. If the building has two or more zones, each pressure zone should have its own fire department connection.

These fire department connections are easily accessed, usually on the street side of the building, and are conspicuously marked with a sign stating “STANDPIPE.” If the hose connection also supplies an automatic sprinkler system, the sign or combination of signs will specify both services, for example, “AUTOSPKR. and STANDPIPE.” The connections usually are fitted with protective caps that the fire department can easily remove to attach hoses. The fire department obtains water for these connections from water hydrants using fire department pumpers.

The sequence of automatic sprinkler and fire pump system operation in a typical modern high-rise building is detailed in Table 6–1.

Other Fire Protection Equipment and Systems

In addition to water, which is the primary extinguishing agent for building fires, there are other special extinguishing agents that may be employed in a high-rise building. Examples are carbon dioxide, halon and halon replacements, dry chemical, and wet chemical.

The authority that has jurisdiction will require the fire command center to supervise any special extinguishing systems located within the building.

Carbon Dioxide Systems

Carbon dioxide is one and half times heavier than air; it is a colorless, odorless, non-combustible, electrically nonconductive inert gas. Carbon dioxide can be used to extinguish fires because it reduces the amount of oxygen in the atmosphere to the point where combustion cannot be supported. Because it does not conduct electricity, it can be used on live electrical equipment. Also, it has the advantage that no cleanup is required after use because it does not leave behind a residue. One disadvantage, however, is that it produces solid dry ice particles on discharge that, because of their low temperature, may damage electrical equipment that they contact. Carbon dioxide is not used in normally occupied areas and would require a predischarge alarm because it may cause suffocation.

---

Four Basic Types of Application

NFPA 12, *Standard on Carbon Dioxide Extinguishing Systems*, recognizes four basic types of systems for applying carbon dioxide to extinguish fires:

1. A total flooding system involves a fixed quantity of carbon dioxide that is stored in containers and, on activation of a manual control station (equipped with a manual override) or an automatic detector, is discharged through fixed nozzles attached to fixed pipes into a fixed enclosure surrounding the fire hazard. Because carbon dioxide is dangerous to human beings, the enclosed area must be evacuated of all occupants before the gas is discharged.

2. A local application system involves a fixed quantity of carbon dioxide stored in containers and, on activation of a manual control station (equipped with a manual override) or an automatic detector. It is discharged directly onto the fire hazard through nozzles attached to fixed pipes.

3. A hand hose line system involves a fixed quantity of carbon dioxide that is stored in containers and has hand hose lines permanently attached and ready for immediate, usually manual, application to small fire hazards.

4. A standpipe system and mobile supply involves a mobile quantity of carbon dioxide that is stored in containers that in the event of a fire can be rapidly shifted into position and attached to a total flooding, local application, or hand hose line system.

Carbon dioxide can be used to suppress fires involving gas, flammable liquids, electrical equipment, and common combustible elements such as wood and paper.

Halon and Halon Replacement Systems

Since the evidence indicating the adverse effect of halon on the earth’s stratospheric ozone layer and the requirements of the 1993 Montreal Protocol, halon production has been curtailed. “Production of Halons 1301, 1211, and 2402 ceased in developed countries on January 1, 1994, and is currently being phased out in the last developing country that produces halons.... Since Halon 1301 is no longer manufactured in most industrialized nations new fire extinguishing systems that employ Halon 1301 are generally not allowed except for certain specific national defense applications.”

Halon

In buildings, halon can still be found in electrical switchgear rooms and in computer rooms and data centers. The total flooding system application involves a fixed quantity of halon® that is stored in containers and, on activation of a manual control station (equipped with a manual override) or an automatic fire detector, is discharged through fixed nozzles attached to fixed pipes into a fixed enclosure surrounding the fire hazard. Because it is not dangerous to human beings at low concentrations, halon can be discharged first, and then occupants can safely evacuate the area.

---


® Usually Halon 1301 within the United States.
The local application system involves a fixed quantity of halon® that is stored in containers and, on activation of a manual control station (equipped with a manual override) or an automatic fire detector, is discharged directly onto the fire hazard through nozzles attached to fixed pipes.

**Halon Replacements**

Inergen is an alternative agent for Halon 1301 in total-flooding operations within spaces or areas where people work and may be exposed to the agent on discharge. Produced by Ansul Fire Protection, it is a mixture of three inert gases: nitrogen, argon, and carbon dioxide. Like halon, it is colorless, odorless, noncorrosive, and electrically nonconductive. It does not raise the carbon dioxide level enough to prevent respiration and the absorption of oxygen (occupants, therefore, are still able to breathe); but it lowers the oxygen content below the level required for combustion.

Other halon replacement agents include FM-200, Triolide, Argonite, and Argon, 3M Novec 1230, and FE-36. These agents should never be used except with the approval of the authority that has jurisdiction.

**Dry Chemical Systems**

A dry chemical is a powder composed of small particles. “The principal base chemicals used in the production of currently available dry chemical extinguishing agents are sodium bicarbonate, potassium bicarbonate, potassium chloride, urea-potassium bicarbonate, and monoammonium phosphate. Various additives are mixed with these base materials to improve their storage, flow, and water repellency characteristics.”

The exact way dry chemical agents extinguish fires is not yet fully understood. According to NFPA 17, Standard for Dry Chemical Extinguishing Systems,

> It is now generally accepted that the flame extinguishing properties of dry chemicals are due to the interaction of the particles, which stops the chain reaction that takes place in flame combustion. Dry chemicals vary in their flame extinguishing effectiveness. Multipurpose dry chemical owes its effectiveness in extinguishing fires in ordinary combustibles, such as wood and paper, to the formation of a glow-retarding coating over the combustible material.

Dry chemical is primarily used as an extinguishing agent for flammable liquid fires. The dry chemical system is “a means of applying dry chemical that can be automatically or manually activated to discharge through a distribution system onto or into the protected hazard. The system includes auxiliary equipment.” Fixed nozzles or hand hose lines use expellant gas to discharge dry chemical.

---

* Often Halon 1211 within the United States.


51 Ibid., Section 3.4.
In high-rise buildings, dry chemical systems are used mainly for restaurant hood, duct, and cooking appliance systems located in kitchens and cafeterias. NFPA 17 outlines preengineered dry chemical systems for such equipment. These systems are activated automatically by a fusible link or heat detector located, in some cases, above each cooking appliance or group of appliances protected by a single nozzle or, in other cases, at or within the entrance to the ducting system. The systems are also designed so that when activated, the fuel or power to all the protected appliances will automatically shut down.\(^{52}\)

Because dry chemical is electrically nonconductive, it is also used for electrical equipment susceptible to flammable liquid fires. However, in telephone switching, computer rooms, and data centers, where there are sensitive electrical contacts and relays, its use is not recommended. Application in these areas may cause the equipment to malfunction. Dry chemical should be removed as quickly as possible from surfaces to which it has been applied because it may be corrosive.

**Wet Chemical Systems**

A wet chemical is defined by NFPA 17A, *Standard for Wet Chemical Extinguishing Systems*, as “normally an aqueous solution of organic or inorganic salts or a combination thereof that forms an extinguishing agent.”\(^{53}\)

> Its effect on fires in common cooking oils and fats is to combine with these materials to form a vapor suppression foam that floats on a liquid surface, such as in deep fat fryers, and effectively prevents reignition of the grease....

> Wet chemical solution applied to flammable liquid surfaces will result in the rapid spreading of a vapor-suppressing foam on the fuel surface. The foam extinguishes and secures the flame by forming a barrier between the liquid fuel and oxygen. This barrier excludes oxygen from the fuel source and eliminates the release of flammable vapors from the fuel surface. The cooling effect of this solution also lowers the temperature of the flammable fuel, further decreasing fuel vapor release.\(^{54}\)

Wet chemical systems are applied in a manner similar to that used for dry chemical systems. The wet chemical can be activated automatically or manually to discharge through fixed nozzles and pipes by way of expellant gas.

In high-rise buildings, wet chemical systems are used mainly for restaurant hoods, plenums, ducts, and associated cooking appliances in kitchens and cafeterias. NFPA 17A outlines preengineered wet chemical systems that are used for restaurant, commercial, and industrial hoods, plenums, ducts, and associated cooking appliances. Like dry chemical systems, these systems are activated automatically by a fusible link or heat detector located in some cases above each cooking appliance or group of appliances protected by a single nozzle or, in other cases, at or within the entrance to the ducting system. The systems are also designed so that when activated, the fuel or power to all equipment protected by the system will automatically shut down.\(^{55}\)

---

\(^{52}\)ibid., Chapter 9.

\(^{53}\)ibid., 3.3.22 Definitions.

\(^{54}\)ibid., A.4.6.1 Definitions.

\(^{55}\)ibid., 4.4.3.1 Definitions.
As with dry chemicals, wet chemicals should be removed as quickly as possible from the surfaces to which they have been applied.

Air-Handling System Controls and Status Indicators

Modern high-rise buildings are equipped with HVAC or air-conditioning and ventilating (ACV) systems. These systems allow the air within a building to be regularly exchanged, distributed, and maintained at certain levels of temperature, humidity, and cleanliness. The air within the building is thus rendered comfortable for the occupants, and the air temperature of certain areas, such as those containing sensitive equipment, is sustained at predetermined safe levels.

“Air conditioning and ventilating systems, except for self-contained units, invariably involve the use of ducts for air distribution. The ducts, in turn, present the possibility of spreading fire, fire gases, and smoke throughout the building or area served.”

Purpose of HVAC Systems

NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems*, outlines the purpose of these systems and prescribes minimum requirements for safety to life and property from fire. According to NFPA 90A, these requirements are intended to accomplish the following:

1. Restrict the spread of smoke through air duct systems within a building or into a building from the outside
2. Restrict the spread of fire through air duct systems from the area of fire origin whether located within the building or outside
3. Maintain the fire-resistive integrity of building components and elements such as floors, partitions, roofs, walls, and floor- or roof-ceiling assemblies affected by the installation of air duct systems
4. Minimize the ignition sources and combustibility of the elements of the air duct systems
5. Permit the air duct systems in a building to be used for the additional purpose of emergency smoke control

It is not within the scope of this book to describe in detail the HVAC systems that may be found in modern high-rise buildings. To determine what specific equipment should be installed in a building, consult the laws, codes, and standards that have been specifically adopted by the authority that has jurisdiction, equipment manufacturer’s operation and service manuals, architectural specifications, the building engineer, a qualified HVAC professional, and possibly the local building or fire department.

In understanding these systems, it is helpful to know that HVAC equipment—heaters, fans, and filters—usually is located in service rooms separated from the remainder of the building by fire-resistive floors, walls, and floor-ceiling assemblies. These rooms generally

---


are locked to deter unauthorized entry and may be equipped with automatic sprinklers for fire protection. They also contain smoke detectors that, on activation, will send a signal to the fire command center, automatically shut down the HVAC system, and close fire and smoke dampers serving that area.

Smoke Control within Buildings

NFPA 101, *Life Safety Code*, and NFPA 90A acknowledge two approaches to smoke control, the passive and active approaches. “To achieve this objective, the HVAC system can be shut down and the fire area isolated or compartmented.” Another approach is to allow fans to continue to run, using the air duct system for emergency smoke control.”

In many high-rise buildings, when a fire alarm occurs, there is automatic pressurization of stairwells using fans that keep smoke out of the stairwells. However, each building’s smoke control systems will differ according to the laws, codes, and standards required at the time the system was installed.

Status indicators for the HVAC systems and stairwell pressurization fans, and the controls that enable them to be operated manually, are located in the fire command center.

Control of Chemical, Biological, and Radiological Contaminants within Buildings

In a high-rise, the impact of the release of airborne chemical, biological, and radiological agents is accentuated by the fact that a building’s HVAC systems could provide a means for the rapid spread of contaminants throughout a building. This fact has caused considerable debate among industry experts as to what actions should be taken with regard to these complex systems, whose operations often vary from building to building and system to system.

Protecting Exterior Air Intakes and Mail Rooms

Openings for outdoor air intakes and ducts for the heating, ventilation, and air conditioning (HVAC) systems and air handling units should be constructed or modified (Figure 5.17) for ways to enclose vulnerable outdoor air intakes (or, if possible, their location changed so that access from the street level is denied) so that it is extremely difficult, if not impossible, to introduce materials such as toxic chemical, biological, and radiological agents.

---

*A smoke damper is “a device to restrict the passage of smoke through a duct that operates automatically and is controlled by a smoke detector” (NFPA Glossary of Terms, National Fire Code. Quincy, MA: National Fire Protection Association; 2005). A fire damper is “a device within the air distribution system to control the movement of smoke” (NFPA 90A. Standard for the Installation of Air-Conditioning System(s) with Building Construction, 3.3 Definitions. Quincy, MA: National Fire Protection Association; 2009). There may also be a combination smoke and fire damper that meets the requirements of both.

**Compartmentation also involves the automatic closing of fire doors, such as stairwell and elevator vestibule doors, to protect occupant escape routes during the early stages of a fire.


***Also, additional security measures such as intrusion detection devices, CCTV, and security staff can be used to help detect unauthorized intrusions. For other protective measures such as high-efficiency filters, ultraviolet light, and biological-agent detection devices, a biochemical expert or qualified HVAC professional should be consulted.
If a building or a large tenant in a building has a separate mail room, consideration should be given to isolating its HVAC systems from the building's HVAC system. Isolating a mail room will involve sealing existing air vents and doors and installing a separate ventilation system. It may also require relocation of the mail room itself to another area of the building or moving it outside of the building.

The American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (ASHRAE), in an initial report, Risk Management Guidance for Health and Safety Under Extraordinary Incidents, stated, “Do not close outdoor air intake dampers or otherwise block ventilation paths; do not change the designed airflow patterns or quantities; and do not modify the fire protection and life safety systems without approval of the local fire marshal.” 59 Commenting in the Engineering News-Record, Nadine M. Post said,

Risk Management Guidance for Health and Safety Under Extraordinary Incidents also offers guidance on steps that can be taken to render buildings somewhat less vulnerable to bioterrorism and other attacks. But for the time being, unless the building is an obvious target, ASHRAE recommends operating buildings normally and, in every case, not making any changes without consulting a professional engineer or expert.

The report, written by a 10-person committee, is not a “definitive piece” and not based on a specific building or HVAC system, said James E. Woods, committee chair and president of HP Woods Research Institute, Herndon, VA. It does advise owners to get to know their buildings before making changes and to develop a preparedness plan in case of an incident. It is important to look at the building operation as a whole and to avoid measures that can backfire, caution the authors. For instance, closing off air intake vents can decrease a system’s ability to purge contaminants.

Sensors and other warning devices are not available or are not reliable for many contaminants so they cannot be used as a control strategy, says the report. For protection against aerosol attacks from outside, openings “must be capable of timely closure, located sufficiently remote from any launch site or the building must be equipped with adequate filtration.”


Reportedly, there are systems capable of reliably and rapidly detecting chemical or biological agents. For example, “The Building Sentry One™ is the first complete system designated by the Department of Homeland Security capable of quickly and reliably detecting toxins then taking immediate action to protect a building, its assets, and the innocent people inside. With detection in milliseconds, the Building Sentry One’s sensor array network, strategically placed in the supply and return air ducts, automatically directs the building management system to shut down the air distribution system in under 5 seconds and activate the appropriate Con-Ops plan protocols. Via the Remote Monitoring Center, the Building Sentry One™ simultaneously contacts first responders and relays real-time toxin and location data, enabling rescue teams to handle the problem effectively—protecting occupants and expediting a safe building recovery” (Building Protection Systems Inc. website, <www.bpsiglobal.com/products-solutions/buildingsentry1.htmlspecifications>; December 15, 2008).

Also, “Smiths Detection today announces the introduction of its next-generation SABRE CENTURION II, air monitoring system designed to detect and identify Chemical Warfare Agents (CWAs) and Toxic Industrial Chemicals (TICs) in critical infrastructures… Centurion II uses Smiths Detection’s proven Ion Mobility Spectrometry (IMS) technology and can be networked with up to 70 other detectors to provide a comprehensive threat detection system that is then programmed to control air handling systems to isolate and contain a potential threat.” Reuters, “Smiths Detection Introduces Advanced Air Monitoring System to Detect and Mitigate Chemical Threats,” Coltrin & Associates for Smiths Detection. September 15, 2008. <www.reuters.com/article/pressRelease/idUS145678+15-Sep-2008+BW200809152sp=true>, Thompson Reuters; December 15, 2008.
Areas of refuge are not economically viable in many buildings. Consequently HVAC systems can be used to pressurize building egress paths and to isolate significant contamination to “selected building volumes,” says the report. Finally, enhanced air filtration alone is not sufficient to reduce airborne contamination. It should be coupled with pressurization of the interior relative to outdoors.  

Additional Sources of Information

Sources for information for safeguarding buildings against chemical, biological, or radiological attacks are as follows:

- **Advice for Safeguarding Buildings Against Chemical or Biological Attack.** Lawrence Berkeley National Laboratory, http://securebuildings.lbl.gov. Website with advice for safeguarding buildings against chemical or biological attack.

Fire Life Safety System Reset Procedures

The status indicators, control panels, and procedures used to reset building fire and life safety systems will vary considerably from system to system, manufacturer to manufacturer, and even from model to model within the same manufacturer’s line.

Elevator Systems

Elevator Status Panel Displaying Elevator Operations

Elevator annunciator panels usually are located in the fire command center or at a designated location in the main building lobby. These panels visually display the location of passenger and freight/service elevators operating in the building. They indicate the

---

number of the elevator car (sometimes called a cab) and the number of the floor on which the elevator is located at any particular time. Some elevator systems visually display on a computer monitor screen the floor that each elevator car is on, whether it is parked or traveling up or down, whether the elevator car door is opened or closed, and whether the elevator is empty or contains passengers.

Devices operated by key or by computers controlling the elevators may also be provided so that elevator cars can be individually selected and their movement up and down manually controlled without anyone being at the elevators themselves.

Elevator Safety Developments

Over the years, safety developments for elevators have included the following:

- A self-leveling device that greatly reduces the tripping hazards for passengers as they step off elevators.
- Hoistways and the sides and backs of elevators are enclosed.
- A door interlock system prevents an elevator from operating unless the door at each floor is closed and locked.
- An electronic safety device, the photoelectric eye, detects the presence of a person standing in the elevator’s doorway, and causes the doors to return automatically to the fully open position.
- As mentioned earlier, six to eight hoisting ropes or steel cables are used to lower and raise the elevator. Any one of these cables is strong enough to support the weight of the car plus the maximum allowable weight of the passengers.
- Weight sensors that stop an elevator car from operating if it is overloaded.
- The governor, a safety device that prevents an elevator car from falling or from moving downward too fast. A steel rope or governor cable runs from the elevator car to the driving wheel of this device. If the elevator car exceeds its normal design speed for any reason, the driving wheel trips a safety switch that sets the brake on the elevator’s driving machine. Usually this braking action is enough to stop the car. If for some reason it doesn’t stop the car and its speed continues to increase, the governor causes safety clamps to be released against the elevator’s guide rails, which are firmly secured to the building structure. This brings the car to a smooth, sliding stop.
- Seismic devices, designed to shut down elevators when the building itself moves, are incorporated into elevator systems in areas subject to earthquakes. On sensing movement, the device automatically sends a signal to the elevator control system and causes each affected elevator car to go to the nearest floor in its current direction of travel, makes its doors open automatically, and then shuts down the elevator. The elevator can only be restarted after the seismic device has been reset. After the probability of aftershocks has passed, a qualified individual—an elevator mechanic, building inspector, or possibly the building engineer—should inspect elevator shafts and elevator cars to check for any possible damage or safety hazards before resetting the seismic device. Possible damage could include loosening of counterweight guide shoes and counterweight rails, jammed hoistway doors, failure of hoisting ropes or supports, and dislocated control equipment in elevator machine rooms.

Elevator Controls

Although, elevator systems vary from building to building and even from model to model within the same manufacturer’s line, there are basic similarities of elevator controls.
Controls Inside Elevator Cars

Inside the elevator car there is often an internal control panel that consists of two main parts: the passenger open control panel and the locked control or service panel.

1. Passenger Open Control Panel

The passenger open control panel or main car station consists of a floor selection panel that enables the passenger to select the desired floor by pressing the appropriately numbered button. The selected button then lights up, indicating that the selection has been registered. As required by code, Braille markings and raised numerals indicating the number of each floor are provided adjacent to the push buttons to assist people with a visual impairment. Some ultramodern elevators have incorporated high-fidelity synthesized voice systems for the sight impaired; these systems announce the floor, the direction of travel, and the next stop floor.

In elevator systems, manual floor selection can occur through completion of an electrical circuit either mechanically (like a door buzzer) or by heat being sensed from the passenger’s finger (the latter does not meet disability requirements). Other elevators use inductance of electricity (the application of the passenger’s finger or other object causes a change in an electrical circuit).

In addition to the floor selection buttons, the following buttons usually are available to passengers:

- **Open door.** Pushing and holding this button extends normal door-opening time or reopens a closing elevator door so that the car doors can be kept open longer than the normally programmed time (e.g., to facilitate passenger loading).
- **Close door.** Pushing this button closes the elevator car door.
- **Emergency call, emergency alarm, or emergency only.** Pushing this button (often red) annunciates an audible and visual alarm in the fire command center, security console, or similarly supervised location within the building, or to an outside monitoring agency (such as the elevator company itself) to indicate that there is a possible emergency situation in the elevator concerned. The alarm will sound both within the car and outside the hoistway in the vicinity of the involved elevator.
- **Emergency push to stop/pull to run.** Pushing this button (usually red) stops the elevator car and annunciates an alarm similar to the one described earlier. Returning the button to its normal position restores normal operation. In some jurisdictions this device is located in the locked control or service panel where it is not accessible to passengers. This prevents nuisance use and the associated unnecessary sudden stops.

There usually is a two-way emergency communication device such as a telephone housed in a compartment (that automatically connects to an elevator maintenance company or other answering service inside or outside the building) or an intercom (that is connected to the fire command center or similarly supervised location within the building). If the call is directed offsite, the caller will need to communicate the name of the building and the number of the elevator car in which he or she is located. Some cities require new or modified elevators to provide a form of communication that is not totally based on voice in case the caller is hearing or speech impaired.

2. Locked Control or Service Panel

The locked control or service panel consists of key-operated controls or controls located in a locked cabinet. It usually is provided for the use of elevator maintenance, building
A power or motor generator switch that is normally left in the ON position when the elevator car is in constant use. When moved to the OFF position, the elevator cannot be operated.

An independent service device (or “manual operation” or “service switch”) that permits the use of floor selector buttons to take the car directly to any floor, irrespective of any calls that have been registered inside or outside the elevator car. On independent service, if the car doors are open, the CLOSE DOOR button must be pushed continuously until the car starts to move. On arrival at the selected floor, the doors open automatically and remain open until another floor selector button is pushed (this mode of operation may vary from system to system). If the operator wants to shut down the elevator while it is on independent service, the switch usually labeled POWER or MOTOR GENERATOR will need to be turned to the OFF or STOP position. Locking of the control panel door prevents any further use of the car without the appropriate key.

An emergency door open switch that, irrespective of where the car is positioned in relation to the floor level, can be used to open the inner car door. This device may be useful if the car will not open normally because it is stalled above or below the floor level.

An ON and OFF switch to control lighting inside the car. It must be in the ON position whenever the car is in use.

An ON and OFF switch to control the car ventilation fan. It too should be in the ON position when the car is in use.

An ON and OFF switch to control the electronic sensing devices (photoelectric or possibly infrared) that control automatic door opening when the elevator doorway is obstructed by a passenger or an object. This device causes the elevator doors to remain open or to reopen if they have started to close.

Depending on the elevator system, some of the preceding devices, and additional controls, may be openly displayed on the control panel. These are usually key operated to manage their usage. Also, the operating and inspection license is posted inside each elevator car.

Controls in Elevator Lobbies
In elevator lobbies there are two controls for the operation of elevators.

Passenger Controls
Elevator call stations are usually located on the elevator bank walls and are pushed to summon a car to the floor. (The operating mechanism is similar to that described for operating floor selection buttons inside the elevator car.) The elevator call station lights up to indicate that the hall call has been registered by the elevator system. (Repeated pushing of the station has no effect on calling the elevator.) Some multiple-elevator installations have hall position indicators that visually inform waiting passengers of the location and direction of travel of elevators in the hoistways.

Some elevator systems are equipped with destination dispatch or control technology. In high-traffic buildings, this technology can direct waiting passengers to elevators
that will provide the shortest travel times to their respective destinations. It achieves this by grouping together people by destination floors and minimizing the number of immediate floors at which the elevator stops.

In the elevator lobby, the waiting passenger uses a touch screen or a keypad located on elevator bank walls or lobby kiosks (Figure 6–21) to select their required destination floor (some systems also require the person to present a valid access card to a reader incorporated into the system) or uses an access card to pass through an optical turnstile that controls access to the elevator banks. The elevator control system evaluates the data, dispatches an appropriate elevator car to the floor where the passenger is waiting, and directs the person to the appropriate car.

According to the article “Smart Lifts Eliminate Floors Getting Up and Down,”

Prices [for destination dispatch systems] can also depend on features such as customised keypads, functions that let executives ride alone by assigning only them to a given car, and turnstile readers that know what floor passengers typically want as soon as they swipe their company ID cards.

---

Most destination systems have handicap [disability] functions that use voice and light signals for audibly or visually impaired passengers, assign fewer people to a car to allow room for a wheelchair, and delay door-closing time to give disabled passengers more time to enter and exit.

A potential flaw in the system can be caused by several people trying to get to the same floor but only one of them putting in a request for the floor number. This can cause the system to assign more people to a car than can comfortably fit. Likewise, if one impatient passenger punches in the same floor number multiple times, the system could be fooled into thinking that several people had requested trips to the same floor and assign fewer people to the car.

But most destination systems have load-weighing technology that can tell if more or fewer people have boarded than anticipated. If that’s the case, the car will not respond to other requests or accommodate additional passengers.

Emergency Use of Elevators

Firefighter Controls

So that elevators are not available to building occupants during a fire, elevator systems in many high-rise buildings are designed so that when an elevator lobby smoke detector is activated, all elevators serving the floor on which the alarm is occurring will be automatically recalled nonstop to a designated level (generally the ground floor) or alternate level, the elevator doors will open to allow passengers to exit, and the elevators will shut down. If the floor where the elevator lobby alarm is occurring is the designated floor, then the elevators will be recalled to an alternate floor.

In order for firefighters to control fire-recalled elevators, a FIRE BYP OFF ON device (“Fireman’s Return Override,” “Fireman’s By-Pass,” “Fireman’s Service,” “Fire Service,” or “Firefighter’s Service”) is provided.

At the main floor of a single elevator or for each of a group of elevators, there is a three-position (ON, OFF, BY-PASS) key-operated switch. During normal elevator operations, the switch is in the OFF position. When the switch is in the ON position, all elevators controlled by this switch and that are on automatic service will return nonstop to the main floor, and the doors will open and remain open. Any elevator moving away from the main floor will reverse at the next available floor without opening its doors. An elevator equipped with automatic power-operated doors and standing at a floor other than the main floor, with doors open, will have its doors close without delay, and then proceed to the main floor.62

---

*This is known as Phase I operation. “Phase I is the automatic or manual return, or recall, of elevators to a designated level or alternate level. Phase I also ensures that an elevator is not available to the general public during a fire. If the fire is in the designated level elevator lobby, the elevator will be recalled to an alternate level.


Insertion of a special key in the three-position switch and turning it to BYP will bypass the fire life safety system and allow control of each group of elevators. “Another two-position—on, off—key-operated switch may be provided in the building’s central control station. In the on position, the switch instructs all controlled elevators to return nonstop to the recall floor. All registered calls will be canceled. An ascending elevator will stop and reverse direction, without opening its doors.”

It is important that the use of such elevator keys is strictly controlled.

Present and Future Use of Elevators
Whether firefighters should use elevators during fire situations is a debatable issue. As reported by Klaene and Sanders, “Some fire service professionals say that elevators should never be used under fire conditions or suspected fire conditions until their safety can be verified from the fire floor.” However, Donoghue stated that “It is standard operating procedure in high-rise structures for fire fighters to use elevators not only to carry equipment for fire-fighting or evacuation purposes, but also to deliver fire personnel to nonfire floors.” A critical concern is whether using elevators during fire emergencies is dangerous to life safety."

Presently, unless an elevator is rated for use in a fire situation (i.e., it is a fire service elevator), in line with the thinking of some fire service professionals (see previous comment by Klaene and Sanders), it is not considered safe for anyone, including firefighters, to use a fire unprotected elevator whose shaft penetrates the fire floor. (Some fire departments—for example, the Los Angeles Fire Department—do not permit its firefighters under fire conditions to use any elevator whose elevator shaft terminates within five floors of the fire floor. This does not mean that elevators cannot be used as part of firefighting operations. If a building has low-, mid-, and high-rise elevator banks and a fire incident is occurring in the high-rise zone, it may be possible to safely use an unprotected elevator in the low-rise zone or possibly in the mid-rise zone, if the shaft in which it is housed does not terminate within five floors of the fire floor.)

In 2004, the Council on Tall Buildings and Urban Habitat (CTBUH) published an Emergency Evacuation Elevator Systems Guideline, prepared by a task force comprising “some of the world’s leading architects, engineers, building owner representatives, elevator consultants, life safety consultants, fire engineers, and elevator companies involved in

---

* “The provision that allows fire-fighting personnel to operate the elevator from within the car, or emergency in-car operation, is commonly referred to as Phase II [operation]” (Donoghue EA. Building transportation systems. In: Fire Protection Handbook. 20th ed. Quincy, MA: National Fire Protection Association; 2008:10–64).


** This discussion is primarily focused on the United States and does not necessarily apply to other countries where dedicated elevators are already used for fire service access. “Dedicated elevators have been used for fire service access in the United Kingdom and other locations for decades and there is general interest in employing such elevators [in the United States] for certain classifications of high-rise buildings” (Meacham BJ, Carl G. Protecting against extreme events. In: Fire Protection Handbook. 20th ed. Quincy, MA; National Fire Protection Association; 2008:1–32).

*** And building engineering and security staff, who are not trained as first responders, do not wear fire protective clothing, do not having breathing apparatus, and are not equipped with portable fire fighting equipment.
the design of structures.” As stated in its introduction, “This guideline will identify key issues that design teams should consider in the development of emergency evacuation systems. It is intended to serve as a tool for design teams who are considering the use of elevators as part of the egress system serving their designed structure... The goal of this publication is not to provide technical solutions but rather to bring forth issues for debate and to generate awareness of emergency evacuation needs related to tall buildings.”

“In March 2004, ASME [American Society of Mechanical Engineers] (the developer of ASME A171, Safety Code for Elevators and Escalators) sponsored a symposium, cosponsored by NFPA, on the use of elevators in fire emergencies for egress and for fire service use. Recommendations from the symposium were distributed to a host of code-making bodies, including NFPA, to promote concurrent development of provisions to support elevator usage.... Preliminary work by the task groups [two ASME task groups were formed—“one on the use of elevators by building occupants during emergencies and one on the use of elevators by emergency responders during emergencies”] indicates that it should be feasible to develop code criteria to permit occupants to use elevators safely after activation of the building fire alarm system and up until the time that a smoke detector in an elevator lobby or associated elevator machine room recalls the elevator. At that time, the elevator will remain locked-out from use until emergency responders place the elevator back into service. Emergency responders (typically fire service personnel) can then use some of the building elevators to ferry occupants to safe discharge levels, while other elevators are used to carry fire fighters and their equipment to floors in the vicinity of the fire floor.”

Depending on the outcome of the ASME debate, there may be a major shift in the way building occupants and emergency responders use elevators during high-rise emergencies, particularly during fires and fire alarms. If new guidelines are developed, it will impact the way in which building occupants evacuate buildings, fire fighters use elevators to travel to fire situations, and building engineering and security personnel use elevators. Of course, any such shift will require a massive reeducation effort.

At the time of this writing, the ASME has released no specific guidelines (however, as discussed in Chapter 3, “Status of Recommendations,” U.S. code agencies, such as the International Code Council [ICC] and NFPA International, are already making changes relating to elevators in their 2009 codes). “ASME expects to have recommendations for its own code changes sometime in 2009.”

State-of-the-Art Computerized Controls

Some elevators have fully integrated state-of-the-art microcomputer-based systems that analyze calls, set priorities, dispatch cars on demand, and enable one to control every aspect of the elevator. For example, a simple stroke on the computer keyboard can program a particular elevator not to stop on a particular floor during certain time periods. Such controlled access is important from a security standpoint.

67 ibid., pp. 7, 8.
69 Comment by David McColl, chairman of the ASME 17 task group, on the use of occupant egress elevators, in “Opening the door to elevator evacuation” by Brandon L. Building Operating Management. Milwaukee, WI; November 2008:22.
Emergency and Standby Power
During electrical power failures, for life safety reasons, emergency and standby power systems (discussed next) allow certain elevators to be operated. The emergency power control panel for elevator operation may be located at a separate locked control panel or within the fire command center. Emergency power systems may vary, but basically they are designed to provide power to emergency lighting within the elevator car, permit the operation of each elevator to allow passengers to exit the car, establish reduced service during the time of an emergency, and return the elevator system to normal service when electrical power has been restored. Standby power must be available to at least one elevator serving all floors, and this power can be transferred to any one elevator.

Emergency and Standby Power Systems Status Indicators
In the event of an electrical power outage, modern high-rise buildings are equipped with private, permanently installed power supply systems to mitigate such a threat to building operations. Indicators of these systems' operating status are found in the fire command center. NFPA 70, National Electrical Code (2002, Articles 700, 701, and 702), outlines two such power systems: emergency and standby. (The requirements for these systems for individual buildings may vary depending on the laws, codes, and standards that have been adopted by the authority that has jurisdiction.)

Emergency Power Systems
Emergency power systems are required to supply power and illumination automatically to areas that are essential for the life safety of building occupants. Typically these include public address systems, means of egress lighting and other lighting specified as necessary, fire detection and alarm systems, fire pumps, elevators, and other facilities that could pose a threat to life safety when electrical power is interrupted.

Usually, emergency power systems are designed to provide an automatic transfer to emergency power within 10 seconds after failure of normal electrical service to the building. This transfer can be powered by devices such as a storage battery or group of batteries, a generator driven by a fuel-supplied prime mover (Figure 6–22), a UPS, or any other means authorized by the authority that has jurisdiction. Lead-acid or nickel-cadmium batteries are dependable but must be located in well-ventilated areas because gases they release may be a fire hazard. They must also be recharged after each use. (Batteries may also be used to power self-contained lighting assemblies on failure of electrical power.) For generators driven by a prime mover, if the prime mover is an internal combustion engine, an onsite fuel supply, usually with a fuel supply sufficient for not less than two hours of full-demand operation of the system, will need to be provided. A UPS is an invaluable system for rooms containing sensitive computer equipment because it automatically “on loss of normal power, continues to supply power without waveform distortion, and the load is totally unaware of normal power loss.”

Standby Power Systems

Standby power systems are subdivided into two categories: legally required and optional standby systems.

Legally Required Standby Systems

Legally required standby systems are those mandated by the authority that has jurisdiction to automatically supply power to systems other than emergency power systems, the loss of which could create hazards or have an adverse effect on fire fighting and rescue operations. Typically these include communication systems, ventilation and smoke removal systems, heating and refrigerating systems, and lighting systems.

Legally required standby systems usually are designed to provide an automatic transfer to standby power within 60 seconds of failure of normal electrical service to the building. This transfer can be powered by devices such as a storage battery or group of batteries, a generator driven by a fuel-supplied prime mover, a UPS, or any other means authorized by the authority that has jurisdiction.

Optional Standby Systems

Optional standby systems are designed to protect property when life safety is not involved. These systems may supply power, either automatically or manually, to data processing and communication systems, to heating and refrigerating systems, or to any other areas where a loss of power could cause discomfort to people or serious disruption or damage to the systems involved.

Use of the Terms “Emergency Power System” and “Standby Power System”

The previous differentiation of emergency power systems and standby power systems was based on NFPA 70, National Electrical Code (2002). If, however, one considers NFPA 110,
Standard for Emergency and Standby Power Systems (1999), the meaning of these terms may overlap and lead to confusion. The reason for this is that NFPA 110 places all such systems into categories defined in terms of type, class, and level. “Type defines the maximum allowable time [in seconds] that the load is without acceptable electrical power. [For example, Type U refers to UPS systems, Type 10 refers to a maximum allowable time of 10 seconds, and Type 60 refers to a maximum allowable time of 60 seconds.] Class defines the minimum allowable time [in hours] that the alternate source has the capability of providing its rated load without being refueled. Level defines the equipment performance stringency requirements.” For instance, in the case where 60 seconds is the maximum allowable time for the load to be without acceptable electrical power, according to NFPA 70, the correct term is standby power system, whereas according to NFPA 110, the correct term is emergency power system. These terms are different but, in fact, refer to the same thing.

Controls for Simultaneously Unlocking Stairwell Doors Locked from Stairwell Side

In modern high-rise buildings, locking systems that automatically unlock during a fire emergency often are provided for stairwells in the building tower. During normal building operations, these locking systems, primarily for security reasons, permit doors to be locked from the stairwell side. However, during a fire emergency, these doors either automatically unlock on activation of the building fire alarm system (i.e., fail safe)—and they remain unlocked until the fire protective signaling system has been manually reset, or else they are unlocked manually at the door or by pressing or turning a switch in the fire command center.

Table 6–1 outlines the sequence of operation of fire life safety systems in a typical modern high-rise building. This illustrates how fire life safety systems may be designed to operate. The actual mode of operation will vary according to the building and the requirements of the laws, codes, and standards that have been adopted by the authority that has jurisdiction.

Other Building Systems and Equipment

The fire command center may also contain other building systems and equipment as sanctioned by the authority that has jurisdiction. There may be automatic dialing equipment to send signals from the building’s fire life safety system to an offsite monitoring location, and there may be keys for the fire department to access elevators and all locked areas of the building. The provision of building and elevator keys at the fire command center is not to be confused with rapid entry systems described in Chapter 5. (Rapid entry systems—or rapid entry key vaults or fire department lock boxes, as they are commonly called—are designed for emergency access from the exterior of a locked building.)

Building Emergency Procedures Manual

Many jurisdictions require that the fire command center contain the Building Emergency Procedures Manual so that it is readily available for immediate reference by building emergency staff, fire departments, and other emergency response personnel. Chapter 9,
Appendix 9–2 (which is on the CD-ROM provided with this book), details the content of a Building Emergency Procedures Manual. Also, the authority that has jurisdiction may require certain equipment operating licenses and permits to be displayed in the fire command center.

Before completing this description of fire life safety systems and equipment, with its particular reference to the fire command center, it is appropriate to describe three other valuable types of equipment and material for the fire life safety of building occupants and property: portable fire extinguishers; photoluminescent signs, strips, and exit path lighting; and automated external defibrillators.

**Portable Fire Extinguishers**

There are a number of portable fire extinguishers used in high-rise buildings. They can be a first line of defense in handling fires of limited size. The selection of the most appropriate fire extinguisher depends on the specific hazard it is designed to address, the effectiveness of the fire extinguisher on that type of hazard, and the ease with which the extinguisher can be used. A portable fire extinguisher is “a portable device, carried or on wheels and operated by hand, containing an extinguisher agent that can be expelled under pressure for the purpose of suppressing or extinguishing fire.”  

**Classes of Fire and Recommended Extinguishing Agents**

NFPA 10, *Standard for Portable Fire Extinguishers* (2007), classifies fires, depending on fuel type, as Class A, Class B, Class C, Class D, or Class K. Class D fires involve combustible metals such as magnesium, titanium, zirconium, sodium, lithium, and potassium. Because the occurrence of Class D fires is unusual if not nonexistent in commercial high-rise buildings, neither they nor the dry powder that can be used to extinguish these types of fires will be discussed.

The ensuing review of classes of fire and recommended extinguishing agents, followed by the description of portable fire extinguishers, has been compiled using NFPA 10 and the *Fire Protection Handbook* article “Fire Extinguisher Use and Maintenance.”

Classes of fire in high-rise buildings and their recommended extinguishing agents are as follows:

1. **Class A**—fires in ordinary combustible materials, such as wood, cloth, paper, rubber, and many plastics.
   Class-A-rated extinguishers are frequently used for ordinary building protection. The agents used are water-based, loaded stream, aqueous film-forming foam (AFFF), film-forming fluoroprotein foam (FFFP), multipurpose (ammonium-phosphate-base), dry chemical, and halogenated types.

2. **Class B**—fires in flammable liquids, combustible liquids, petroleum greases, tars, oils, oil-based paints, lacquers, alcohol, and flammable gases.
   Carbon dioxide, dry chemical, AFFF, FFFP, and halogenated extinguishers are recommended for Class B fires. Water should not be used on Class B fires except in the very rare case where the burning substance is known to be capable of being mixed with water. The water may then be applied in a spray form.

---

3. **Class C**—fires that involve energized electrical equipment and that therefore require the extinguishing media to be nonconductive. Carbon dioxide, dry chemical, and halogenated extinguishers are recommended for Class C fires. When the electrical equipment is de-energized, extinguishers for Class A or Class B fires may be safely used.

4. **Class K**—fires that involve cooking appliances and combustible cooking media such as vegetable or animal oils and fats. Wet chemical-based and dry chemical-based extinguishers can be used for Class K fires.

Figure 6–23 shows the marking recommended by the NFPA to indicate the fire extinguishers suitable for use on each type of fire. These pictographs are designed so...
that the extinguisher’s proper use may be determined at a glance. When an application 
is prohibited, the background is black and the slash is bright red. Otherwise, the back-
ground is light blue.  

Most high-rise buildings have Class A fire hazards in public access or common 
areas and within tenant, guest room, or apartment areas; Class B and Class K fire haz-
ards in special areas such as kitchens; and Class C fire hazards in maintenance spaces 
such as electrical switch gear, generator, or elevator machine rooms, and computer 
rooms and data centers. Fire extinguishers in these locations should correspond to the 
hazards of that area, have sufficient extinguishing capacity, and be immediately avail-
able in adequate numbers for persons trained in their operation.

The following types of portable fire extinguishers may be found in buildings.

Water-Based Extinguishers
Water-based extinguishers use water or water solutions that have a cooling, heat-absorbing 
effect on fires, particularly those of Class A. (The water solutions include antifreeze and 
wetting agents.) Older, inverting types of water extinguishers, such as soda acid and car-
tridge-operated water, are no longer manufactured.

Water extinguishers that contain water, stored under pressure, are still in use today 
for Class A fires (Figure 6–24a). They can be used even in areas where temperatures may 
go below freezing, as long as they are charged appropriately or if an antifreeze solution is 
added to the water. Wetting agents allow water discharged from the extinguisher to spread 
and penetrate more effectively by facilitating a reduction in the surface tension of the water.

![Figure 6-24](safetymessage.com)

<table>
<thead>
<tr>
<th>(a)</th>
<th>(b)</th>
</tr>
</thead>
</table>

---

74 NFPA 10. Standard for Portable Fire Extinguishers, 2007 Edition-Annex Figure B.1.1. Quincy, MA: 
How to Use

When using a water extinguisher, the first step is to place the extinguisher on the ground, hold the handle in one hand, and pull out the ring pin with the other hand. The ring pin normally keeps the operating lever locked and prevents the extinguisher from discharging accidentally. Then take hold of the hose and squeeze the operating lever (usually located directly above the handle) with the other hand. “The stream initially should be directed at the base of the flames. After extinguishment of flames, it should be directed generally at smoldering or glowing surfaces. Application should begin as close as possible to the fire. Deep-seated fires [i.e., smoldering fires such as those involving upholstered furniture] should be thoroughly soaked and might need to be 'broken apart' to effect complete extinguishment.”75 NFPA 10, *Standard for Portable Fire Extinguishers*76 states that a 2-1/2-gallon water extinguisher has a horizontal stream range of 30 to 40 feet (9.2 to 12.2 meters) and an approximate discharge time of one minute.

A person operating a water or water-based extinguisher may be injured, or the fire spread farther, if the extinguisher is discharged on an electrical or flammable liquid fire.

Carbon Dioxide Extinguishers

Carbon dioxide extinguishers stop fires by using carbon dioxide to reduce the amount of oxygen in the atmosphere to the point where combustion cannot be supported. For a description of the gas and its advantages and disadvantages in fire life safety, see the “Carbon Dioxide Systems” section in this chapter.

Carbon dioxide can be used to suppress fires involving gas, flammable liquids, electrical equipment, and, although less effectively, common combustible elements such as wood and paper. Figure 6–24b shows a portable carbon dioxide extinguisher.

How to Use

When using a carbon dioxide extinguisher, the first step is to place it in an upright position using its carrying handle, hold the carrying handle in one hand, and pull out the ring pin with the other hand. The ring pin normally keeps the operating lever locked and prevents the extinguisher from discharging accidentally. Then direct the extinguisher as described next, taking care not to hold the discharge horn (it may become very cold during discharge), and squeeze the operating lever (usually located directly above the carrying handle) with the other hand. When discharging the extinguisher on flammable liquid fires, the extinguisher should be aimed at the near edge of the flames and swept from side to side toward the back of the fire or aimed downward at a 45-degree angle toward the center of the area that is burning with the discharge horn kept stationary. The risk in discharging the extinguisher too close to oil and grease fires is that it may cause these substances to splash and thereby spread the fire.

For fires involving electrical equipment, the extinguisher should be aimed at the base of the fire. To prevent reignition, the equipment should be switched off promptly. NFPA 10, *Standard for Portable Fire Extinguishers*,77 states that a 2-1/2- to 5-pound
hand portable carbon dioxide extinguisher has a horizontal stream range of 3 to 8 feet (0.9 to 2.4 meters) and an approximate discharge time of 8 to 30 seconds.

**Halon and Halon Replacement Extinguishers**

To extinguish fires involving expensive electrical office equipment such as computers, generally halon was used in the past. However, due to environmental concerns, halon has been severely restricted to essential purposes and its production has ceased. Halon replacement extinguishers are now available.

The technique for using these types of extinguishers is similar to that employed for carbon dioxide extinguishers.

**Dry Chemical Extinguishers**

For a description of dry chemical agents and an estimate of their function as fire extinguishers, see the “Dry Chemical Systems” section presented earlier in this chapter.

Ordinary dry chemical extinguishers (sodium bicarbonate, potassium bicarbonate, urea-potassium bicarbonate, or potassium chloride base) are primarily for use on Class B and Class C fires.

Multipurpose (ABC) dry chemical extinguishers (multipurpose ammonium phosphate base) are used primarily on Class A, Class B, and Class C fires.

**How to Use**

A dry chemical agent can be discharged from an extinguisher in two ways, depending on the basic extinguisher design. The cartridge-operated extinguisher uses an external pressurized gas cartridge to discharge the dry chemical, whereas the rechargeable stored pressure extinguisher pressurizes the dry chemical chamber to discharge the dry chemical itself.

The operation of dry chemical extinguishers varies not only with extinguisher type but also with fire type. Ordinary dry chemical extinguishers, when used on flammable liquid fires, should be aimed at the near edge of the flames and swept from side to side toward the back of the fire. The initial discharge from the extinguisher will generate a sizable force; thus it should not be used at a range closer than 5 to 8 feet (1.5 to 2.4 meters) for flammable liquid fires because it may cause the liquid to splash and thereby spread the fire.

Multipurpose dry chemical extinguishers are used in the same manner as ordinary dry chemical extinguishers on Class B fires. However, on Class A fires it is important to attempt to coat all burning areas because the multipurpose agent tends to soften and adhere to burning materials and creates a coating that smothers and isolates the fuel from air.

NFPA 10, *Standard for Portable Fire Extinguishers*,\(^7^8\) states that a 1- to 2-1/2-pound dry chemical (sodium bicarbonate stored-pressure) extinguisher has a horizontal range of 5 to 8 feet (1.5 to 2.4 meters) and an approximate discharge time of 8 to 12 seconds. These ranges and discharge times vary according to the type of dry chemical being used.

Because dry chemical is electrically nonconductive, it is also useful against Class C fires. However, in telephone switching rooms, computer rooms, and data centers, where there are sensitive electrical contacts and relays, its use is not recommended. Application in these areas may cause the equipment to malfunction. After use, any dry chemical

\(^7^8\)ibid.
should be removed as quickly as possible from the surfaces to which it has been applied, as it may be corrosive.

Wet Chemical Extinguishers
For a description of wet chemical agents and an estimate of their function as fire extinguishers, see the “Wet Chemical Systems” section presented earlier in this chapter. Wet chemical extinguishers are primarily used in kitchens and restaurants to combat fires in cooking oils and fats.

Positioning of Portable Fire Extinguishers
The distribution of the portable fire extinguishers throughout a building is determined by a survey of the areas that need to be protected. After the selection of the appropriate number and type of extinguishers is made, they should be located conspicuously in positions that make them readily available in the event of a fire. Often this will require that they be located in areas where there are specific hazards and along the normal paths of egress from a space to an exit.

The NFPA states in its codes that 75 feet (22.9 meters) is the maximum travel distance a fire extinguisher can be from Class A hazards; the distance is 30 to 50 feet (9.15 m to 15.25 meters) for Class B hazards (unless the fire is in a flammable liquid of appreciable depth); for Class C hazards, the distance depends on whether the electrical equipment is a Class A or Class B hazard; and the maximum travel distance is 30 feet (9.15 meters) from a Class K hazard. 79

In high-rise buildings, portable fire extinguishers are located in areas such as public access or common areas such as freight/service elevator lobbies and outside entrances to stairwells; in kitchens, restaurants, cafeterias, photocopier rooms, computer rooms, data centers, and laundries; and in maintenance spaces such as electrical switch gear, generator, and elevator machine rooms.

The extinguishers are mounted on hangers or brackets, kept in locked or unlocked cabinets (provided the former can be easily accessed in an emergency), or placed on shelves. They should be mounted in such a way that the operating instructions are immediately visible and the extinguisher is readily accessible to the user (Figure 6–25).

Exit Signs
The authority that has jurisdiction will require exit signs to be posted in high-rise buildings so that a means of egress is clearly visible at all times. Means of egress is defined by NFPA 101, Life Safety Code, as, “a continuous and unobstructed way of travel from any point in a building or structure to a public way consisting of three separate and distinct parts: (a) the exit access, (b) the exit, and (c) the exit discharge.”

NFPA 101, Life Safety Code, Section 7.10, “Marking of Means of Egress,” states the following concerning signs designating exits or ways of travel:

Section 7.10.1.2. Exits, other than main exit doors that obviously and clearly are identifiable as exits, shall be marked by an approved sign readily visible from any direction of exit access.

Section 7.10.1.3. Tactile signage shall be located at each door into an exit stair enclosure, and such signage shall read as follows:

EXIT

Signage shall comply with CABO/ANSI A117.1, American National Standard for Accessible and Usable Buildings and Facilities, and shall be installed adjacent to the latch side of the door 60 in. (152 cm) above the finished floor to the centerline of the sign. Exception: This requirement shall not apply to existing buildings, provided that the occupancy classification does not change.

Section 7.10.1.4. Access to exits shall be marked by approved, readily visible signs in all cases where the exit or way to reach the exit is not readily apparent to all occupants. Sign placement shall be such that no point in an

* Tactile signage means that a blind and visually impaired person could comprehend the meaning of the sign. Commonly Braille is required on such a sign.
exit access corridor is in excess of 100 ft. (30 m) from the nearest externally illuminated sign and is not in excess of the marked rating for internally illuminated signs. Exception: Signs in exit access corridors in existing buildings shall not be required to meet the placement distance requirements.

The code goes on to address the size, color, design, mounting, and illumination of these signs, yet this is a suggested standard—it is up to the individual authority that has jurisdiction to specify what additional exit signage is required.

Disability requirements\textsuperscript{*} classify exit signs, except for the one at the exit door, in two ways. Directional signs read “EXIT” with an indicator showing the direction of travel (Figure 6–26). Informational signs are located on stairwell landings and usually indicate the stairwell number, identify what uppermost and lowermost floor the stairwell serves, and include a notation specifying whether or not the stairwell has roof access. They are likewise in every elevator lobby above and below the ground floor and in other conspicuous floor locations as required by the authority that has jurisdiction such as inside all public entrances of the building and on the inside of hotel guest room doors. Those in elevator lobbies usually include the following information:

- A building floor plan that shows the building core and perimeter, stairwells, fire escapes, elevators and every wall that faces every exit route.

\textsuperscript{*}In this case, the United States, the Americans with Disabilities Act (ADA).
A “YOU ARE HERE” direction arrow.
Exit routes to the appropriate stairwells.
Symbols depicting locations of fire equipment and manual fire alarm stations.
Information such as the building name and address, floor number, fire department and building emergency telephone numbers, what stairwells have roof access, and what the building fire alarm looks and sounds like.
If incorporating language similar to “IN CASE OF FIRE USE STAIRWAY FOR EXIT. DO NOT USE ELEVATOR,” the sign should be installed adjacent to the elevator call station (Figure 6–27 presents variations of the simple “IN CASE OF FIRE DO NOT USE ELEVATORS. USE STAIRWAYS FOR EXIT” sign; Figure 6–28 shows a sample floor evacuation plan sign).

Signs inside stairwells may also include details regarding the reentry of occupants from the stairwell onto the floor during a fire.

Photoluminescent Lighting, Signs, Markers, and Exit Path Lighting Systems
Photoluminescent lighting, signs, and markers indicating egress paths can be an invaluable means to assist evacuating occupants to navigate in total darkness or through smoke-filled areas. Inside building stairwells, photoluminescent exit signs and photoluminescent strips applied to stair treads, handrails, door handles, and perimeters of doorways can be used (Figure 6–29). Also, some photoluminescent strips come preinstalled in the cover base (skirting board) that is attached to the wall at a low level along egress paths other than inside building stairwells.

In addition, some building stairwells have floor proximity exit path lighting affixed to the stairwell wall just above the level of the stair treads. When power fails, the building emergency generator electrically powers this exit path lighting.

---

*Stair treads are “the upper horizontal boards of a flight of steps; the portion actually stepped upon” (Construction Dictionary, 9th ed. Greater Phoenix, Arizona, Chapter 98. Phoenix, AZ: The National Association of Women in Construction; 1996:506).
The intensity of the fluorescent light, the minimum distance at which a person can view the sign or marker, and the duration period for which the fluorescent light must remain visible after all other light has been removed are critical issues regarding the effectiveness of this life safety measure. In some jurisdictions, photoluminescent egress path markings are mandated by law.

For example, in New York City they are required for commercial buildings. Local Law 26 of 2004, New York City Building Code 27-383(b) states, “This standard is intended to provide minimum requirements for photoluminescent exit path markings that will aid in evacuation from buildings in the event of failure of both the power and back-up power to the lighting and illuminated exit signs. Photoluminescent material is charged by exposure to light and will emit luminance after the activating light source is unavailable. The markings covered by this standard are not designed to provide enough light to illuminate a dark egress path, but rather will provide luminescent signs and outlines of the egress path, stairs, handrails, and obstacles, so that occupants can discern these egress path elements in dark conditions. The markings are generally required to be located at a low location in case of smoke and to be readily seen, such as in a crowd situation.”
Emergency Call and Assistance Stations

Emergency call and assistance stations (Figure 6–30) are provided in areas, such as parking garages and parking lots, including in isolated areas such as stairwells, where people may need immediate two-way communication due to a security problem or a medical condition (even the proliferation of mobile phones will probably not do away with the need for these systems, particularly in areas such as parking garages where cellular phone coverage can be poor).

Many facilities include phrases such as “EMERGENCY,” “SECURITY ASSISTANCE,” “EMERGENCY INTERCOM,” or “EMERGENCY CALL STATION” printed in...
bold letters on signs at each location where these systems are installed. They are usually housed in a vandal-resistant, weather-protected enclosure as a stand-alone pedestal or are surface mounted on walls and poles. They may have a continuous light to draw attention or, upon activation, sound an audible alarm and flash stroboscopic lights. These devices utilize different communications technologies to connect to a monitoring station and are designed to operate during power failures (with battery backup, whereas others are solar-powered). Also, some are equipped with a camera so that on activation of an intercom station the image will be automatically called up for the operator who is monitoring the system.

Personal Alarm, Personal Protection, Medical Alert Systems

Personal Alarm Systems
Personal alarm devices may be issued to tenants, residents, or regular users of a facility to call for emergency assistance. According to Moser,

> These devices can replace security escort services, which are highly effective, but they also can place a strain on limited security staff resources.

*However, “if your emergency phone is on VoIP and your server goes down, your emergency phone goes along with it” (“Focus: Emergency phone towers,” comment by Sam Shanes, Talk-a-Phone Co. Security Technology & Design. Cumming, GA; January 2007:44).
Before purchasing such a system, it is important to verify that if a button is pushed, the incoming signal [to the monitoring location] will identify which unit has been activated and the location of the alarm signal. It is also advisable to purchase a system that can be tied into the existing emergency phones. If the button is pushed, the strobe and alarm of the nearest phone unit turns on and opens up two-way communication. Pushing the button also activates the CCTV to provide remote assessment \(^8^0\) [if a camera is located in the area where the incident is occurring].

**Personal Protection Devices**

Personal protection devices can be carried in a person’s pocket, briefcase, handbag, or purse to help protect the individual from or warn off a would-be assailant (if permitted by law). Such nonlethal equipment ranges from mace and pepper sprays to battery-operated devices that emit high-pitched sounds.

**Medical Alert Systems**

Medical alert systems are similar to panic alarms (described in Chapter 5) but are intended for people to signal for emergency medical assistance. These activator devices may be installed inside buildings in places such as health clubs, saunas, apartments and residences, and hotel rooms, particularly in bathrooms and toilets; or they may be worn around the neck or on the wrist or clipped on a belt. They can be used to activate a two-way conversation with those monitoring the system.

**Automated External Defibrillators**

Automated (or sometimes, automatic) external defibrillators, or AEDs (Figure 6–31), are devices to allow nonmedical personnel, such as security staff, to administer potentially life-saving shocks to a person in cardiac arrest. “Sudden cardiac arrest is usually caused by an electrical malfunction of the heart called ventricular fibrillation (VF)—an ineffective quivering of the heart muscle that makes it unable to pump blood through the body. Once the blood stops circulating, a person quickly loses consciousness and the ability to breathe, and will die without effective treatment. The chance of survival drops about 10 percent each passing minute. Defibrillation is the definitive treatment for VF—but it is effective only if it reaches the victim in time. A brief but powerful electrical shock is applied to the person’s chest, interrupting the VF and allowing the heart’s natural rhythm to regain control.” \(^8^1\)

Generally AEDs are in the possession of trained first responders (including emergency services units) or are public-accessible units located in places that include office buildings, hotels and casinos, residential and apartment buildings, restaurants, fitness centers, and health clubs.

Due to the numbers of people using high-rise buildings, a cardiac arrest may occur at any time. Placement of AEDs at strategic locations within a building offers a potential solution for administering immediate attention to a victim before the emergency medical responders arrive. This is particularly important in skyscrapers where a victim could be stricken on an upper floor, a considerable travel distance away for responders entering


\(^8^1\) Cardiac response works for high-rises. Security. Highlands Ranch, CO; May 1998:47.
the building at the ground level. Because they are small, portable devices, AEDs can be quickly and easily carried to the emergency scene.

**Placement of AEDs**

BOMA International recommends the following:

- Place AEDs in central locations near a telephone where they can be easily accessed;
- Place AEDs so any victim can be reached in less than three minutes;
- Place AEDs close to the person(s) trained to respond to an emergency; and
- Notify everyone of [the] AED location.  

“Despite the simplicity of the AED, it is not enough to purchase and install units in a facility. Units must be properly placed where they will do the most good. Personnel must be trained in their use. Units must be maintained. And because AEDs are still a prescription device, the entire program must be supervised by a physician.”

---


Potential liability exposure can be reduced by public laws that protect the person administering the AED treatment, as long as gross negligence or intentional misuse is not involved.

Fire Life Safety Systems and Equipment Selection

To assist in determining what specific systems and equipment are installed and operating at a building, one should consult the building engineer (particularly the chief engineer) or the operations manager of the site concerned, equipment manufacturer’s operation and service manuals, architectural specifications, and the local building, fire department, or other authority that has jurisdiction. Further expertise may require the services of a fire life safety consultant, such as a registered fire protection engineer. When changes are contemplated for any life safety systems, it is critical that only properly qualified and licensed personnel are consulted for professional advice.

Fire Life Safety Systems and Equipment Maintenance

To maintain a building’s fire life safety systems and equipment in an operable condition, the authority that has jurisdiction will require periodic inspection, testing, and maintenance according to specified guidelines and for these activities to be thoroughly documented.

Buildings commonly employ a licensed contractor and support team specializing in life safety system operations to perform some testing and maintenance work. Typically in large high-rise buildings, building engineers do not have the time to perform these labor-intensive duties and sometimes they do not possess all the skills necessary to work on the diverse equipment involved.

Summary

- Many types of fire life safety systems and equipment are found in high-rise buildings.
- To maintain good working order, the systems and equipment must undergo periodic testing, inspection, and maintenance.

Key Terms

**Addressable device.** “A fire alarm system component with discrete identification that can have its status individually identified or that is used to individually control other functions.” 84

**Automatic sprinkler.** “A device for automatically distributing water on a fire in sufficient quantity either to extinguish it entirely or to prevent its spread in the event that the initial fire is out of range, or is a type of fire that cannot be extinguished by water.” 85

---

Cross-over floor. A floor where occupants can cross over from an express elevator to another group of elevators. Also known as a sky-lobby.

Destination dispatch. Elevator (lift) technology to direct waiting passengers to elevators that will provide the shortest travel times to their respective destinations. It achieves this by grouping together people by destination floors and minimizing the number of immediate floors at which the elevator stops.

Dry chemical system. “A means of applying dry chemical that can be automatically or manually activated to discharge through a distribution system onto or into the protected hazard. The system includes auxiliary equipment.”

Fire command center. Focal point for a building’s fire life safety operations and communications. Also known as the fire control room, the central control station, the command center, the control center, the fire control center, or the building command station.

Fire damper. “A device within the air distribution system to control the movement of smoke.”

Fire hydrant. “A valved connection on a water supply system having one or more outlets and that is used to supply hose and fire department pumpers with water.”

Fire pump. A mechanical device for improving the water supply pressure from public water systems and storage tanks. Sometimes are called booster pumps. (“Some [fire pumps] are called booster pumps because they ‘boost’ the pressure of the public supply.”)

Fire service elevator. A hardened fire protected (fire rated) elevator dedicated for fire service use.

Gas detectors. Automatic detection devices that monitor low-level concentrations of combustible gases such as methane, ethane, natural gas, and propane.

Governor. A safety device that prevents an elevator car from falling or from moving downward too fast.

Gurney. “A metal stretcher with wheeled legs, used for transporting patients.”

Heat detectors. “Respond primarily to the convected thermal energy of a fire. They operate either when the detecting element reaches a predetermined fixed temperature or when a specified rate of temperature change occurs.” Also, known as a thermal sensor.

Ionization smoke detection. “The principle of using a small amount of radioactive material to ionize the air between two differentially charged electrodes to sense the presence of smoke particles. Smoke particles entering the ionization volume decrease the conductance of the air by reducing ion mobility. The reduced conductance signal is processed and used to convey an alarm condition when it meets preset criteria.”

---


**Jockey pump.** A small pump that automatically maintains the operating pressure in the fire protection system.

**Manual fire alarm station.** "A manually operated device used to initiate an alarm signal." Also known as the manual fire alarm box, the manual pull station, or the manual pull alarm.

**Mobile phone.** "A long-range, portable electronic device used for mobile communication." Also, known as a cell phone.

**Municipal fire alarm box.** A means for a fire alarm to be manually sent directly to the local public fire service from a municipal fire alarm box (street box) housed in an enclosure in the street outside of a building.

**Nonsprinklered.** The absence of a sprinkler system. Also known as unsprinklered.

**Nuisance alarm.** "Any alarm caused by mechanical failure, malfunction, improper installation, or lack of proper maintenance, or any alarm activated by a cause that cannot be determined."

**Phase I operation.** "The automatic or manual return, or recall, of elevators to a designated level or alternate level. Phase I also ensures that an elevator is not available to the general public during a fire. If the fire is in the designated level elevator lobby, the elevator will be recalled to an alternate level."

**Phase II operation.** "The provision that allows fire-fighting personnel to operate the elevator from within the car, or emergency in-car operation, is commonly referred to as Phase II [operation]."

**Photoelectric smoke detection.** Uses light to detect visible smoke particles produced by burning material. It is designed to detect smoke when smoke either obscures a light beam (thereby reducing the amount of light received by a photosensitive device) or the smoke scatters a light beam (thereby causing the light to fall on a photosensitive device that would not usually receive light when smoke was not present). The former is known as photoelectric light obscuration smoke detection and the latter as photoelectric light-scattering smoke detection. "The light signal is processed and used to convey an alarm condition when it meets preset criteria."

**Portable fire extinguisher.** A "portable device, carried or on wheels and operated by hand, containing an extinguisher agent that can be expelled under pressure for the purpose of suppressing or extinguishing fire."

**Public address system (PA).** A one-way communication system to the occupants of the building.

**Public telephone emergency telephone number.** A single, typically three-digit telephone number a caller can dial on the public telephone network to contact local emergency services for help. This telephone number differs from country to country (for example, 000 in Australia; 111 in New Zealand; 112 in European Union countries; 119 in parts of East Asia; 911 in the United States, Canada, and other countries; and 999 in the United Kingdom).

---

93 ibid.
97 ibid.
99 ibid.
100 ibid.
United Kingdom, Ireland, and Poland). Sometimes known as the emergency services number or the universal emergency telephone number.101

**Smoke damper.** “A device to restrict the passage of smoke through a duct that operates automatically and is controlled by a smoke detector.”102

**Smoke detector.** “A device that detects visible or invisible particles of combustion.”103

**Sprinkler system.** “A combination of underground and overhead piping that is connected to an automatic water supply. The piping is specially sized or hydraulically designed with that portion of the piping within the building generally located overhead. Sprinklers are attached to the overhead piping in a systematic pattern and a valve controlling each riser is located either directly on the system riser or in the supply piping. The system is usually activated by heat from a fire and discharges water over the fire area. A device actuating an alarm when the system operates is located on the system riser.”104

**Stair treads.** “The upper horizontal boards of a flight of steps; the portion actually stepped upon.”105

**Standpipe system.** “An arrangement of piping, valves, hose connections, and allied equipment installed in a building or structure.”106

**System riser.** “The aboveground horizontal or vertical pipe between the water supply and the mains (cross or feed) that contains a control valve (either directly or within its supply pipe) and a waterflow alarm device.”107

**Uninterruptible power supply (UPS).** “A system that provides continuous power to an alternating current (AC) line within prescribed plus or minus tolerances. A UPS protects against over-voltage conditions and brownouts. Also called *uninterruptible power source.*”108 “It differs from an auxiliary power supply or standby generator, which does not provide instant protection from a momentary power interruption. A UPS, however, can be used to provide uninterrupted power to equipment, typically for 5–15 minutes until a generator can be turned on or utility power is restored.”109

**Unsprinklered.** The absence of a sprinkler system. Also known as nonsprinklered.

### Additional Reading


---


103 ibid.


107 ibid.


Management of the Security Function

The security function encompasses the security-related tasks performed in a facility. Within a high-rise building, these responsibilities usually are performed by the security department acting on behalf of the facility owner or manager. The size and makeup of the security department will vary depending on the complexity of the facility and requirements of its security and fire life safety program.

The head of the security department may have one of various titles—director of security, security director, director of loss prevention, security manager, chief of security, head of security, security supervisor, or site supervisor; in a smaller building, this individual may be called a post commander. For the purposes of this chapter, this person will be called the director of security. Whether the security department is made up of contract or proprietary staff, the director of security has a key role in determining the quality and performance of the department. The director of security “must have security experience, leadership ability, be an excellent communicator both verbally and in writing, be organized and a strong time manager, enjoy and interface well with all kinds of people, be intelligent and able to understand and teach complex systems, be patient, upbeat, positive, outgoing, self-disciplined, caring, energetic.”

The remainder of the security department consists of supervisors and staff with job titles determined by the functions they perform, for example, lobby director, lobby ambassador, lobby officer, concierge, doorman, console operator, command center operator, patrol officer, rover, courier, dockmaster, watch commander, shift supervisor, security guard, and security officer.

The Security Budget and Key Performance Indicators

The cost of security in a high-rise building needs to be justified to the building owner and manager so that the security department remains adequately funded. A budget is “an estimate, often itemized, of expected income and expenses for a given period of

---

* Just as the term night watchman was replaced by security guard, security officer is now used interchangeably with security guard.
time in the future…. A plan of operations based on such an estimate.” According to Sennewald,

Planning and budgeting go hand-in-hand; a budget is a plan stated in financial terms. Budgeting requires a realistic estimate of programs and their costs, and an allocation of resources to achieve planned objectives. Because budgets are planned well in advance, effective budget management requires thinking ahead, anticipating needs based upon relatively predictable conditions. The budget then becomes a tool to ensure that plans are carried out.

Key Items
A security budget may include as line items the estimated cost of the following:

- The itemized capital cost of security systems, equipment, and fixtures (e.g., physical barriers, locks and locking systems, intrusion detection systems, duress alarm systems, lighting, communication systems, closed-circuit television (CCTV) systems, and other equipment used by security staff), including installation and maintenance costs. Security budgets may also include costs of fire life safety systems, equipment, and fixtures, if these costs are not part of a separate safety budget.
- Insurance charges for systems and equipment (adding systems and equipment may reduce insurance premiums for other areas of coverage such as theft, liability, and fire).
- Legal, professional, and consulting fees and charges.
- Permits and licenses.
- Security department, including (1) staff wages and benefits, payroll taxes, workers’ compensation claims and insurance, costs of uniforms, hiring, training, supervision, administration, liability claims, and liability insurance; (2) sundry items such as office and stationary supplies, administrative support, and so on; (3) utilities such as lighting, electricity, telephone, and network fees; (4) maintenance of systems and equipment used by the security department.

Depending on the building owner or manager, certain of these line items may be amortized over time, equipment may be leased, or other arrangements made to suit the building operation. It must be kept in mind that “one does not plan or budget for the unknown

---


* For office building and residential and apartment building owners and managers a key budget issue is whether such costs are escalatable or not. The term escalatable refers to costs the building itself incurs that may be charged proportionately to tenants and residents based on lease provisions. For example, costs associated with the building parking operation may be nonescalatable if parking operations are a separate profit center; whereas costs associated with the security operation are typically escalatable because they are part of the building’s operating expenses.

** Worker’s compensation insurance is “basic insurance [that] provides for medical costs, lost wages, and rehabilitation of workers injured on the job. There are also death benefits available” (Fischer, RJ, Halibozek E, Green G. Introduction to Security. 8th ed. Burlington, MA: Elsevier Butterworth-Heinemann; 2008:169).

*** Liability insurance is “that form of insurance which indemnifies against liability on account of injuries to the person or property of another” (Publisher’s Editorial Staff, Black’s Law Dictionary. 6th ed. [Nolan JR, Nolan-Haley JM, co-authors]. St. Paul, MN: West Publishing; 1990:805.
or the unpredictable; one budgets for intelligently anticipated and predictable conditions, based on known conditions in the present and the past.\textsuperscript{5} Natural disasters and catastrophic events are not predictable; budgeting, therefore, usually will not take them into consideration. (However, some buildings provide various supplies and equipment in case of an emergency or disaster. Of these items, food, water, and some medical supplies have a predetermined shelf life, and their replacement costs should be included in annual cost estimates.)

**Key Performance Indicators (KPIs)**

When the budget is reviewed, it is often difficult to measure the value of the services that the security department provides and to convince management that the security function does in fact generate income for the facility, if only indirectly. How does one, for example, place a monetary value on the security benefit video cameras installed in elevators have on building operations while other departments, such as parking, can justify their activities based on actual income produced, measured in hard currency? (A possible solution is offered later in this section.)

Key Performance Indicators, also known as KPI or Key Success Indicators (KSI), help an organization define and measure progress toward organizational goals.

Once an organization has analyzed its mission, identified all its stakeholders, and defined its goals, it needs a way to measure progress toward those goals. Key Performance Indicators are those measurements. Key Performance Indicators are quantifiable measurements, agreed to beforehand, that reflect the critical success factors of an organization. They will differ depending on an organization.

If a Key Performance Indicator is going to be of any value, there must be a way to accurately define and measure it. It is also important to define the Key Performance Indicators and stay with the same definition from year to year.

Many things are measurable. That does not make them key to the organization’s success. In selecting Key Performance Indicators, it is critical to limit them to those factors that are essential to the organization reaching its goals. It is also important to keep the number of Key Performance Indicators small just to keep everyone’s attention focused on achieving the same KPIs.\textsuperscript{6}

The director of security needs to demonstrate that the security function’s duties performed within a particular period of time (usually the past 12 months) have produced value commensurate with the funds allotted to it. This will establish the foundation for the budget for the ensuing fiscal period. For instance, with our aforementioned example regarding the benefit of cameras, it would be useful to quote previous expenses incurred to repair damage caused by vandalism in the elevators for a period of time


before and after the video installation. If the incidence of reported vandalism is lower after the installation, the monetary value, or KPI, of the security measure can be demonstrated. Not all aspects of the security function, however, can be assessed in terms of currency. For instance, how can one evaluate in monetary terms the absence of crimes of opportunity, such as thefts by intruders, which resulted from an effective security awareness program conducted by the security department?

Other criteria that can be established as KPIs for security staff are decreased number of security incidents, increased customer service satisfaction, increased completion of training courses, decreased staff turnover rates, and increased staff retention rates. Each of these KPIs must be clearly defined and then reasonable targets for each one agreed upon.

Contract versus Proprietary Security Staff

Security staff members that make up a security department in a building can be either employed directly by the building owner or manager (i.e., proprietary or in-house security) or employed by a contract security company (the process of contracting for a contract security service is referred to as outsourcing). Today, office buildings, hotels, residential and apartment buildings, and mixed-use buildings employ either proprietary or contract security personnel, or a mix of both proprietary and contract employees.

An office building, or a residential and apartment building, unless it is a major facility, usually does not have the luxury of a large human resource department to handle the many facets of recruiting, hiring, personnel management, and training required for security staff who work in their building and is therefore more likely to use a security contractor to supply its security staffing needs. A major hotel, which may have a large human resource department to handle the hiring of hotel staff, is more likely to hire its own security staff or at least a hybrid proprietary-contract security operation (where in-house employees staff the loss prevention management and supervisory positions, complemented by outside contract security staff).

The use of proprietary security staff has certain advantages to building owners and managers while the use of contract security staff has others.

---

*It has always been difficult to quantify the contribution that a security program makes to the overall operation of an organization. In addition, by the nature of what security does, the better the program that exists the more difficult it is to see the need. If we have a very secure environment, we will have few or no incidents. When management sees few or no incidents, it tends to downplay the need for the security function* (Azano HJ. *Fire Safety and Security for High-Rise Buildings.* Crete, IL: Abbott, Langer & Associates; 1995:25).

**Turnover rate** can be defined as the number of terminations for performance issues and voluntary resignations over a period divided by the total number of staff at the commencement of the period, whereas **retention rate** is the average time period for which staff have been employed. For the same sampled group, sometimes turnover rates for the staff may be relatively high due to a small portion of newly hired employees who continually turn over, whereas retention rates may be high due to the majority of the staff being stable and employed for extended periods of time.

***Of course, there may be exceptions where, for example, a residential building, despite the lack of a personnel department, may hire its own people, such as a doorman or a concierge.

****In facilities where there is a hybrid proprietary-contract security operation, communication between in-house management and supervisory personnel and the security contractor is crucial. The success of such an arrangement largely depends on there being a clear understanding of the responsibilities and duties of both parties.
Advantages of Proprietary Security Staff

- Staff is directly employed by the building owner or manager and so building management does not need to communicate with a contractor to supply their staffing needs.
- Staff is recruited, screened and selected using procedures and methods stipulated and controlled by the client.
- Staff can share the same benefit programs as other building employees.
- Staff, as employees of the building, usually has an undivided loyalty to the building and, depending on the building’s management arrangements, to the company that owns or manages the facility. As a result, there may be career opportunities for the security staff with the building owner or management firm.
- Staff is under the direct “employer–employee” control of the building owner or manager.
- Since a security contractor is not being used, there is no contractor management fee.

Advantages of Contract Security Staff

- Staff is recruited, screened, selected, uniformed, equipped, trained, supervised, insured, and paid for by the contractor, and building management does not need to be involved in the process.
- A contractor, particularly a major one, has access to a large labor pool of employees and can provide additional personnel and supervision during emergencies and special events.
- Building management can request under the terms of the contract that unsuitable staff working at the building be removed quickly.
- Replacements for employees who are absent from work because of sickness, holidays, vacations, and so on are the responsibility of the contractor.
- The security department can be rapidly downsized and employees reassigned by the contractor rather than being laid off from working.
- The contractor can supply forms, records, reports, office supplies, and auxiliary equipment required to carry out the security operation.
- The security contractor, if properly selected, will have staff within the company who can provide expertise to building management. A professional security contractor can formulate and document policies and procedures for the security staff, conduct investigations, provide advice and knowledge regarding developments in the security and life safety field, and assist building management in developing relationships with local law enforcement and the fire department.
- “An important benefit to all parties is that a guard now can aspire to advancement, and to promotion to a salaried status that includes the more attractive benefits that a major [security] company is able to provide. Consequently, the job attracts better-qualified guards and results in improved job placement.”
- Because most of the security program is being carried out by the contractor, although dependent on contractual terms, a portion of liability burdens reside with the contractor, not the building owner or manager.

---

Selection of a Contract Security Service

Building owners or managers who decide to employ a contract service to staff their security department and operate their security program must take special care to select a professional contractor—one that conducts business according to the highest ethical and industry standards and provides properly selected, screened, trained, and supervised staff. The building owner or manager also must ensure that fundamental provisions of the security services agreement between their facility and the contractor constitute an attainable goal—that the contractor reasonably can be expected to provide the requested level of service.

Prerequisites for a Successful Program

Competitive wages and benefits for staff, adequate working conditions and amenities, and a reasonable profit margin for the contractor providing the services are prerequisites for a successful security program. In addition to these factors, the client–contractor relationship must be clearly delineated and an essential element of trust established.

One does not have to go far to ascertain the root cause of high turnover of unsuitable, poorly trained, poorly supervised, poorly motivated, and disheveled security personnel—a predicament that, if it persists, will have devastating effects on any building security program. If this happens, the chances are that a professional contractor has not been selected or that the provisions, especially funding, of the security service agreement are not adequate for quality service. “The traditional contracting process for security guards involves few, if any, performance specifications. The user relies on the assumption that he [or she] is requesting and receiving proposals on a service with generally accepted performance standards.”

Vital Issues

The following issues need to be addressed in the contracting process:

- The state and local business licenses of the contractor should be examined.
- The history, ownership, and financial stability of the contractor should be reviewed.
- The liability insurance coverage to be provided by the contractor should be specified and proof of such insurance furnished.
- The requirements for each position that needs a contract security staff member (including a job description of the basic work to be performed, specific qualifications, and the expected hours of coverage) should be outlined in the proposal specifications.
- The wages and especially the benefits of the security staff need to be specified. These factors will not only impact the quality of service to be provided but will also permit the building owner and manager to make an “apples to apples” comparison.

---

*Including a provision in the contract for the hiring of a professional, adequately compensated contract security manager.

comparison between contractors. It is not enough for a contractor to say, “Yes, we provide vacations, holidays, and health insurance benefits for our security officers”; further information should be ascertained: How many days of vacation? What holidays are recognized? What is the name of the health plan? What benefits does the health plan provide? Does the employee contribute to its premiums? How much? What is the qualifying period before the plan is in effect? What is the deductible? What is the maximum allowable claim?

- A contractor’s management approach and depth of organizational staffing also need to be examined. Who are the managers and supervisors? How will they interface with the client and the site operation? What are their security qualifications, background, and experience both within the security industry and with the present contractor? How would they handle the startup and transition of contract security staff at the client site? Are they able to conduct risk assessments? How do they formulate and document policies and procedures for security staff working at client sites? How do they conduct training at client sites? How will they audit and evaluate performance at the job site?

- To help evaluate operational capabilities, it is a sound move to visit the contractor’s office and meet the administrative staff responsible for supporting the contract. A guided tour of the operation should be included to understand how essential tasks such as recruiting, screening, selecting, outfitting and cleaning of uniforms, issuing equipment, training, scheduling, supervising, administering the payroll, and billing are performed. One should also request sample personnel files to see whether the contractor has kept employment applications and records and has conducted background checks. If time permits, one should attend a training session to examine the quality of training and materials provided.

- To help determine whether the contractor has the necessary proven expertise, examine references of comparable clients to whom the contractor is currently providing service. Such references should reveal whether the contractor has fulfilled contractual requirements and performed at the level of service originally agreed upon, and they should also show the contractor’s responsiveness to problem solving and other requests. One might even visit and inspect client sites where the contractor provides a similar type of service to that being requested.

**Costs for Contract Service**

Contractors usually base their charges on an hourly billing rate for security staff working on a client site, commonly using the terms *spreadsheet* and *spread*. The *spreadsheet* details each hourly pay rate and its associated billing rate (or provides a weighted average or composite billing rate for all hours worked). The difference between pay and billing rates is the *spread*. The spread may include costs of background checks; uniforms; training; estimated overtime; paid holidays; sick leave and vacation; payroll taxes; health, life, and accidental death and dismemberment insurance; miscellaneous benefits; workers’ compensation and liability insurance; administrative overhead; and profit. The administrative overhead can include branch management, operations management, account management, human resources, scheduling, field supervision, legal expenses, training and communications, information systems, risk management, accounting (payroll, billing,
accounts payable,\footnote{Accounts payable is “monies due from others for services rendered or goods ordered and received” (Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:2.).} and general ledger\footnote{General ledger is “a formal record of all the financial transactions of a business. Ibid. p. 70.})), credit and collections, purchasing, sales and marketing, quality assurance, and executive costs. The costs of purchasing and maintaining equipment—such as vehicles, portable radios, mobile phones, and patrol management systems—usually are itemized separately.

**Importance of a Thorough Process**

Only after an exhaustive investigative proposal process can a client make a thoroughly informed and sound selection of a contract security provider. Once this is accomplished, a security services agreement outlining the general and specific terms of the contract, including terms of payment, should be fully executed with the client and contractor agreeing on its contents. If the selection process is pursued thoroughly, the client will not only be completely familiar with the selected company’s policies, procedures, and operations but also will have established a working relationship with key members of the contractor’s management team.

**Determining Adequate Levels of Security Staffing**

The level of security staffing needed to operate an adequate security and fire life safety program for any facility requires a two-step analysis. “It is necessary first to analyze the security mission, to determine the organization’s security [and fire life safety] vulnerabilities, and to identify the services to be rendered. The next step is to design a program that will address the mission, properly manage these vulnerabilities, and implement the intended services. Only then can the number of staff required to operate the program be determined.”\footnote{Colling RL. Security staff organization. In: Hospital and Healthcare Security. 4th ed. Woburn, MA: Butterworth-Heinemann; 2001:139.} In the high-rise setting, building management will first need to have a risk assessment conducted. After that, a security and fire life safety program can be designed and the appropriate staffing levels determined for the building.

The required levels of security staffing for high-rise buildings will vary according to a number of factors including the type of occupancy and its pattern of use, as well as the time of the day and the day of the week. For example,

- **Office buildings.** Staffing will tend to be higher during normal business hours, Monday to Friday, than after hours (including weekends and public holidays). During normal business hours, most tenants are open for business and there is an increased building population of tenant employees, visitors, salespersons, trades people, building management staff, building contractors, couriers, delivery persons, solicitors, building inspectors, and others who may require the attention of building security staff. After hours, pedestrian (and vehicle) traffic usually lessens and only the number of janitorial staff increases (unless special activities, such as a tenant renovation or a tenant move in or out, for example, are occurring). The actual numbers of staff will vary according to the size and design of the building, the services being offered, the complexity of operations, and the security needs of the facility.
- **Hotel buildings.** The actual numbers of staff will vary according to the size and design of the hotel, the services being offered, the complexity of operations, and the security needs of the facility.

- **Residential and apartment buildings.** Generally speaking, one would expect that after hours (including weekends and public holidays), fewer security staff members would be required. However, the actual numbers of staff will vary according to the size and design of the building, the services being offered, the complexity of operations, and the security needs of the facility.

- **Mixed-use buildings.** Staffing will vary according to the size and design of the building, the type of occupancies in the building, the services offered, the complexity of operations, and the security needs of the occupancies in the facility.

**Typical Positions**

Levels of security staffing, hours of coverage, and specific functions vary from building to building. The following supervisory and nonsupervisory positions (with actual job titles varying from building to building, region to region, and country to country) often are found in larger buildings:

- **Director of security** (or security director, security manager, chief of security, head of security, security supervisor, or, in a smaller building, post commander). He or she oversees and coordinates the activities of the security department.

- **Director of loss prevention or loss prevention manager.** Oversees and coordinates the activities of the security department, usually for a hotel (or a retail operation).

- **Fire safety director.** Establishes, implements, and maintains the building emergency management plan. In some buildings the director of security and the fire safety director is the same person. Sometimes known as the life safety director, life safety manager, building evacuation controller, or emergency coordinator.

- **Shift supervisor and watch commander.** Assigned to the various shifts—usually designated as day, swing or mid, and graveyard; or perhaps first, second, and third. Oversees and coordinates the activities of security staff assigned to their shift. Shift supervisors usually report to the director of security.

- **Lobby director, lobby ambassador, lobby officer, and doorman.** Assigned to lobby areas, control access to the building, provide information to building users and visitors, and perform other duties as specified by the facility.

- **Concierge.** Assigned to building lobby areas to provide information and services to tenants, residents, guests, and visitors, and perform other duties as specified by the facility. Traditionally a feature of major hotels, now many residential buildings provide concierge services.

- **Console operator and command center operator.** Assigned to the security command center to monitor and operate building security and fire life safety systems and equipment.

---

*The advent of web-based guest services software has considerably helped concierges to become more efficient and productive in their work. For example, “GoConcierge has simplified and helped automate reservation processes and guest activity tracking that concierges previously were doing manually via logbooks, binders and log sheets…. In addition to having a robust Guest Task Calendar component, GoConcierge also includes a customized, searchable database and contact list that includes links to area restaurants, attractions.*
- **Dockmaster.** Supervises the loading dock/shipping and receiving areas, including all loading and unloading operations.
- **Doorman.** “An individual hired to provide courtesy and security services at a residential building or hotel. They are particularly common in urban luxury highrises [and major hotels]. At a residential building, a doorman is responsible for opening doors and screening visitors and deliveries. He [or she] will often provide other courtesy services such as signing for packages, carrying luggage between the elevator and the street, or hailing taxis for residents and guests.”\(^{10}\) At hotels, doormen provide a wide variety of guest services.
- **Freight/service elevator operator.** Operates the freight/service elevator and screens all elevator users for authorization to travel to various floors of the building.
- **Security officer.** Performs security and fire life safety functions as determined by the building operation. Also known as a **security guard.**
- **Patrol officer, parking patrol, and rover.** Patrol various parts of the building and parking areas and perform other duties as specified by the facility (patrols may be on foot or using a motor vehicle, an electric cart, a bicycle, a tricycle, or a personal transporter).
- **Training officer.** Particularly in larger projects, trains and tests all building security staff in their duties and responsibilities.

The essential functions required for each of these positions should be specified in a job description and a job specification. A **job description** is “a written statement of what a jobholder does, how it is done, and why it is done. It typically portrays job content, environment, and conditions of employment.”\(^{11}\) The **job specification** “states the minimum acceptable qualifications an incumbent must possess to perform a given job successfully. It identifies the knowledge, skills, and abilities needed to do the job effectively.”\(^{12}\)

“The job description and job specification are important documents when managers begin recruiting and selecting new hires. The job description can be used to describe the job to potential candidates. The job specification keeps the manager’s attention on the list of qualifications necessary for an incumbent to perform a job and assists in determining whether candidates are qualified.”\(^{13}\)
Security Staff Duties and Written Instructions

The primary role of security staff in a high-rise building is to help implement the security and fire life safety program. Some buildings may have a separate safety department; in others, the security department may assume safety responsibilities. Duties of the security staff vary from building to building and depend largely on the policies and procedures determined by management.

Security staff duties should be written clearly, concisely, and accurately and kept readily accessible for training and for reference during an emergency. These security instructions (commonly called post orders or standard operating procedures) should be periodically reviewed and regularly updated.

What Should Post Orders Contain?

Post orders should contain at least the following information:

- Statement of purpose and a notice of confidentiality.
- An overview of the building and a profile of the tenants or residents.
- List of public telephone emergency telephone numbers for police and fire departments, emergency services, paramedics or ambulance services, utility companies, and other agencies.
- List of after-hours telephone contact numbers for building management, engineering, security, janitorial and parking staff, elevator company representatives, security and fire alarm companies, hazardous material contractors, window boardup contractors, and so on.
- Description of the building and its operation, including up-to-date floor plans and maps and security and fire life safety systems and equipment. This should include an overview and description of each system, an account of how the systems operate under normal and emergency conditions, and an explanation of how system components are related and connected. Photographs and diagrams make the descriptions more understandable.
- Review of subjects such as building access control, handling trespassers, tenant/resident/guest access, handling service of process (writs, complaints, summonses, etc.), key and equipment control, property control, escorts of building users, mobile patrols, arrest policy, and other policies and procedures.
- Specific instructions on handling emergency situations such as aircraft collisions; bombs and bomb threats; daredevils, protestors, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstrations, and civil disorder; medical emergencies; natural disasters; contractible diseases; power failures; slip-and-falls; workplace violence; traffic accidents; and water leaks.

---


**A procedure is “detailed instructions for implementing security policies; often presented as forms or as lists of steps to be taken.” Ibid.

***Post orders are detailed procedures for carrying out security policies and routinely performing duties.
• List of security staffing levels, hours of coverage, and specific functions and job duties. Wherever possible, the duties should be described by shift, day of the week, and specific time. Key performance indicators should be explained in terms that the security staff can clearly understand.

• Instructions on public relations (including how to handle hostile situations and telephone and radio communications techniques) and how to conduct interviews and write reports. (These subjects either may be included in the instructions or may be communicated to security staff through other means.)

• A code of ethics and standards of conduct. These should be established to help foster a strong ethical climate throughout the security organization and to provide clear and specific guidance to employees.

  ◦ Code of ethics. Adherence to professional ethics is critical in any organization, but particularly so in one entrusted with the security of a high-rise building. Ethics is defined as “a system or set of moral principles … the rules of conduct recognized in respect to a particular class of human actions or governing a particular group.”

  An ethical act or decision is “something judged as proper or acceptable based on some standard of right or wrong. Although people often have different morals and standard of right and wrong, many are shared by most members of our society.” Professional ethics are very much a matter of conscience, which is defined as “the inner sense of what is right or wrong in one’s conduct or motives.” Because ethics require this inner sense, there is no guarantee that the existence of a code of ethics will prevent undesirable actions by a security employee. However, such a code does clarify to security staff what is expected of them. See Appendix 7–1 on the CD-ROM provided with this book for a Sample Security Officer Code of Ethics.

  ◦ Standards of conduct. These specify behavior that may be subject to disciplinary action: unexcused absences or excessive tardiness, unacceptable appearance or attire, use of profane language, making racial or ethnic slurs, engaging in sexual or other forms of harassment, disorderly conduct, sleeping or dozing on the job, being insubordinate, unauthorized disclosure of confidential information, making false statements, unauthorized use of company property, unauthorized acceptance of gifts, failure to observe security and safety rules and regulations, and so on.

These instructions may be housed in one binder (preferably a ringed one that permits easy removal and replacement of pages) or in separate binders or folders (or possibly stored online). The binders or folders should be clearly labeled for easy reference. All copies should include the date the instructions were established or last revised, by whose authority the instructions were made, and which individuals have the authority to change or modify them. Changes and modifications made to operating procedures should be dated and incorporated into all existing copies of instructions as soon as possible. Outdated instructions should be retained for a period varying from five to seven years (as determined by the building’s document retention policy or legal advisor), because they may be needed later in litigation defense.

---


Writing Post Orders

Instructions for complex procedures and systems must be comprehensively written in easy-to-understand, action-oriented terms, keeping in mind the literacy level of the intended reader. The writer should avoid cumbersome writing and overuse of the passive voice. For example, “Building console operators while away from the security command center are required to maintain a two-way radio on their persons at all times” can be understood more easily if written, “When away from the security command center, always carry a two-way radio with you.” Like any extensive document, the instructions should have a clearly labeled table of contents and numbered pages and, for ease of reference, each subject should be separately tabbed and there should be an index. Photographs, diagrams, checklists, summary sheets, and flowcharts should be included to make the material more interesting and easier to comprehend.

Written Records and Reports

Security staff in a high-rise building must make observations and provide thorough and accurate recording and reporting of security and safety operations, activities, and incidents. Observation may involve any of the senses—sight, hearing, smell, or touch—and requires the capacity to understand the meaning of what has been observed. “In security work it is important to determine whether what has been observed is significant for security or safety and is routine or unusual.” After observation and appropriate action, security personnel must furnish an accurate record and report of important observations.

Forms, records, and reports used by security staff may vary from building to building, but all aim to provide a thorough, accurate, and permanent account of events that have occurred. Such documentation can be used to generate statistical data that may be useful to justify, for example, existing or future expenditures for security and fire life safety systems and equipment.

Types of Forms, Records, and Reports

Some common forms, records, and reports found in high-rise facilities are as follows:

- **Shift activity report.** Includes the date and commencement time of duty; name, badge, or employee number (if appropriate), and signature of the reporting officer; passed down information from the previous shift; position or post to which the officer is assigned; equipment the officer received (including keys, patrol...
monitoring devices, radio, pager, etc.) and where or from whom this equipment was received; a chronological narrative of events and incidents that occurred while the officer was on duty; the time of completion of duty; and possibly the name of any supervisor who reviewed the report (including the date and time of this review). It generally does not contain detailed descriptions of unusual events and incidents such as crimes and accidents. The report should be in duplicate so that an original is available to building management and the security department can retain a copy. Some reports are compiled using shift log database software.

- **Incident report.** Elaborates on unusual events and incidents and may include name, badge number (if appropriate), and signature of the reporting officer; the incident’s date, time, type, and location; a full description of the incident; names and contact details of any victims, suspects, and witnesses; action taken (including who was notified of the situation); and follow-up action that may be required. Any photographs, sketches, or exhibits should be noted on the report and clearly labeled. The report should be in duplicate or triplicate, so that the original can be supplied to building management, and the security department can keep at least one copy. Some reports are compiled using incident reporting software (see the later section, “Computerized Incident Reporting”).

- **Safety hazard report.** Similar to the incident report but reports a hazard rather than an incident.

- **Vehicle accident report.** Includes name, badge, or employee number (if appropriate), and signature of the reporting officer; date, time, and precise location of the accident; description of the accident (including a sketch of the accident scene) and property damage; posted speed limits, stop signs, traffic lights, and signals; license number of vehicle(s); estimated speed of vehicle(s); weather and light conditions; indication of whether seat belts were in use; any evidence of substance abuse; name, driver’s license number, and contact details of driver(s); details of insurance companies of driver(s); name(s) and contact details of injured person(s) and witnesses; the action taken (including who was notified of the situation and whether a traffic citation was issued); and follow-up action that may be required. Any photographs, sketches, or exhibits should be noted on the report and clearly labeled. The report should be in duplicate or triplicate, as in the case of an incident report.

- **Tenant/resident and visitor log.** Includes the name (printed for legibility) and signature of persons entering or leaving the building, the name of the company they represent or the tenant/resident they are visiting, the date, and times in and out.

- **Courtesy notices.** Vary in format depending on designated purpose. The security or parking department may use special parking courtesy notices to inform a driver that his or her vehicle was found parked (1) illegally (with a reminder to park in designated areas only); (2) incorrectly (with a reminder to park correctly in a designated parking stall); (3) in a space reserved for the disabled; (4) with the vehicle unlocked, with windows open, or with personal property in view; or (5) to report some other vehicle-related matter that needs to be brought to the driver’s attention. These notices should be designed so that an original can be left on the vehicle—• and a duplicate retained by the issuing department.

---

• When placing such a notice on a vehicle, locating it in the lower corner of the driver’s window (immediately above the door handle) will make it visible to the driver when entering the vehicle, but will not obstruct his or her field of vision when driving.
• **Tenant/resident security notice.** Used by security staff to notify a tenant/resident, for example, that a door to its area was found unsecured and subsequently locked by security at a specific time. The notice could be designed to hang on a door and a copy or tear-off portion retained for future reference. The building security department also should notify the designated tenant contact person of the security violation on the next business day, or the resident as soon as possible.

• **Security and fire life safety equipment maintenance reports.** Malfunction or failure of security and fire life safety systems and equipment should be reported in a timely manner; also, records of such work should be maintained to aid in planning future capital expenditure.

There may also be contractor sign-in logs; personnel escort logs; elevator malfunction reports; security and fire life safety systems and equipment checklists; fire alarm report logs; stairwell inspection reports; lost and found property reports; and various other forms, records, and reports designed for use in the building.

**Use of Notebooks**
Security staff may also use notebooks to record details that, at a later stage, can be produced as legal evidence. These books should be small enough to fit snugly in a pocket, equipped with hard covers to protect the pages, bound, and sequentially numbered to make the removal of any pages immediately evident. “A bound notebook creates a more favorable impression in the courtroom than the looseleaf type, since its form does not suggest the possible removal of pages…. Obviously, ink is preferred to pencil for permanence.”


**Who, What, When, Where, Why, and How**
The Protection Officer Training Manual outlines the six essential components of any successful report as follows:

- **Who**—relates to who was involved in the event, the name(s) of the complainant, client, witnesses, suspects, accused parties, or [security staff].
- **What**—relates to the type of incident or event, what actually occurred.
- **When**—this is the time and date that the incident occurred.
- **Where**—this is the location that the event took place, with subsequent locations depending on the type of incident.
- **Why**—this is the motive. It can frequently be determined by proper investigation. It may explain the reason for the occurrence, but cannot be speculation or unfounded opinion [by security staff].
- **How**—how did the event come to your attention? How did it occur? This means the complete details on how the event happened from start to finish.

All six of these components will be present in even the simplest event. Not recording some details because they seem unimportant at the time results in lost information that eventually may prove valuable; it may also lead to an embarrassed security staff.
member having to explain a sloppy report to an irate security supervisor, a building manager, or an investigator.\textsuperscript{19}

\textbf{Legible, Thorough, Accurate, Clear, Concise, and Prompt}

Legible, thorough, accurate, clear, concise, and prompt documentation of incidents is of inestimable value to building owners and managers, particularly when litigation occurs. Incidents, such as slip-and-falls, do occur in high-rise buildings, and much of the potential for liability can be mitigated substantially by handling, recording, and reporting these incidents in a thoroughly professional and competent manner. “For clarity’s sake the author should write reports in the first person. The narrative should never make judgments regarding responsibility or blame for any loss or injury and should not refer to prior similar events.”\textsuperscript{20}

Reports of security staff should be reviewed by supervisors and “any spelling or structural errors should be noted, and the report rewritten by the original author. Substantive changes—normally made by the author—should only be made after discussion [by a supervisor] with the author. Otherwise, an opposing party in litigation might infer that an effort was made to hide something.”\textsuperscript{21}

\textbf{How Long to Keep Reports?}

The retention period for reports depends on the type of report, the requirements of state law, and the building’s policy. This period may vary from a few months for shift activity reports and activity logs, to three to seven years for incident reports. It should be considered that “reports help identify future security needs and that a claim of inadequate security can be brought anytime during a state’s statute of limitations for negligence (two or three years from the date of injury in most jurisdictions). With that in mind, reports should be kept at least until the local statute of limitations expires.”\textsuperscript{22}

\textbf{Computerized Incident Reporting}

In the past, all records and reports were recorded on paper. Today, because of technological developments, information can be managed using computer software programs. \textit{The PPM 2000 Security Management Software InCase System},\textsuperscript{23} for instance, allows a personal computer to sort data contained in incident reports by time of the day, day of the week, the month, the year, the type of incident, the suspect, or any other user-defined field in the reports. This allows an incident reporting system to be tailor-made for a facility and the analyses it conducts. Trends in certain types of incidents can be discovered, weaknesses revealed, and loss prevention strategies devised. “Computers allow a security department to work smarter since vast amounts of information can be stored in a small space and retrieved at any time. Operations reports no longer have to be done manually. Budget figures can be obtained and expenses monitored at will.”\textsuperscript{24}


\textsuperscript{21}ibid.

\textsuperscript{22}ibid., p. 80.


Selection, Training, Testing, and Supervision of Security Staff

Security staff for a high-rise facility must be properly selected, trained, tested, and supervised. All of these processes must be thorough and well documented, especially in today's litigious society.

Selection

Selecting the right person to work in the high-rise environment begins at recruitment. The applicant should fill out a comprehensive employment application and a thorough background check should be conducted.

A good background check should include the following: proof of identity and right to work; aliases; current address and previous addresses for the past ten years; educational background; current and past employers and supervisors (for the past five years), with explanations of any breaks in employment greater than 30 days; details of any military service; criminal convictions and records check; surety that the applicant can comply with all applicable state and local security personnel registration and licensing laws; a check of financial responsibility and character references; drug screening; integrity testing; and if driving is a job requirement, proof of a valid driver's license and a driver's record check.

Honesty, trustworthiness, helpfulness, and loyalty are important character traits to look for in a candidate. Because certain security positions require specific physical prowess or mental ability, an applicant should be evaluated for meeting essential performance standards.

Today's security officer must successfully operate equipment that is at times highly technical, particularly that installed in high-rise towers. He or she must operate hand-held radios and monitor CCTV systems, elevator recall panels, fire annunciator panels, and card access and intrusion detection systems. Most importantly, from the perspective of fire and life safety, the modern security officer must respond appropriately during building emergencies such as fire, earthquakes, bomb threats, medical emergencies, and power failures.

Individuals monitoring security and fire life safety systems and equipment in the security command center require a certain level of intelligence to handle these complex tasks. Employers are prohibited from discriminating against qualified individuals with disabilities; however, if an applicant cannot perform an “essential job function” (in this case, carrying out complex monitoring duties) because of a physical or mental disability for which the employer cannot make a “reasonable accommodation,” the applicant can be rejected. Applicants also should be tested to determine if they are able to read, write, understand, and speak effectively. Security personnel often are required to understand complex verbal and written instructions and to write detailed reports. They must be able to maintain language comprehension and fluency not only during the performance of regular duties but also under the emotional stress of an emergency or crisis situation.

Applicants should be evaluated for standards of personal appearance and hygiene, and they must possess public relations skills sufficient to allow them to interact in a positive manner with people that include fellow security staff, building management, tenants, residents, guests, and visitors, law enforcement and fire department personnel, the media, and the general public.

Training and Testing
Once appropriate individuals have been selected, they must receive sufficient training to perform duties required of their positions. Training is defined as “the formal procedure which a company utilizes to facilitate learning so that the resultant behavior contributes to the attainment of the company’s goals.”26 In our case, the company is the security department, and the company’s goal is to administer the building’s security and fire life safety program effectively.

Three Key Training Areas
A building training program can be separated into three distinct areas:

1. **New employee orientation.** This basic training should be at least eight hours long and introduce basic security concepts as they relate to high-rise building security and fire life safety programs. Areas to consider are as follows:
   - What is security and fire life safety?
   - Building and assets protection
   - Security systems and equipment
   - Security rules and procedures
   - Mobile patrol techniques
   - Fire life safety systems and equipment
   - Fire prevention
   - Standards of conduct and code of ethics
   - Security and the law (including basic law and arrest law, and legal powers of arrest)
   - Role of law enforcement versus private security
   - Role of public relations and diplomacy
   - Use of force
   - Effective communications
   - Interview techniques
   - Observation techniques and report writing
   - Uniform policies and grooming standards

   The training may include written materials, audiovisual aids, interactive computer programs, and classroom instruction from competent personnel. Testing (whether it is written, verbal, or practical) should be used to evaluate the trainee’s performance, including a performance audit of the trainee’s ability to conduct each step to complete a specific task.

---

2. **On-the-job training.** This basic orientation training, referred to as OJT, will vary from 8 to 40 hours in length depending on the complexity of the building and the position for which the person is being trained. The training should orient the person to the building and its security and fire life safety program, equip the trainee with the necessary skills and job knowledge to carry out the responsibilities of the designated position, and help build confidence through hands-on experience. Activities to include are as follows:

- A tour of the building exterior, selected floors, passenger and freight/service elevators, stairwells, parking areas, loading dock/shipping and receiving areas, roof areas, and maintenance spaces (including mechanical areas and elevator machine rooms)
- Inspection of building fire life safety systems and equipment
- Inspection of building security systems and equipment and key controls
- Review of building security rules and procedures
- Review of building occupant fire life safety instruction
- Review of security instructions or post orders, including the complete job description for the trainee’s position, and emergency response procedures
- Explanation of the chain of command within building management and the security department
- Orientation to the designated position
- Any specialized training such as emergency medical technicians, first aid, cardiopulmonary resuscitation, or use of portable defibrillators may be conducted before assignment or within an agreed-on time period following assignment

There are several problems associated with OJT. Its quality will depend largely on the competency of the trainer; if this person has performance deficiencies, they will be passed on to the trainee. What the individual learns will depend on what events occur during the training session (some areas may be missed simply because on that particular day some routine events did not occur), and the training itself may interfere with the job that is being demonstrated. Written, verbal, and practical tests (including a performance audit of the trainee’s ability to conduct each specific step to complete a specific task) should be used in OJT to evaluate comprehension and performance and help ensure that the trainee has acquired the necessary skills to assume the responsibilities of the position. The extent and complexity of these tests will depend on the size, intricacy, and requirements of the security operation.

3. **Ongoing or in-service training.** After employees have been assigned to work, there should be follow-up to enhance their performance. Employees should be kept constantly informed of changes in the security program and undergo ongoing instruction and testing in key areas. Nowhere is this better demonstrated than with security personnel who handle building emergencies such as fires and fire alarms. Such events usually do not occur on a daily basis in buildings.

---

*A suggested building tour focusing on its fire life safety systems and equipment is provided as Table A9–5 in Appendix 9–2 on the CD-ROM provided with this book.*

**Chain of command is “the line of authority and responsibility along which orders [or instructions] are passed” (Chain of command. Wikipedia. September 6, 2008. <http://en.wikipedia.org/wiki/Chain_of_command>; October 4, 2008).*
(if they do, an investigation should be conducted to determine the reason), but the security staff needs to be in a state of readiness to handle them competently. This is only possible if staff members periodically rehearse the procedures that are involved. Hands-on practice, drills, and testing (verbal and written) are all components that assist in this learning process.

Ongoing training can also be facilitated by: handouts of written policies and procedures, pamphlets, bulletins, newsletters, e-mails, films, videos, interactive computer programs, meetings, briefings, conferences, panels, seminars, and workshops. Also, staff may be given self-instructional material and then be required to satisfactorily pass a written test.

Quality assurance audits by security supervisors are essential. If certain procedures are not being performed correctly or with confidence, the procedure may need to be reevaluated and retraining administered. Inconsistencies or perceived problems in security sometimes are a prompt for training. For example, in an office building, tenants may complain to building management that after normal business hours they sometimes are challenged to produce passes to remove property from their building, and sometimes are not. The supervisors should check that all security personnel fully understand the building property removal control policy and are aware of the need to consistently apply it.

The training program for each person should be thoroughly documented. Training files should be established for every member of the building security department. A Security Officer Training and Testing Log (see Appendix 7–2 on the CD-ROM provided with this book for a sample log) can be used to summarize each individual’s training and testing.

Supervision

When an individual is appointed to a supervisory position, special training may be needed to equip him or her with supervisory skills. To supervise is “to watch over and direct (a process, work, workers).” 27 A supervisor is a person who watches over staff or the labor performed by others. In a building security department, supervisors guide and direct staff to perform security and fire life safety duties. Let us examine this further.

Watching Over Security Staff

There are various ways to watch over staff employed in a high-rise building. Managers and supervisors might visit each position or post staffed by security personnel to observe and evaluate an individual’s performance. Visits may include watching officers carry out their duties and responsibilities, asking them to demonstrate the operation of equipment, reviewing their reports, and posing hypothetical situations to evaluate officers’ responses. Building tenants, residents, and guests can also contribute to the supervisory process by promptly communicating any difficulties with security staff either to building management or directly to the security department.


*In supervising staff it is essential that there is an adequate span of control. Span of control “addresses how many subordinates a manager can efficiently and effectively direct” (Robbins, SP. Managing Today! 2nd ed. Upper Saddle River, NJ: Prentice-Hall; 1999:582).
Guiding and Directing Security Staff

Various ways and means can be used to guide and direct security staff to perform responsibilities as determined by the building’s security and fire life safety program.

Basic Tools

Employees need the following basic tools to do their job:

- A well-defined security and fire life safety program with clearly documented and communicated building policies and procedures
- Security and fire life safety systems and equipment that are adequate for the building’s program and maintained in good working order
- Up-to-date, thorough, accurate, concise, and clearly defined security and fire life safety instructions that are readily available for reference
- Comprehensive and well-designed orientation, training, and testing programs for security staff

Security staff personnel also need a working environment in keeping with their required professional image. Building owners and managers sometimes overlook amenities such as well-maintained changing areas, secure storage areas for personal belongings, and adequate rest areas and break areas, but these are essential to the welfare and morale of security staff. Supervisors should, if possible, have access to a private area where counseling can be conducted in a professional setting with minimal distractions. If the security department is large enough to warrant a director of security, a private office should be provided where the director can work and safely store reports and confidential employee files. It is not uncommon to find building security staff who are required to change uniforms in corridors or public restrooms, security uniforms stored in building fan rooms, nonexistent break areas, and the director of security housed under the stairs or in an area where no privacy or adequate work space is afforded. These conditions degrade the morale of the entire security department and can cause a “less than professional” attitude of security staff at work.

How to Motivate

Many theories are available about motivating employees to perform better, work harder, and stay interested in what they are doing. The following actions can produce positive results when appropriately applied by supervisors.

- Viewing each staff member as a unique individual and approaching each in an appropriate manner.
- Knowing the strengths and limitations of employees and assigning them to positions of responsibility that match those strengths and limitations.
- Taking a genuine interest in employees and treating them with courtesy and respect.
- Adequately training employees so they know what is expected of them.
- Communicating clearly, concisely, and in a timely fashion so employees can adjust to any requested changes in duties and responsibilities. Actively listening to employees and encouraging their ideas and input: “What do you think we can do about the recent vehicle break-ins?”
- Making requests of employees rather than giving direct orders: “Sarah, would you help Philip over at the loading dock?” The problem with direct orders is that people sometimes disobey them. If a person refuses to comply, then the supervisor’s authority and ego are challenged. Of course, direct orders are needed under certain circumstances.
Giving positive feedback, compliments, and recognition to employees: “Searcy, thank you so much for the great job that you did handling the special event today.”

Performing periodic employee performance reviews and evaluations.

Assisting employees to develop skills and self-confidence and encouraging them to accept responsibility.

Assisting employees’ advancement and promotion within the organization.

Supporting employees, particularly during difficult personal situations that they may be experiencing.

Handling complaints from employees in a timely, fair, and equitable manner.

Being decisive and avoiding vacillation.

Not making promises or commitments that cannot be met.

Admitting a mistake when it has occurred and apologizing when necessary or appropriate.

Maintaining a professional code of ethics and a standards of conduct and not compromising personal standards.

Employee recognition programs are an important tool in staff retention, boosting morale, raising the quality of service rendered by security staff, and reducing overall operational costs. They decrease staff turnover, thus reducing the amount of training and supervision required.

Security staff that carry out responsibilities in a competent and professional manner may be recognized by an award for employee of the month, quarter, or year; for an outstanding job performed in handling a particular situation; or for length of service. The recognition program may take the form of a letter of appreciation, newsletter writeup, certificate, plaque, personalized badge, tie tack, pin, gift, or a cash award. The recognition of security staff members often motivates others to excel.

Discipline

Discipline is an effective and necessary tool of supervision. According to Sennewald,

The word discipline is derived from the Latin discipulus ("learning"). The word disciple comes from the same root: the early Christian disciples were considered "students" of Christ. The origin of the word suggest this important concept: Positive and constructive discipline is training that corrects, molds, or strengthens an employee in the interests of achieving departmental and company goals. Punishment, the factor that is feared and disliked by all, is secondary. Any punishment connected with discipline should always be a means to an end, and that end should be organizational, not personal.\textsuperscript{28}

Sennewald added certain principles that need to be taken into consideration when an employee is being disciplined:

\textit{Principle 1—Assume Nothing. Ensure that everyone knows the rules. Put the rules in writing; make them a regular item of discussion in formal and informal}

sessions; disseminate and display them prominently. An employee who does not know the rules cannot be expected to follow them, and a supervisor should not discipline an employee when there is doubt that the employee was aware of the rule.

Principle 2—Discipline in Privacy. Receiving discipline is never a pleasant experience and can be particularly unpleasant in the presence of co-workers or others who have no legitimate role in the process. Embarrassment, anger, and resentment are the natural emotions that follow criticism given publicly. Discipline is a private matter to be handled behind closed doors or in a setting that ensures absolute privacy.

Principle 3—Be Objective. Rely on facts, not opinions and speculations. Consider all the facts and examine them with an open mind. Look for and eliminate any biases, for or against the offender. Make sure there is in fact a violation and determine the relative severity of the violation. Was the offender’s act aggravated or mitigated in any way?

Principle 4—Educate the Violator. Administer discipline that is constructive. The purpose is to bring about a positive change in the violator’s conduct or performance. Discipline should be a learning experience in which the violator gains new insights that contribute to personal improvement.

Principle 5—Be Consistent. Inconsistent enforcement of policy and rules should be totally unacceptable. For example, if the policy of the department is to terminate officers who sleep on the job, then all officers so found must be terminated. To fire one and not another will breed contempt for the rules and those who set the rules [and can result in formal labor complaints and/or lawsuits].

Principle 6—Do Not Humiliate. The intended outcome is to correct, not hurt. When humiliation is made a part of the process, the offender will come away angry, resentful, and perhaps ready to fail again. Both the offender and the organization will suffer as a consequence.

Principle 7—Document Infractions, Counseling, Discipline, and Corrective Actions. Make a record of violations. This is not to say that a negative dossier should be maintained on each employee, but it does mean that instances of unacceptable performance have to be recorded. The record of an employee’s failures is valuable as substantiation for severe discipline, such as termination, or as a diagnostic aid to counseling professionals.

Principle 8—Discipline Promptly. With the passage of time, an uncorrected violation fades into vagueness. The violator forgets details, discards any guilt he or she may have felt at the time of the violation, and rationalizes the violation as something of little importance. When opened for discussion, an uncorrected violation is likely to lead to disagreement about what “really happened” and any disciplinary action at that point can appear to be unreasonable.

Generally speaking most employees want to do a good job. If an employee is having performance problems, however, the supervisor must discipline the employee in a professional manner and focus on the problem, not the personality of the offender.

The intention is to train, develop, and improve performance and, perhaps, to rescue a valuable employee from failure.

**Training Supervisors**

In providing comprehensive training to new or experienced security supervisors, the following areas should be addressed:

- Responsibilities and duties
- Leadership skills
- Communication skills
- How to develop relationships
- How to avoid sexual harassment
- How to avoid favoritism
- How to handle complaints
- How to conduct audits and inspections
- How to document inspections
- How to counsel and discipline
- How to conduct performance evaluations
- How to develop organizational skills
- Time management
- Stress management

Sometimes when nonsupervisory employees are promoted to supervisory positions, they need to be taught to think and behave as supervisors rather than as line employees and to alter their interactive relationships from “peer-to-peer” to “peer-to-subordinate.” If they do not make this transition, they will not become effective supervisors. According to Vail, “the best leaders know themselves, their strengths, their weaknesses, their skills, and their abilities. Most of all, they know how to control themselves and present a commanding image that will inspire subordinates. They commit themselves to continually developing leadership characteristics in themselves and their subordinates.”

**Uniforms and Equipment**

Various types of uniforms and equipment are supplied to security staff working in a building environment. Uniforms are an essential part of the appearance of security staff. Security staffs who are well groomed; outfitted in well-tailored, clean, and pressed uniforms; and have clean and well-polished appropriate footwear exhibit a professional appearance. In so doing, their overall effectiveness is considerably enhanced.

The image that a building’s owners and managers desire security staff to exhibit will determine the style and selection of uniforms. Because security personnel are often viewed as service providers and ambassadors of a building, uniforms tend to project less the military/law enforcement image than the professional concierge image. Instead of security patches

---


* However, security officers, particularly those conducting exterior patrols and working in “back-of-the-house” areas, such as vehicle inspection areas, parking garages, loading docks, shipping and receiving areas, and freight and service elevators, are frequently dressed in military-style uniforms.
and badges on shirts adorned with shoulder epaulets and button-down shirt pockets, staff may be outfitted in a “soft-looking” uniform of tailored slacks, white dress shirt, business tie,* and blazer, or, in some instances, a tailored business suit. Often a discreet nameplate identifying the wearer and possibly a monogram of the building’s logo on the blazer or suit coat pocket, are the only identifying marks on the uniform. There is the potential that the soft look may detract from the perceived authority that the security officer projects.

Some security department manager and supervisor positions may even be required to wear traditional business attire without any conspicuous security identifiers. (In many office buildings, hotels, and residential and apartment buildings the director of security or the director of loss prevention will wear a business suit.)

It is highly unusual for security staff assigned to commercial buildings to be armed with weapons. It is potentially dangerous for weapons such as firearms, chemical agents, aerosol propelled agents, and nightsticks or batons to be used—the chances of a building tenant, resident, guest, visitor, or innocent bystander being injured or killed in a situation involving a weapon are elevated. However, some tenants (such as retail banking institutions) and residents do employ armed security personnel within their premises, and some corporate executives retain armed executive protection staff (as is sometimes the case in hotels when high-profile politicians and celebrities visit). Also, during periods of civil unrest, some buildings have used civilians trained and certified to carry concealed weapons to supplement unarmed security staff. However, such deployment is unusual in the high-rise setting and is generally reserved for special and highly unusual circumstances.

All equipment used by security staff should always be kept in good working condition.

The Role of Public Relations

Public relations plays a vital role in the administration of the security function in a high-rise building. Security personnel are exposed to all types of people in their daily work. They are expected not only to provide directions and information about the facility and its locale but also to persuade people to cooperate willingly with the security program. In carrying out these responsibilities, they are required to conduct themselves in a professional manner at all times. How effectively they interact with people directly influences the overall image of security in the building and indirectly reflects on the facility owner or management.

Good public relations entails creating kindly feelings and positive interaction between an organization and the public. It should not be identified with the image of a slick salesperson promoting a product. Rather, in the security context, it implies professional and well-trained staff interfacing with the public in a manner that favorably reflects on their department and the building. Good public relations allows staff to carry out the roles and objectives of the building security program effectively and can be invaluable in getting people to comply willingly with security rules and procedures. To create the positive impression so essential in human relations, security staff should do the following:

- Be well groomed, with good personal hygiene
- Be outfitted in clean, well-tailored, and pressed uniforms with clean, well-polished appropriate footwear
- Have what is best described as a “military bearing,” whether sitting or standing

*Clip-on ties are often used to alleviate the potential for an officer to be pulled down using the tie or even choked during a physical altercation.
- Have a smile on their faces at the appropriate time
- Maintain good eye contact with people, particularly when they are talking to them
- Use nontthreatening body language
- Practice good listening skills and speak politely and courteously, using key phrases and words such as “Please,” “Thank you,” and “May I help you?”
- Remain calm, avoiding outward displays of emotion when confronted with hostile or hazardous situations
- Carry out their duties and responsibilities with decisiveness and consistency

Good human relations for the security officer begins with an interest in people and in their safety and welfare. When successful, it produces mutual good feelings and willing cooperation. Cooperation is the real meaning of good human relations at all levels…. It is only through cooperation of all concerned that security officers can carry out the mission of protecting people and property. Good human relations is the basis of good security.31

Summary

- A successful security program in a high-rise building must have an adequately funded security budget.
- Key performance indicators help measure the value of security services.
- Security staff may be directly employed by the facility’s owner or manager (i.e., proprietary or in-house staff) or by a contract security firm (i.e., contract staff).
- Adequate numbers of security personnel should carry out the responsibilities and duties of the security program.
- Duties of security staff should be documented in comprehensive security instructions that are clear, concise, accurate, periodically reviewed, and regularly updated.
- All security staff must be properly selected, trained, tested, supervised, uniformed, and equipped in order to perform their job in a professional manner.

Key Terms

Accounts payable. “Monies due from others for services rendered or goods ordered and received.”32
Budget. “An estimate, often itemized, of expected income and expenses for a given period of time in the future…. A plan of operations based on such an estimate.”33
Chain of command. “The line of authority and responsibility along which orders [or instructions] are passed.”34

---

Concierge. Provides information and services to building tenants, residents, guests, and visitors, and performs other duties as specified by the facility.

Console operator and command center operator. Monitors and operates building security and fire life safety systems and equipment.

Contract security. “Protective services provided by one company, specializing in such services, to another company on a paid, contractual basis.”  

Director of loss prevention or loss prevention manager. Oversees and coordinates the activities of the security department, usually for a hotel (or a retail operation).

Director of security. Oversees and coordinates the activities of the security department. Also known as security director, security manager, chief of security, head of security, security supervisor, or, in a smaller building, post commander.

Discipline. “Training that corrects, molds, or strengthens an employee in the interests of achieving departmental and company goals.”

Dockmaster. This individual supervises the loading dock/shipping and receiving areas, including all loading and unloading operations.

Doorman. “An individual hired to provide courtesy and security services at a residential building or hotel. They are particularly common in urban luxury highrises [and major hotels]. At a residential building, a doorman is responsible for opening doors and screening visitors and deliveries. He [or she] will often provide other courtesy services such as signing for packages, carrying luggage between the elevator and the street, or hailing taxis for residents and guests.” At hotels a doorman provides a wide variety of guest services.

Escalatable costs. Costs a building incurs that may be charged proportionately to tenants and residents based on lease provisions. Costs associated with the security operation are typically escalatable because they are part of the building’s operating expenses.

Ethics. “A system or set of moral principles ... the rules of conduct recognized in respect to a particular class of human actions or governing a particular group.”

Fire safety director. Establishes, implements, and maintains the building emergency management plan. In some buildings the director of security/director of loss prevention and the fire safety director are the same persons. Sometimes known as the life safety director, life safety manager, building evacuation controller, or the emergency coordinator.

Freight/service elevator operator. Operates the freight/service elevator and screens all elevator users for authorization to travel to various floors of the building.

General ledger. “A formal record of all the financial transactions of a business.”

In-house security. See proprietary security.
Job description. “A written statement of what a jobholder does, how it is done, and why it is done. It typically portrays job content, environment, and conditions of employment.”

Job specification. “States the minimum acceptable qualifications an incumbent must possess to perform a given job successfully. It identifies the knowledge, skills, and abilities needed to do the job effectively.”

Key Performance Indicators. “Key Performance Indicators, also known as KPI or Key Success Indicators (KSI), help an organization define and measure progress toward organizational goals. Key Performance Indicators are quantifiable measurements, agreed to beforehand, that reflect the critical success factors of an organization.”

Liability insurance. “That form of insurance which indemnifies against liability on account of injuries to the person or property of another.”

Lobby director, lobby ambassador, and lobby officer. Assigned to lobby areas to control access to the building, provide information to building users and visitors, and perform other duties as specified by the facility. Sometimes known as a doorman.

Metrics. “A set of measurements that quantify results. Performance metrics quantify the unit’s performance. Project metrics tell you whether the project is meeting its goals. Business metrics define the business’ progress in measurable terms.”

Nonescalatable costs. Costs the building itself incurs that cannot be charged proportionately to tenants and residents based on lease provisions. For example, costs associated with the building parking operation may be nonescalatable if parking operations are a separate profit center.

Outsourcing. Contracting with outside firms to provide resources or services.

Patrol officer, parking patrol, and rover. Patrol various parts of the building and parking areas and perform other duties as specified by the facility (patrols may be on foot or using a motor vehicle, an electric cart, a bicycle, a tricycle, or a personal transporter).

Policy. “A general statement of a principle according to which an organization performs business functions.”

Post orders. Detailed documented procedures for carrying out security policies and routinely performing duties. Also known as security instructions and standard operating procedures.

Procedure. “Detailed instructions for implementing security policies; often presented as forms or as lists of steps to be taken.”
Proprietary security. “Any organization, or department of that organization, that provides full time security officers solely for itself. Staff employed directly by the facility owner or operator.” Sometimes called in-house security.

Retention rate. The average time period for which staff have been employed.

Security function. The security-related tasks performed in a facility.

Security officer. Performs security and fire life safety functions as determined by the building operation. Also known as a security guard.

Shift supervisor. Assigned to the various shifts—usually designated as day, swing or mid, and graveyard; or perhaps first, second, and third. Oversees and coordinates the activities of security staff assigned to their shift. Also known as watch commander.

Span of control. “Addresses how many subordinates a manager can efficiently and effectively direct.”

Supervise. “To watch over and direct (a process, work, workers).”

Train. “To give the discipline and instruction, drill, practice, designed to impart proficiency or efficiency.”

Training. “The formal procedure which a company utilizes to facilitate learning so that the resultant behavior contributes to the attainment of the company’s goals.”

Training officer. Particularly in larger projects, trains and tests all building security staff in their duties and responsibilities.

Turnover rate. The number of terminations for performance issues and voluntary resignations over a period divided by the total number of staff at the commencement of the period.

Watch commander. Assigned to the various shifts—usually designated as day, swing or mid, and graveyard; or perhaps first, second, and third. Oversees and coordinates the activities of security staff assigned to their shift. Also known as shift supervisor.

Worker’s compensation insurance. “Basic insurance [that] provides for medical costs, lost wages, and rehabilitation of workers injured on the job. There are also death benefits available.”

Additional Reading


---

48Ibid.


51Ibid.


Investigations

Owners and managers of office buildings, hotels, residential and apartment buildings, and mixed-use buildings may require various types of investigations pertaining to security and fire life safety matters. These may include analysis of specific events or conditions; examination of complaints about a particular policy, procedure, or person; investigation of a crime, suspected crime, or some other infraction (criminal or civil actions); and physical or electronic surveillance of someone or something. This chapter provides an introduction to investigations, interviewing techniques, and guidelines for using a private investigator. It does not address background investigations—preemployment histories of job candidates; financial and lifestyle inquiries of present employees; or in-depth fire and explosion investigations. For an in-depth study of investigations, several books are listed as additional reading at the end of this chapter.

What Is an Investigation?

An investigation is an objective, fact-finding, systematic inquiry into particular incidents, conditions, subjects, or behavior with a specific, predetermined purpose in mind.

According to Dempsey, “an investigation is the systematic and thorough examination and inquiry into something or someone (the collection of facts or information) and the recording of this examination or inquiry in a report.”

According to ASIS International, an investigation “is the logical collection of information through inquiry and examination for the purpose of developing evidence leading to problem resolution.”

A fact is an event that has actually occurred or is something known to be true. The inquiry not only involves gathering relevant information, but it also involves making assumptions and logical conclusions based on that evidence.

Evidence is anything that tends to prove a fact or support a conclusion. For most investigative purposes there are three kinds of evidence:

1. Physical evidence: objects, materials, documents
2. Stated evidence: what people such as victims, witnesses, suspects, and technical experts say
3. Circumstantial evidence: facts that lead to a logical or at least a likely conclusion

---

Private Sector and Public Law Enforcement Investigations

The focus of an investigation varies depending on whether it is conducted within the private sector or by a public agency. The primary objective of an investigation by public law enforcement is to serve the best interests of society by identifying and prosecuting offenders, whereas in the private sector the primary objective is to serve the best interests of the organization concerned. “It is interesting to note that what serves the best interests of society may not necessarily serve the best interests of the organization, and vice versa. For example, the society’s interests are protected when an embezzler is prosecuted and sentenced to prison. There are occasions, however, when the embezzler, having banked all his thefts, would be happy to return the stolen funds in order to avoid prosecution. Such an agreement would be unacceptable in the public sector. A seasoned private sector investigator, on the other hand, is not primarily concerned with prosecution and sentencing. Recovery of the loss might be a more important achievement, better serving the interests of the private organization.”

Other factors that influence whether an investigation is carried out in the private or public sector are the nature of the crime and the resources available to conduct the investigation. “Although the crime is of interest to law enforcement (and hence a matter for police investigation), there may be considerable preliminary effort required even to establish the existence of a crime. The police, generally overworked in criminal investigations, will not undertake preliminary inquiries in most situations unless there is a clear threat to public order or the general welfare.”

Rights of Public and Private Investigators

The authority and power of a public investigator is considerable, whereas the authority of a private investigator is limited to that of a private citizen. As a private citizen, the private investigator has no right to detain people against their will for questioning. The authority to conduct a private investigation and request cooperation from tenants, residents, guests, and visitors of a building comes from the rights of a building owner or manager and tenants, residents, or guests themselves within their own areas to maintain order on their property. “Law enforcement and its companion, the criminal justice system, have at their disposal mechanisms and tools unheard of in the private sector.”

“Whatever the capacity in which [an] investigator functions (public or private), it is important that the investigator be informed regarding all relevant legal restrictions, requirements, obligations, standards, and duties. Failure to do so could jeopardize the reliability of any investigation and could subject the investigator to civil liability or criminal prosecution.”

---

Nature of Investigations

Building owners and managers, tenants, residents, guests, security staff, licensed private investigators, public law enforcement or the fire department, and various other municipal, state, and federal agencies may carry out investigations in buildings. These investigations may be informal or formal in nature.

Informal Investigation

An informal or casual investigation involves something unusual or important being observed and then questions being asked or further observations made regarding the matter. For example, a member of building security staff, while patrolling a parking garage that has recently experienced thefts from several vehicles, encounters a person attempting to unlock an expensive automobile using a metal coat hanger. On questioning, it is discovered that the individual is in fact the owner of the vehicle who has locked his keys inside.

Formal Investigation

“A formal investigation may be conducted in response to a major incident or threat, or in response to a complaint. It is more organized than the casual investigation and proceeds through fairly well-defined stages.” For example, an incident that warranted such an investigation involved a fire that occurred after normal business hours in the office of a building tenant. Analysis by a fire department arson investigator revealed that the fire was started by tobacco embers from a smoking pipe discarded into a wastepaper receptacle underneath a desk in the burned-out office. A check of the building’s after-hours access register revealed that the tenant whose office was involved had signed out of the building 20 minutes before the fire command center received a fire sprinkler alarm for the floor in question. A subsequent interview of the tenant by an insurance investigator revealed that the night of the fire, the tenant did in fact clean out a pipe into the trash bin minutes before leaving the building. Another example of a formal investigation involved the following:

Several occupants from one tenant complained that over the past two months business items such as calculators, laptop and notebook computers, and personal belongings (cash, small mementos, and valuable pens) had been stolen from their offices. Building management, in conjunction with the tenant office manager, arranged for a covert surveillance camera to be placed in one of the areas where the thefts had occurred. This camera was connected to a video recorder. The recording from the third day of surveillance showed a tenant employee who walked into the office at 7 p.m., after most workers had left, and proceeded to search through desk drawers, place petty cash and an unsecured laptop in a briefcase, and leave the area. The next day, the tenant’s human resources manager conducted an interview with the employee, a trusted worker who had been with the company for 10 years. Under questioning, the employee admitted to the offenses and subsequently resigned.

Methods of Investigations

According to Eugene F. Ferraro in Investigations in the Workplace, there are six basic methods for conducting workplace investigations,
a. Physical surveillance

Physical surveillance is nothing more than watching people, places and things. Physical surveillance only requires two things: something to watch, and someone to watch it. As such, physical surveillance is relatively inexpensive and easy to use. Those who have conducted surveillance know that as simple as it is, it requires skill and patience. Not everyone is capable of surveillance or doing it properly. In some instances it requires sitting patiently in closed quarters, such as an automobile or van. In other instances it requires following the subject as he drives about. This form of physical surveillance is called moving surveillance and requires even greater skill.

Physical surveillance however has its limitations. Because it is not interactive, that is, the observer has no interaction or communication with whom he is observing, the evidence physical surveillance produces is typically only corroborative. That is, it only supports or corroborates other evidence.

b. Electronic surveillance

Electronic surveillance is similar to physical surveillance in that it too is nothing more than watching people places and things. However, unlike physical surveillance, electronic surveillance employs the use of electronic technology in order to improve the results. It too is relatively inexpensive and easy to use. Electronic surveillance can also be used in places and circumstances [where] simple physical surveillance cannot. Because electronic surveillance uses technology such as video, covert cameras and personal computer monitoring software it can be used when and where physical surveillance is not possible. However, therein lies the rub. Because electronic surveillance is possible in so many circumstances, users of it must be careful not to deploy it where its use might constitute an invasion of privacy.

Electronic surveillance is also not interactive. Like physical surveillance it has no interaction or communication with [those] whom it is observing or monitoring. As such, the evidence it produces is typically only corroborative as well.

c. Research and internal audit

The third method of investigation is the combination research and audit. For the purposes of this work, we shall define research as that investigative activity involving the collection of information from public sources. Public records often afford the workplace investigator a huge source of information and, depending on the type of matter under investigation, possibly the very clues that may make his case.

On the other hand, the internal audit method is reserved for the examination of nonpublic records, such as those in the possession of the employer-victim. Such records include attendance, productivity, and financial records, and even prior investigations. The use of such data is manifold in many workplace investigations.

d. Forensic analysis

Forensic analysis is the fourth method of investigation. It includes all manners of investigation that employ science or scientific method[s]. In this category are bodily fluid analysis, chemical and substance analysis, fingerprint examination and comparison, computer forensics, various deception detection methods, and forensic document examination.

e. Undercover

Corporate undercover investigation is one of the most powerful methods of investigation. "By definition, corporate undercover investigation is nothing more than the surreptitious placement of a properly trained and skilled investigator, posing as an employee, into an unsuspecting workforce for the purpose of gathering information." \(^9\) Undercover is one of only two forms of investigation that are interactive. That is, it permits the investigator to interact and communicate with those he is investigating. However,

undercover is immensely complex and is fraught with challenges. When conducted improperly, it can create unfathomable liabilities for both the employer-client and the investigator.

Undercover investigations are also time consuming and expensive. The typical investigation might take three to six months and cost upwards of $100,000. Because of the cost and liability associated with undercover, I tell my clients it should be used only as the option of last resort [a]fter all other alternatives and solutions have been thoroughly contemplated.

f. Interviews and interrogation

The sixth and final method of investigation is the systematic collection of information via interviews and interrogation. Unfortunately these terms mean different things to different people. The term interview seems less harsh than interrogation to most people. It describes a process that is less formal, less structured. But Merriam-Webster® defines these terms similarly, distinguishing interrogation as a process in which one “questions formally and systematically.” But in actuality, the word interrogation is rarely used to describe a formal and systematic interview. Instead, when one uses the word interrogation it seems to mean so much more. The thought of interrogation conjures up images of an offensive and coercive interview during which the subject is harshly questioned under a bright light. It’s stigmatized, carrying with it the inference or suggestion of coercion, intimidation and trickery. Some even consider an interrogation to be unlawful. As such, I rarely use the word to describe my interviews....

Interviews conducted during workplace investigations fall into two categories. The less formal of the two is called an administrative interview. It includes interviews of witnesses, by-standers and others not or likely not capable of the offense or matter under investigation. Investigative interviews, on the other hand, are reserved for those who we have very convincing reason to believe committed the offense or had direct involvement in it. Both forms of interviews are highly structured, but neither is confrontational or accusatory. Largely what distinguishes the two is the intended outcome. During administrative interviews we are simply looking for information. We are attempting to learn, gain insight and collect information. During investigative interviews, first and foremost, we are seeking an admission. An admission is not a confession. A confession is a statement that includes an admission to all of the elements of the crime. In workplace investigations, confessions are not necessary. In order to discipline an offending employee in most instances, the employer needs only to prove the employee in question committed the offense. The employer does not need to prove or demonstrate things such as means, motive, or intent. Those elements of the offense are inconsequential and have no bearing on the employer's determination of guilt or culpability or the right to impose discipline. Armed with a properly obtained admission, an employer needs nothing more to take disciplinary or corrective action against the offender. The same is not the case for criminal prosecution. Employers tend to over investigate. Many of them believe they must prove their case beyond a reasonable doubt. This extraordinarily high standard of proof is reserved only for criminal prosecution. In pursuing it, the employer expends more time and resources than necessary.

Like undercover, interviews are also interactive. They afford the investigator the opportunity to exchange information with the subject. Specifically, interviews afford the investigator the opportunity to determine the who, what, where, when, how and why from the very person who was there. It provides the investigator the unique opportunity to peek into the mind of the offender. This benefit combined with the opportunity to obtain an admission, make interviews the most powerful [form] of investigation for those conducting workplace investigations.10

Interviewing Techniques

“The most common way to get information and gather evidence, or at least identify it, is through people. Any time someone is spoken to for these purposes, an interview is conducted. Like the investigation itself, it can be casual or formal.”11 The reason for conducting an interview is to obtain information or evidence relevant to the investigation.


The interviewing techniques in the following sections are taken (with minor modifications) from an article by R. Lorne Brennan in the Protection Officer Training Manual.

Planning the Interview

It is important for the interviewer to go into an interview with a game plan in mind and with all available facts ready at hand. The success or failure of an interview depends on many factors, some beyond the control of the interviewer. The more factors that can be controlled by the interviewer, the greater the chances are for a successful interview.

[One important factor to consider is where the interview is to be conducted. It needs to be in a location where there is privacy, where there will be no unnecessary interruptions, and where the subject of the interview will feel relatively comfortable.]

The first approach to the subject is very important. Many people will be emotionally upset, angry, hostile, physically injured, and so on. It may be necessary to tend to the subject’s needs first before attempting to conduct a meaningful interview. Try to calm the subject, make him or her more comfortable, and enlist his or her active cooperation. Do not be rushed into an interview by the subject. Take your time, obtain all the facts, and get as much background information as possible before taking any action.

At times this approach will upset the subject, who feels that you should be taking swift action on his or her behalf; however, it is important to remember you are in charge and you are responsible for actions you take.

Make sure you have all the information before committing yourself to a course of action.

Conducting the Interview

Getting Acquainted

Your greeting should be cordial and sincere. Identify yourself, and if you are not in uniform, produce your identification. Your initial approach can be formal or informal, depending on the circumstances.

Attempt to set the subject at ease by entering into a general conversation with him or her before getting to the matter at hand. People like to talk about themselves and their interests and this is a useful tool in obtaining information about your subject and locating a common ground for communication. At this stage, allow the subject to become accustomed to your presence and to the surroundings by setting the pace.

Developing Rapport

Your immediate objective is to establish common ground on which you can communicate with the subject. By following the preliminaries, you should have a good idea of what the subject’s educational background is and at what level it is best to talk with him or her. If you are dealing with a laborer, do not speak down to him or her, or use terminology and words that he or she is not accustomed to hearing.
By the same token, you would not speak to an executive as you would a laborer. Find common ground and speak to the subject at his or her level. By finding areas of common interest, such as sports or hobbies, you can establish a rapport with the subject that will lead to easier communication.

In developing a rapport with another person, you must be able to put aside your personal feelings, respect the subject as a person and show your understanding of the subject and the circumstances that have brought you together. If you are unable to establish a rapport with the subject, an unbridgeable gap will be created that may make further communication difficult, if not impossible.

Motivating the Subject
Most people you interview will be in a strange and stressed situation that makes them uncomfortable. It will be necessary for you to remove any fears they may have. Many people are afraid of “authority” as shown by a uniform; they also are afraid of appearing as witnesses, incriminating themselves or others, or may simply be unsure of what they are to do.

If you have developed a rapport with the subject, it will help to convince the subject of the need to tell the truth and to enlist his or her active cooperation.

Keeping the Subject Talking
Once rapport has been established and the subject is motivated, turn the conversation toward the topic you wish to discuss. Allow the subject to give a complete account of his or her involvement without interruptions, but be alert for inconsistencies or omissions.

At times, you may have to interrupt to guide the subject back in the direction you wish the conversation to go. You must control the conversation so that the subject keeps talking until you have all the information you require.

Listening to “What Is Said” and “How It Is Said”
The interviewer must not only induce the subject to freely relate information she or he may possess, but must also evaluate the person and the conversation. In many instances, it is not what the subject says that is important, but the manner in which she or he says it or what a subject does not say.

The interviewer must be constantly alert for signals that indicate she or he is telling the truth, lying, or merely withholding information. Your interviewing abilities can be advanced considerably by learning how to interpret body language.

Repeat the Process
In most instances, the content of an incident will be covered in more than one conversation. The subject will be asked to repeat his or her story again to properly fill in gaps and correct previous statements. Again, it is important not to interrupt the subject during the initial stages and to allow the subject to recount his or her version in full.
After the initial story has been told, the interviewer may then ask the subject to repeat it, this time taking notes and stopping the subject from time to time to get the “full” story “straight.” Most people will never include all the details in the first attempt because they usually blurt out the information in rapid succession. After the initial telling, they will relax a bit, become more specific, and provide greater detail.

Obstacles to Conversation

Specific Questions

By asking specific questions, the interviewer diverts and limits the interview rather than letting the subject give a narrative of the whole or part of the story. Direct questions may also lead the subject into a false line of thinking as to what you consider to be important areas of the story; as a result, the subject may omit some details in an effort to supply the information he or she thinks you consider important.

Direct questions do have a place in an interview, but they should not be asked until the subject has given a complete narration. Direct questions can then be used to clear up various areas within the narrative. If the subject hits a block and stops talking, a direct question can be used to lead him or her back into the conversation.

Yes/No Questions

For the interviewer to obtain full and detailed facts, the subject must respond with an explanation detailing the events. If a question is asked that only requires a yes or no answer, the subject will normally respond with a yes or no, and information that may have been gained will be lost. By avoiding yes/no questions, you also reduce problems of subjects not understanding your question, agreeing or disagreeing based solely on what they perceive you want to hear, or what they want to tell you.

Leading Questions

Leading questions have the same effect as yes/no questions. They may cause the subject to give false or misleading information to the interviewer. This may be done either mistakenly or on purpose.

Rapid-Fire Questions

Rapid-fire questions may seem appropriate to the inexperienced investigator, but they only lead to confusion, emotional tenseness, and resistance to the rapport that may have been developed. They also stop the cooperative witness from completing his or her statement, thereby possibly losing information.

*A leading question is defined as “one which instructs witnesses how to answer or puts into his [or her] mouth words to be echoed back” (Publisher’s Editorial Staff. Black’s Law Dictionary. 6th ed. [Nolan JR and Nolan-Haley JM co-authors.] St. Paul, MN: West Publishing; 1990:889).*
Encouraging Conversation

Open-Ended Questions
By asking a series of questions in the early stages of an interview, you may be conditioning the subject to believe that if you want to know any information, he or she will be asked—that no spontaneous information is expected. On the other hand, asking relatively few questions leading into a conversation will give the subject the feeling that everything he or she tells has significance.

Typical open-ended questions are general queries: “Tell me what you saw,” “Can you tell me more about that?” or “What happened next?” These types of questions do not permit yes/no answers and allow for no misunderstanding of what the interviewer wants. The subject is forced to give a narrative to answer the question.

The Use of the Long Pause
Sometimes during an interview, the subject will stop talking and a silence will descend on the room. To the inexperienced interviewer, this can be unnerving and cause the interviewer to lose control of the interview and start talking. Pauses in conversation are normal and are never as long in duration as they seem to be. The subject is as ill at ease as you are during these silences, and the experienced interviewer will use them to advantage. Be patient and wait—many times the subject will resume talking and frequently will volunteer additional information just to break the silence.

Non-directive Approach
The non-directive approach is a technique that turns the subject’s statements into questions calling for more information. In using this method, simply repeat the subject’s last phrase, but with a rising inflection on the last word so that it becomes a question.

During such an interview, control your emotions, do not register surprise or anxiety, but merely restate the subject’s statement. The effect of this technique is that further information is drawn out without giving direction or restricting the thinking as in direct questioning.

Ending the Interview
No interview should be abruptly terminated with a curt dismissal of “Thank you,” “O.K.,” and so on. When it is apparent the interview is ending, close the conversation in a courteous and friendly manner. You may wish to summarize what has been said and ask the subject if there is anything else he or she wishes to add.

[At this point a written statement may be taken from the subject. “A properly obtained written statement, and written confessions are a specialized kind of written statement, follows from a properly conducted interview…. Assuming that the interview has identified all of the relevant information available from a particular witness regarding a particular subject, the investigator should commence the preparation of the written statement.”]^{12}

---

Let subjects know you appreciate what they have done, and that they have performed a valuable service. Thank subjects for their time and assistance. Treating subjects with concern and good manners will help ensure that, if you or another interviewer needs to speak with them in the future, they will be more cooperative and ready to assist instead of resist.  

Using a Private Investigator

Sources of Private Investigators

A private investigator may be identified from a number of sources. (These sources will vary from country to country.)

Local, county, and state law enforcement; municipal and county fire departments; and the local or state fire marshal’s office often will be amenable to providing information and possible lists of investigators and specialists.

In the security and fire life safety fields, there are a number of professional associations who may be able to provide referrals, such as ASIS International, the National Fire Protection Association, the Society of Fire Protection Engineers, the International Association of Arson Investigators, the International Association of Professional Security Consultants, the Association of Certified Fraud Examiners, the Society of Professional Investigators, the Association of Federal Investigators, the Council of International Investigators, the International Association of Credit Card Investigators, the International Association of Credit Card Investigators, the International Professional Security Association, the Security Institute, the Security Industry Association, and the Building Security Council. Finally, an investigator may be personally recommended by other security and life safety directors, risk managers, property or building managers, hotel managers, loss prevention departments, and insurance companies.

Selection Criteria

In selecting a private investigator, it is imperative to consider the following:

1. Request the investigator’s résumé and review his or her education, qualifications, licensing, and professional experience and affiliations. If the investigator is certified through a professional organization, or licensed through, for example, a state board, then the investigator’s certification or license can be verified. “A state board can also tell a prospective client how long a firm has been in business, whether it has branch offices, who the company’s principals are, whether complaints have been filed against the company, and the nature and disposition of those complaints.”

2. Ask how long the investigative company or individual has been in business.

“A firm should consider looking for agencies that have been in business for at

---


least two years. It is best to work with a stable agency because a company may need testimony later or require an additional follow-up investigation on the case.’’

3. Determine if the investigator has the necessary skills to carry out the particular investigation required. Request corporate references (business names, addresses, and telephone numbers) of clients for which similar investigations have been conducted. Call these businesses and ask detailed questions about “the quality of work performed by the investigator, timeliness, as well as confidentiality, results obtained, and the cost of the investigation. An organization should also ask references whether they received a full and detailed report of the agency’s investigative efforts.”

4. Request a certificate of insurance to verify that the investigator’s company has adequate liability insurance coverage, including errors and omissions. The certificate of insurance should be requested directly from the insurance carrier.

5. Have the investigator submit a written proposal detailing the purpose of the investigation; how it is to be carried out (depending on the circumstances, only a general statement may be possible); assurance that the investigation will be conducted in an ethical manner within the boundaries of local, state, or federal laws; how long it is expected to take (if known); what form the final written report will take; and how fees for the project will be handled. A total fixed cost may be proposed for the project, or hourly or daily costs may be quoted; in addition, transportation, accommodation, and administrative costs may be billed separately. A retainer fee might be stipulated on acceptance of the proposal or commencement of the investigation, with additional regular payments scheduled during the investigation.

6. When both parties have accepted the terms of the agreement, a written contract should be drawn up to include the proposal, incidental items such as a confidentiality agreement, and acknowledgment that the results of the investigation are the property of the client and the investigator. Once the contract is fully executed, the investigation should commence as outlined in the agreement, and all known facts should be revealed to the investigator.

Investigation Criteria

When a private investigator is hired to conduct an investigation, certain criteria should be clearly established before the investigation commences. They are as follows:

- What is the [objective] of the investigation and what is expected from the investigator?
- What is the scope of the investigation, and how far can the investigator go in conducting it? For example, are there certain individuals who are not to be approached? Are there certain areas that cannot be entered?

---

15 ibid.
16 ibid.

*Errors and omissions insurance is “insurance that indemnifies the insured for any loss sustained because of an error or oversight on his part” (Publisher’s Editorial Staff. Black’s Law Dictionary. 6th ed. [Nolan JR, Nolan-Haley JM, co-authors]. St. Paul, MN: West Publishing; 1990:803).
● What are the time or financial limits on the investigation?
● How frequently or under what circumstances should the investigator provide progress reports?
● Should the investigation necessitate calling in outside agencies, such as law enforcement, will the person(s) requesting the investigation be notified when this occurs?
● How will final investigative results be handled?

These considerations do not imply that the person(s) requesting the investigation is at liberty to manage the investigation. If a professional, well-trained, highly skilled, and trustworthy investigator has been selected, that individual will ensure the investigation is properly managed. However, as Hertig has warned, “If the investigative effort is not properly controlled, man-hours will be wasted, confidentiality may be compromised, and objectives will not be met.”17 There also is the possibility that court action may ensue if the investigation is not properly conducted within the law and according to ethical principles.

Summary

● Investigations are an invaluable tool in managing security and fire life safety programs.
● Investigations carried out by building owners and managers, security staff, or private investigators differ from those conducted by public law enforcement agencies.
● There are different types of investigations and methods for conducting them.
● In using a private investigator, there are basic criteria to consider.

Key Terms

Errors and omissions insurance. “Insurance that indemnifies the insured for any loss sustained because of an error or oversight on his part.”18
Evidence. Anything that tends to prove a fact or support a conclusion.
Fact. An event that has actually occurred or is something known to be true.
Investigation. An objective, fact-finding, systematic inquiry into particular incidents, conditions, subjects, or behavior with a specific, predetermined purpose in mind. “The systematic and thorough examination and inquiry into something or someone (the collection of facts or information) and the recording of this examination or inquiry in a report.”19

Additional Reading

Criminal and Private Security Investigations


Fire and Explosion Investigations

Office Buildings

An office building is a “structure designed for the conduct of business, generally divided into individual offices and offering space for rent or lease.”¹ The types of office buildings addressed in this chapter are those that have one or more tenants conducting various types of commercial business and may include public service offices (however, they do not comprise tenants such as courthouses and police holding cells). Depending on the country, state, or city in which such buildings are situated, they have to be operated according to specific industry-related guidelines and standards, many of which are government mandated.

Office buildings usually “include parking facilities which may be open, enclosed, above- or below-ground, and often directly beneath or adjacent to the [office building] itself. These arrangements may require special types of fire protection, and the building codes may require fire separations.”²

To systematically examine the security and fire life safety of office buildings, this chapter addresses the following areas: occupancy characteristics; assets, threats, vulnerabilities, and countermeasures; security programs; and emergency planning.

Occupancy Characteristics

“The types of building tenancy and the pattern of use are important factors to consider when we plan and carry out a security [and fire life safety] program. A building can be (1) single-tenant/single-use, (2) single-tenant/multiple-use, (3) multiple-tenant/single-use, or (4) multiple-tenant/multiple-use.”³

- A **single-tenant/single-use** building is occupied by one particular tenant and is used solely for one type of business—for example, a bank building where the business of that bank alone is conducted.
- A **single-tenant/multiple-use** building, however, is occupied by one particular tenant who uses the building not only for one type of business but also for other purposes. An example would be a bank building that has parking facilities, restaurants, a cafeteria, or retail outlets open to the public.
- A **multiple-tenant/single-use** building is occupied by more than one tenant, each of whom uses the building to conduct a similar type of business—for example, a medical office building where tenants conduct medical business.

---

¹ *Glossary of Real Estate Management Terms*. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:120.
A multiple-tenant/multiple-use building is occupied by more than one tenant, each of whom conducts business not necessarily related to the other businesses. An example would be a commercial office building that has law firms, public utilities or agencies, management consultants, financial institutions, retail outlets, and public restaurants.

Office buildings usually have a higher concentration of occupants during normal business hours (i.e., Monday to Friday, during daytime hours), when the building or property management staff tend to be on duty. After hours (i.e., Monday to Friday, early evening until the next morning, and on weekends and holidays), most buildings (except major facilities, including mega high-rise buildings) have fewer engineers (if any), security personnel, elevator technicians, and other support staff on duty; however, there is usually a higher concentration of janitorial and cleaning staff from early evening (Monday to Friday) until the early hours of the next morning, because cleaning operations are generally focused during the hours when most tenants are not present.

Generally speaking, office buildings are managed by one group; this will consist of a building or property manager and administrative staff, plus support staff such as in-house or contract engineers, security personnel, janitors and cleaners, elevator technicians, landscaping staff, and other vendors associated with building operations. The actual numbers of staff will vary according to the size of the building, the complexity of its operations, and the security needs of each individual facility.

Building or property management staff tends to be on duty during normal business hours (i.e., Monday to Friday, during daytime hours). After hours, such staff can be contacted using various means of communication that includes telephones, pagers, e-mail, and text messaging. Some buildings designate an on-duty manager to handle after-hours calls relating to building operations.

Assets, Threats, Vulnerabilities, and Countermeasures

A risk assessment (as detailed in Chapter 4) is an important tool for developing an appropriate security and fire life safety program for an office building. A “risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple low cost[, mitigation measures [countermeasures], but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with identified vulnerability, allow prioritization of resources to implement mitigation measures.”

---

*The hypothetical multiple-tenant/multiple-use high-rise, Pacific Tower Plaza, earlier described in Chapter 4, is a 36-story building with a triple-level underbuilding parking garage, located in a major downtown financial district.

Key steps in the process involve examining the assets, the threats against the assets, the vulnerabilities of the assets, and the countermeasures or mitigation measures that can be used to address identified vulnerabilities of the assets (within the confines of risk management). These areas are now examined for office buildings.

Assets
Tangible assets in office buildings include the lives of tenants, visitors, contractors, vendors, and the office building staff; tenant property; and the building itself, its fittings, and its equipment. Building equipment includes electrical, water, gas, mechanical, heating, ventilating, air-conditioning, lighting, elevator, escalator, communication, security, and life safety systems. In addition, there are other types of assets that may include telephones, computers, printers, typewriters, fax machines, photocopiers, audio-visual equipment, and general-use items (coffee machines, vending machines, refrigerators, microwaves, ovens, and furniture) and sometimes antiques and works of art, cash and negotiable instruments, and vehicles parked in a building’s parking garage. In addition, there may be assets in cafeterias, restaurants, retail shops, newsstands, copy/print services, and other common area facilities.

Intangible assets include the livelihood of building tenants, visitors, contractors, vendors, and office building staff; intellectual property and information stored in paper files, reference books, microfilm, and within computer systems and peripherals; and the reputation and status of the office building and its tenants.

Threats
The types of security and fire life safety threats to office building assets are outlined in Chapter 3. Briefly, they include the following:

- Security threats to people: assault, assault and battery, kidnapping, manslaughter, mayhem, murder, robbery, sex offenses (including rape, sexual harassment, and lewd behavior), and stalking.
- Security threats to property and information: aberrant behavior, arson, burglary, cyberattack, disorderly conduct, espionage, larceny, sabotage, theft, trespass, and vandalism. In addition, there may be the disruption of building utilities such as water, electrical power, natural gas, sewer, HVAC (heating, ventilation, and air-conditioning), telecommunications, security, and life safety systems. Some security threats may involve terrorism.
- Security threats to people and property: bombs, chemical and biological weapons, riots and civil disturbances, fires and fire alarms, hazardous materials, natural disasters, and nuclear attack.
- Life safety threats: aircraft collisions; bombs and bomb threats; daredevils, protesters, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstraions, and civil disorder; medical emergencies; natural disasters (earthquakes, tsunamis, volcanoes, heat waves, storms, and floods and landslides); contractible diseases (pandemic influenza, severe acute respiratory syndrome, and tuberculosis); power failures; slip-and-falls; stalking and workplace violence; traffic accidents; and water leaks.
Notable Incidents
Some notable incidents⁵ that have occurred in high-rise office buildings are shown in Table 9–1.

Fire Risk in Office Buildings
Fire is a constant risk in high-rise office buildings. In discussing fire risk,† it is helpful to analyze fire incident data‡ for the four property classes—office buildings, hotels and motels,§ apartment buildings, and hospitals (and other facilities that care for the sick)—that account for the majority of high-rise building fires.⁸ Even though this data pertains only to the United States, it is worth considering because it includes the types of commercial buildings that are addressed in this book (namely, office, hotel, residential and apartment, and mixed-use buildings).

A study by Dr. John Hall, Jr., of the National Fire Protection Association’s (NFPA) Fire Analysis and Research Division, using statistics from the U.S. Fire Administration’s National Fire Incident Reporting System (NFIRS), stated that from 1987 to 1991, office buildings, hotels and motels, apartment buildings, and facilities that care for the sick averaged 13,800 high-rise building fires per year and associated annual losses of 74 civilian deaths, nearly 720 civilian injuries, and $79 million in direct property damage. However, “most high-rise building fires and associated losses occur in apartment buildings.”⁷ Hall added that for this period:

- Only a small share of high-rise building fires spread beyond the room of origin, let alone the floor of origin.
- In high-rise buildings [office buildings and hotels and motels], electrical distribution system fires rank first in causes of fire-related property damage.⁸

---

⁵Dates and some details of bombing incidents involving Al Qaeda versus United States and Allies, 1995-2003, was obtained from The Chicago Project on Suicide Terrorism, Robert Pape, Professor of Political Science, The University of Chicago. <http://jtac.uchicago.edu/conferences/05/resources/pape_formatted%20for%20DTRA.pdf>; May 17, 2008.


Other information was obtained from various agencies and news sources, many of which are identified in the summaries of a number of the incidents in Chapter 3. However, at times, reports of casualties were conflicting. Therefore, the number of persons killed and injured could not always be definitively determined.


‡“Tracking of the fire experience in [U.S.] high-rise buildings, however, has been less than systematic because the nationally representative fire incident data bases did not originally include reporting of height of structure. Reasonably good reporting began with 1985 fires…. NFPA and other analysts have long used lists of particularly memorable incidents to study the high-rise fire problem, but these and other available special data bases are heavily weighed towards larger and more severe incidents.” ibid., p. 1.

§Beaudry MH. The term “motel” is a general designation for lodging establishments that specialize in attracting the motoring public by offering parking accommodations. The distinctions between hotels and motels are gradually disappearing, however. Contemporary Lodging Security. Newton, MA: Butterworth-Heinemann; 1996: ix.


⁸ibid., p. 53.
<table>
<thead>
<tr>
<th>Date</th>
<th>Building</th>
<th>Incident</th>
<th>Persons Killed/ Injured</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 1, 1974</td>
<td>Joelma Building, São Paulo, Brazil</td>
<td>Fire</td>
<td>179 killed, 300 injured (greatest loss of life in an office building fire)</td>
</tr>
<tr>
<td>May 4, 1988</td>
<td>First Interstate Bank Building, Los Angeles, California</td>
<td>Fire</td>
<td>1 building engineer killed, 40 injured</td>
</tr>
<tr>
<td>June 30, 1989</td>
<td>Peachtree 25th Building, Atlanta, Georgia</td>
<td>Fire</td>
<td>5 killed, 26 injured (including 6 firefighters)</td>
</tr>
<tr>
<td>February 23, 1991</td>
<td>One Meridian Plaza, Philadelphia, Pennsylvania</td>
<td>Fire</td>
<td>3 firefighters killed</td>
</tr>
<tr>
<td>February 26, 1993</td>
<td>New York World Trade Center, New York</td>
<td>Truck bomb</td>
<td>6 killed, 1042 injured</td>
</tr>
<tr>
<td>April 24, 1993</td>
<td>Bishopsgate area of London’s financial center, U.K.</td>
<td>Truck bomb</td>
<td>1 killed, 44 injured</td>
</tr>
<tr>
<td>July 1, 1993</td>
<td>101 California, San Francisco, California</td>
<td>Shooting</td>
<td>8 killed, 6 injured, gunman killed himself</td>
</tr>
<tr>
<td>April 19, 1995</td>
<td>Alfred P. Murrah Building, Oklahoma City, Oklahoma</td>
<td>Truck bomb</td>
<td>167 killed, 782 injured</td>
</tr>
<tr>
<td>November 20, 1996</td>
<td>Garley Office Building, Hong Kong</td>
<td>Fire</td>
<td>40 killed (incl. 1 firefighter), 81 injured</td>
</tr>
<tr>
<td>July 29, 1999</td>
<td>Several buildings, Atlanta, Georgia</td>
<td>Shooting</td>
<td>9 killed, 13 injured, gunman shot himself</td>
</tr>
<tr>
<td>September 11, 2001</td>
<td>New York World Trade Center, New York</td>
<td>Aircraft collision</td>
<td>2749 killed, thousands injured</td>
</tr>
<tr>
<td>March 11, 2002</td>
<td>Rembrandt Tower, Amsterdam, Holland</td>
<td>Hostage</td>
<td>18 held hostage (none hurt), gunman shot himself</td>
</tr>
<tr>
<td>October 17, 2003</td>
<td>69 West Washington, Chicago, Illinois</td>
<td>Fire</td>
<td>6 killed</td>
</tr>
<tr>
<td>November 20, 2003</td>
<td>HSBC Bank AS and British Embassy, Istanbul, Turkey</td>
<td>2 truck bombs</td>
<td>30 killed, 400 wounded</td>
</tr>
<tr>
<td>October 15, 2004</td>
<td>Parque Central, Caracas, Venezuela</td>
<td>Fire</td>
<td>Building unoccupied apart from several security staff who evacuated safely</td>
</tr>
<tr>
<td>February 12, 2005</td>
<td>Windsor Building, Madrid, Spain</td>
<td>Fire</td>
<td>Building unoccupied apart from several security staff, was demolished due to extensive fire damage</td>
</tr>
<tr>
<td>December 8, 2006</td>
<td>Citigroup Center, Chicago, Illinois</td>
<td>Shooting</td>
<td>3 occupants killed, gunman shot himself</td>
</tr>
</tbody>
</table>
The most recent published study by Hall shows that “in 2002, high-rise buildings in these four property classes combined had 7,300 reported structure fires and associated losses of 15 civilian deaths, 300 civilian injuries, and $26 million in direct property damage.” He concluded that “these statistics generally show a declining fire problem over the nearly two decades covered” and, similar to his previous findings, “most high-rise building fires and associated losses occur in apartment buildings.” However, Hall did caution that, due to a number of factors (one being lower participation in national fire incident reporting in recent years), “the patterns shown in data available so far should be given limited weight.”

Vulnerabilities
Weaknesses that can make an asset (in this case, an office building and its operations) susceptible to loss or damage will largely depend on the building itself and the nature of its operations. A vulnerability assessment is required to “evaluate the potential vulnerability of the critical assets against a broad range of identified threats/hazards.”

Countermeasures
Mitigation measures to counteract identified vulnerabilities of an asset to a threat may consist of security systems and equipment (see Chapter 5), fire life safety systems and equipment (see Chapter 6), security personnel (see Chapter 7), security policies and procedures (see the next section, “Security Programs”), and emergency management (see the later section, “Emergency Planning”). These countermeasures need to be looked at in terms of security design. “Security design involves the systematic integration of design, technology, and operation for the protection of three critical assets—people, information, and property.... The process of designing security into architecture is known as Crime Prevention Through Environmental Design (CPTED).” As mentioned previously, the key to selecting appropriate countermeasures for a particular facility is for a risk assessment to be conducted. (See Chapter 4.)

Because fire is a risk in high-rise buildings, the following is noted regarding their fire protection features (which are detailed in Chapter 6): office buildings that have properly designed, installed, operated, tested, and maintained automatic fire detection and suppression systems and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes and automatic smoke control systems to restrict the spread of smoke—do have the necessary early warning systems to quickly detect fires and warn occupants (including tenants

---

9 2002 is the most recent year for which data was available for this report.
10 ibid., p. 3.
11 ibid.
12 ibid., p. 4.
13 ibid., p. 3.
14 ibid., p. 4.
and visitors) of their presence, as well as the necessary automated sprinkler systems to quickly extinguish a fire in its early stages. One of the key issues here is the presence or absence of sprinklers.

In the study mentioned in the previous section on “Threats,” Hall commented on fire protection in high-rise buildings by stating that

> In several instances, the value of these fire protection features [i.e., automatic extinguishing systems (primarily sprinklers), fire detection equipment, and fire-resistive construction] may be seen clearly in a statistical analysis of 1994-1998 loss per fire averages, with and without the protection. For high-rise buildings, automatic extinguishing systems are associated with a reduction of at least 88% in the rate of deaths per 1,000 fires for each of the three property classes (excluding office buildings, which had no deaths recorded in NFIRS [National Fire Incident Reporting System] in high-rise buildings) and at least 44% in the average dollar loss per fire for each of the four property classes....

Automatic extinguishing systems and fire detection equipment and the compartmentation features associated with fire-resistive construction all contribute to fire protection by helping to keep fires small, with extinguishing and construction doing so directly and detection doing so by providing early warning that can lead to earlier manual suppression.18

### Security Programs

Security programs for office buildings and for individual tenants involve policies, rules and regulations, and procedures designed “to prevent unauthorized persons from entering, to prevent the unauthorized removal of property, and to prevent crime, violence, and other disruptive behavior.”19 Security’s overall purpose is to protect life and property.

### Building Access Control

There are many different people who may, at any one time, wish to enter an office building. They include building owners and management staff, building contractors (such as engineering, maintenance, security, janitorial, and parking personnel and elevator technicians), tenants (and the employees working for them), visitors, salespersons, tradespeople (including construction workers, electricians, plumbers, carpenters, gardeners, telecommunications repair persons, persons replenishing vending machines, and others who service equipment within the building), building inspectors, couriers, delivery persons, solicitors,18 sightseers, people who are lost, vagrants or homeless people, mentally disturbed individuals, vandals, suicidal persons, protestors, and daredevils. There may

---


*In this context, a solicitor is a person who approaches building occupants with the intent to sell something, to ask for business for a company, to request charitable contributions, or to obtain magazine subscriptions. This definition would include people who beg or panhandle for money or food.
also be others who try to enter a building—or an individual tenant space—with the sole aim of committing a crime.*

It is primarily the building owner and manager who determine the access control measures for this wide spectrum of persons. These measures aim to screen out unwanted persons or intruders and at the same time provide a minimum of inconvenience to legitimate building users. When a security program is designed, occupancy characteristics such as the type of building tenancy, its pattern of use, and the time and day (normal business hours or after hours, weekends, and holidays) need to be considered. “The dilemma that office buildings owners and managers face is to keep the building secure, while allowing entry to legitimate users and exit under emergency conditions. While authorized personnel should be allowed to come and go with relative ease, unauthorized individuals require restricted access.”

Varying degrees of access control can be achieved using security staff— in some office buildings they are known as security officers, security guards, or other titles that differ according to their respective duties and responsibilities—or nonuniformed receptionists and customer service staff, along with various other security measures.

As explained earlier in this chapter, an office building can be single-tenant/single-use, single-tenant/multiple-use, multiple-tenant/single-use, or multiple-tenant/multiple-use. A single-tenant/single-use building is much more conducive to strict access control of employees and members of the public: standard security rules and procedures can be communicated and enforced more easily with employees of one tenant only. “Access control may be tight and involve a badging system for regular employees and a careful monitoring of visitors through direct observation, or video displays and other devices.”

Implementation of strict access control for a multiple-tenant/multiple-use building, however, is more difficult because each tenant may have different expectations of the degree of security the building should have.**

*Such persons may include a “building or office creeper,” who may enter a building that does not have strict access control measures. For example, late in the afternoon, dressed in conservative business attire, the creeper might confidently enter through the main lobby and nonchalantly pass by building security staff. Taking an elevator to an upper floor, this “businessperson” enters a common area restroom and quietly sits in a cubicle until the tenants on the floor are about to close business for the day. He or she then exits the restroom and systematically walks the corridors checking doors to see if they have been secured. On finding one unlocked, the creeper enters the tenant space and proceeds through it looking for laptop computers, personal data assistants, mobile telephones, cash, checks, credit cards, and other items that can be easily placed in a jacket or a briefcase. On being challenged in one suite by building janitorial staff, a tenant business card (which moments before was lifted from an executive’s desk) is politely presented with the statement of gratitude, “I’m so glad to see that even janitorial staff in our building are so security conscious!” After 15 minutes of work, the creeper descends to the lobby in a passenger elevator and warmly waves to the security staff as he or she exits the building. The advent of mobile phones has made it possible for such persons to operate in pairs.

To deter this type of activity, tenants should ensure that all perimeter doors not supervised by staff be kept locked; employees should be instructed to not allow unknown persons to tailgate or piggyback into their offices, to challenge unknown persons encountered inside their offices (even if they are wearing a service uniform and look like a delivery person, janitor, or maintenance worker), and to not leave business and personal items unattended.

** Before the September 11, 2001, destruction of the New York World Trade Center, access controls in many multiple-tenant commercial office buildings were generally loose during normal business hours, Monday to Friday, and tightened up after hours. Since that incident, many buildings have implemented strict access controls 24 hours per day, 7 days per week (as detailed in Chapter 2).
Building access controls include vehicle access to parking lots, garages, and loading dock/shipping and receiving areas; pedestrian access to building lobbies, elevator lobbies, and passenger and freight/service elevators; and access routes to retail spaces, restaurants, promenades, mezzanines, atria, and maintenance areas. Measures for controlling access to these areas vary from site to site, depending on building management’s policy, but generally incorporate some or all of those described in the following sections.

Vehicle Access to Parking Lots or Garages
Access to parking lots or garages may be manual or automatic using a variety of methods that include the following:

1. Entry at will. There are no controls on the entry of vehicles (apart from possible vehicle height, weight, and width restrictions at the point of entry).
2. A vehicle detector embedded in the roadway, which automatically opens an entry gate or raises a gate arm.
3. A parking attendant, a valet, or a security person stationed either at the point of entry or at a remote location linked to the point of entry by an intercom or a closed-circuit television (CCTV) system and a key switch or a remote control device that opens an entry gate, raises a gate arm, or lowers a surface-mounted traffic barrier.
4. A ticket (imprinted with the date and time of entry) dispensed by a machine at the point of entry that when withdrawn from the control unit automatically opens an entry gate or raises a gate arm.
5. An electronic access card, an alphanumeric key pad, or a vehicle identification system such as a transponder that opens an entry gate, raises a gate arm, or lowers a surface-mounted traffic barrier.

When exiting a controlled-access parking lot or structure, the driver usually is required to submit to a similar procedure to that encountered on entry, make a monetary payment (sometimes using a pay-on-exit machine), or use a token. Many access control systems with entry and exit card readers incorporate an antipassback feature. This prevents an access card from being used again to authorize entry of a second vehicle before the card has been used to authorize exit of the first vehicle.

Vehicle Access to Loading Dock/Shipping and Receiving Areas
Vehicles entering loading dock/shipping and receiving areas may do so at will and park at whatever loading bays or docks are available, or they may be permitted to enter and be directed to park in certain areas by a loading dock attendant who will then supervise subsequent loading or unloading. (Some buildings keep loading dock doors and gates closed between delivery and pick up of items. Also, docks that are normally unattended may have an intercom or buzzer system, possibly in conjunction with CCTV, to allow drivers to remotely summon building staff for assistance.)

Some higher-security buildings require vehicles, particularly vans and trucks, and especially those that will proceed to underbuilding loading dock/shipping and receiving areas, to undergo an on-street visual inspection before being allowed to enter. (As a result of the events of September 11, 2001, some landmark high-risk office buildings deployed a mobile X-ray vehicle to screen such vehicles, including trucks, for explosives, prior to entry.)
For security purposes, the dock attendant normally will maintain a log or record of the vehicle license plate number, the driver’s name and company, the time in, and the time out. Depending on building policy, vehicle keys may remain in the vehicle or be given to the dock attendant for safekeeping and to permit moving the vehicle if necessary.

The activity of drivers and delivery persons usually will be confined to the loading dock/shipping and receiving areas, unless they need to proceed to tenant areas for deliveries or pickups of items. For this reason, rest areas, toilet facilities, and pay phones often are provided in these areas. If drivers and delivery persons enter the building, they are usually required to notify the dock attendant of the specific building area they will be visiting and the approximate duration of their stay. They may also be issued special identification badges and required to leave some form of personal identification (such as a driver’s license) with the attendant. (Since September 11, 2001, many office buildings strictly control drivers and delivery persons entering loading dock/shipping and receiving areas. Again, some landmark facilities, due to the perceived risk of dangerous or illegal items being brought into the loading dock area, have installed walk-through metal detectors and pallet-size X-ray machines and have utilized portable, hand-held explosives trace detectors or explosives-detection trained dogs.) (See also the “Dangerous or Illicit Items” section presented later in this chapter.)

**Pedestrian Access to Buildings**

Pedestrians entering office buildings during normal business hours may simply enter at will and proceed to whatever area they desire, or they may be asked to submit to some form of credentialing process before they are permitted to enter the facility and proceed to interior locations. The process in place may vary according to the time (either normal business hours or after hours) and the day (either standard working days or weekends and holidays) that the access is requested.

**Normal Business Hours**

During normal business hours, access control for some office buildings and their common areas is relaxed and may solely rely on a security officer or receptionist trained to observe both incoming and outgoing pedestrian traffic. Persons who do not appear to belong in the business environment may be challenged with a simple “May I help you?” Specific questions can then determine the particulars—for example, whether the person is a tenant, is visiting a tenant (if so, which one?), is delivering or picking up items (if so, to whom? from whom?), or is servicing or inspecting equipment in the building (if so, where? at whose request?). These questions not only help screen out intruders with no legitimate reason for entering but also assist persons who need directions.

For other buildings, access control is stricter, relying on a variety of methods such as electronic access cards (which are presented to readers at building entrance doors, at lobby kiosks, on elevator bank walls, or inside elevator cars) and optical turnstiles. For tighter security applications, access control may even involve biometric devices or a combination of technologies for identity management. The degree of access control imposed by building policy determines the percentage of unwanted persons successfully screened out. “The security program should be designed just tight enough to screen out as many intruders as it takes to reduce problems to the level that can be accepted. This

* A credential is something that entitles a person to certain rights or privileges.
means that a useful security program will rarely screen out all intruders."22 If all intruders were screened out, it may result in what could be considered by building management unacceptable delays or inconvenience to the legitimate occupants and visitors.

The screening of visitors may be facilitated by establishing separate visitor centers and using visitor management software to expedite entry. The former allows visitors to be moved to a separate staging area for processing. The latter is a password-protected, web-based management system that permits authorized users of the system to preregister visitors online before they arrive at a building. All relevant information about the visitor (such as name, company, person they will be visiting, time of visit, and any special instructions for handling the visitor) can be stored in a database and used to print out a visitor badge when the person is cleared for entry. This not only facilitates visitor handling but also records visitor traffic and could be used to track the attendance of vendors and contractors. Some systems even allow the visitor to self-register by scanning an identification document, such as a driver's license, through a verification machine.

Access control to building maintenance spaces—mechanical rooms and floors, air-conditioning rooms, telecommunications and utilities access points, elevator machine rooms, and janitorial closets—and areas under construction or renovation usually will be tight. Depending on building policy, persons accessing these areas may be logged in and out, required to wear special identification badges, given keys (although issuing keys to vendors or visitors can be a security risk) or an electronic access card to a particular area (if the card is not returned it can be immediately deactivated), or provided an escort. Some contractors servicing certain types of equipment in specific building areas may be permitted to install their own locking devices at access points leading to this equipment (see further comments in the “Key Points to Consider” section later in this chapter). Main electrical switchgear and power transformer rooms are usually deemed such a life safety risk that building personnel are not issued keys to these areas.

After Normal Business Hours

After normal business hours, access control to most office buildings and interior areas is usually strict. An obvious way to provide off-hours access to an office building would be to furnish keys to all building occupants or to those who need to enter the facility after hours. This approach, however, can have disastrous consequences proportional to the size of the building and the number of occupants. A heavy workload and costly expense can be created by lost keys, keys not returned by departing tenant employees, and the necessity of rekeying building entrances and reissuing keys to building key holders every time a key has gone astray. In addition, there may be the problem of the unauthorized duplication of keys. To avoid all these consequences, most office buildings never issue building access keys to tenants but rely on some way of verifying a person’s right to enter the building. This verification may involve the following procedures:

Visual Recognition

Building security staff or a receptionist may verify on sight a person’s right to enter. Several problems may result, however, from this form of verification. For example,

someone who closely resembles a person authorized to enter may be admitted in error. Also, particularly if the building is large with a high population, it will be difficult for security staff or the receptionist to recognize all persons authorized to enter. If there is a change or substitution of the security staff or receptionist, the new person will not be familiar with the persons authorized to enter. This may result in the questioning of authorized persons who normally are never challenged and subsequent complaints to building management. Finally, if the security staff is distracted by another duty, an unauthorized person may gain entry without being observed.

Authorization Documents
A document (a letter, a memorandum, or an e-mail) listing those authorized for after-hours access may be provided in advance to security staff at the building entrance. Persons requesting access will identify themselves to building security staff. Security will compare their name (which should be confirmed by a driver’s license or other photo identification) with the names listed in the document. In many buildings, tenants will provide management with a written request on their own stationery listing the names of the persons involved and the time after-hours access is permitted. Building security staff or the receptionist often will set up a file sorted alphabetically by tenant name, or by the last name of the person to be granted access, to minimize time spent searching for the appropriate authorization.

Building security staff must thoroughly check all documents authorizing access to ensure that the decision to grant access is valid. An unusual example illustrates the point. Building management of a major office building gave building security staff a memorandum to allow access of a pest control company to a specific tenant suite on a particular Friday night. The pest control company failed to appear on the night authorized but did arrive the following Monday evening. Building security staff did not thoroughly check the paperwork and permitted the pest control company to enter and carry out their work. The next business day, several of the tenant employees became ill from the lingering effects of the pest treatment. The reason for authorizing entry on Friday evening was to allow two days for any residual pesticide to dissipate. Permitting the work to occur on a Monday evening negated this precautionary safety measure.

Building Identification Cards, Passes, and Badges
A building identification card, a pass, or a badge is sometimes used to verify the bearer’s identity and privilege to enter after hours. The identification means should be numbered sequentially, stating the person’s name and the company’s name, and should contain the person’s signature, a color photograph, and in some instances an expiration date. It should be laminated for durability, and be tamper resistive (although this will not necessarily eliminate the potential for the plastic envelope being cut and the card, pass, or badge being modified and then relaminated). The development of laser technology to create holograms (three-dimensional images) may lead to their future use for building identification cards, passes, or badges.

The credential can be presented by the bearer to security staff for entry to the building or used to verify identification within the building. However, if the card, pass, or badge is not thoroughly checked for details, this form of access control soon loses its effectiveness. Also, it must be retrieved from holders whose employment is finished, or else it could be used after the person no longer has a legitimate reason for gaining access to the building.
Building Electronic Access Cards

Building electronic access cards can provide after-hours access by operating a building entry door. An intercom, a telephone, or a CCTV camera may also be situated at the point of entry. If there is a problem using the card, the person requesting access can use the intercom or telephone to communicate with onsite security staff or an offsite central monitoring station. If the person’s right of entry is confirmed, the staff can grant access in person or remotely.

Once a person is inside a building lobby, his or her progress may be controlled using a variety of methods. These include electronic access cards being presented to readers at lobby kiosks, on elevator bank walls or inside elevator cars, and to optical turnstiles; for higher security applications, the method may even involve biometric devices or a combination of technologies for identity management.

Building access cards can feature the same data, tamper-resistive protection, and lost-card notice as identification cards, passes, and badges. However, for security reasons managers of some buildings prefer to have no information displayed on the card apart from its sequential number and, if used with an insertion or swipe-type card reader, an arrow depicting the correct way to insert or swipe the card. Then if a card is lost, there are no identifying marks to indicate where it may be used. An advantage of an electronic access card is that if the cardholder’s employment ceases, a computer can be used to deactivate the card immediately, eliminating the need to retrieve the card itself.

Visitor Management Software

As previously explained, visitor management software is a password-protected, web-based management system that permits authorized users of the system to preregister visitors online before they arrive at a building. All relevant information about the visitor (such as name, company, person they will be visiting, time of visit, and any special instructions for handling the visitor) can be stored in a database and used to print out a visitor badge when the visitor is cleared for entry. Such a system not only facilitates visitor handling but also records visitor traffic. It also could be used to track the attendance

---

\*\*\*An access control system installed in passenger and freight/service elevator cars provides controlled access to building floors. Some systems can be programmed so that during certain time periods the elevator car will only respond to a particular floor if an authorized access card is used. The person will enter the elevator, insert, swipe, or bring the card into close proximity to the card reader, and select the desired floor by pressing the appropriate button on the floor selection panel. (Additionally, in high-traffic buildings that have elevator systems equipped with destination dispatch technology, access control systems may be incorporated with such technology. In the elevator lobby, the waiting passenger uses a touch screen or a keypad located on elevator bank walls or lobby kiosks to select the required destination floor and is also required to present a valid access card to a reader incorporated into the system; or a person uses an access card to pass through an optical turnstile that also controls access to the elevator banks. The elevator control system evaluates the data, dispatches an appropriate elevator car to the floor where the passenger is waiting, and directs the person to the appropriate car.)

\*\*\*The value of visitor badges decreases if the visitor is allowed access to areas where occupants are not required to wear identification badges. In such a case, the visitor can simply remove the visitor badge and blend in with the regular occupants.
of vendors and contractors. Some systems even allow visitors to self-register by using a scanned identification document, such as a driver’s license.

**After-Hours Access Register or Log**

Whichever access control procedures are used, many office buildings maintain an *after-hours access register or log* to record after-hours access activity. This log includes details such as the person’s name (printed for legibility) and signature, the name of the company the person represents or the tenant he or she is visiting, the date, and time in and out. In case of an after-hours building emergency, the log can be used to help ascertain who is in the building. However, the register or log does not provide a record of all persons in the building after hours, because some persons will have accessed the building during normal business hours before the access control log was in use. To determine exactly which tenants are in the building after hours, it would be necessary either to telephone or to personally visit every tenant. Such a procedure, particularly in large office buildings, is not considered practical.

**Right to Pass Signs or Plates**

Signs or sidewalk plates, generally located outside the building, may state the following:

“RIGHT TO PASS BY PERMISSION, AND SUBJECT TO CONTROL, OF OWNERS”

or “PERMISSION TO PASS REVOCABLE AT ANY TIME.”

If a person who does not have a legitimate reason for being in the building is discovered, then the owner, manager, or agent acting on behalf of the building may revoke that person’s right to remain. After being told to depart the premises, those who refuse to leave may be subject to arrest by law enforcement. Also, anyone reentering a building after having been warned that he or she is not authorized to enter may be treated as a trespasser.

**Tenant Access Controls**

Tenant access control involves *rented* or *assigned occupancies*. These are leased or owner-occupied spaces on various floors that are either open to the public during normal building hours or restricted to identified and authorized persons. The access control measures for tenant areas vary from tenant to tenant, depending on their type of business activity, the design of the tenant space, and the individual tenant’s management policy.

In some cases, visitors entering tenant space may simply enter at will and, in some instances, proceed directly to any area in the tenant space. However, in today’s security-conscious world, many tenants require visitors to be greeted by someone and asked to submit to some form of verification procedure before being permitted to enter the tenant space.

**Normal Business Hours**

During normal business hours, most tenants in office buildings practice some form of access control. For larger tenants, often a receptionist is present at the main point of entry to act as the first line of defense.

---

*An example of a sidewalk plate outside an office building appears in Chapter 5.

Rent is “payment for the use of space or personal property owned by another. In real estate, a fixed periodic payment by a tenant to an owner for the exclusive possession and use of leased property” (Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:146).
Tenant space design varies from tenant to tenant; however, if possible, it is helpful to channel incoming persons through one area and keep all other access points properly secured. Some tenants establish a staffed reception area that is separated by physical barriers from the interior tenant space. Once a person has been cleared for admittance, the receptionist can allow entry.

Large companies that occupy several full floors served by one elevator bank can establish access control to their elevator bank at the street level. If there is no single elevator bank serving the tenant floors exclusively, the individual elevators can be programmed to each stop at one designated floor of that particular tenant. A reception area at this point can be used to control access to that tenant’s other floors by way of an internal staircase or card-controlled access to the elevator. It is the responsibility of the receptionist (often in addition to answering telephones and handling other duties) to monitor both incoming and outgoing pedestrian traffic.

Only a receptionist who is properly trained to screen and handle incoming persons can enhance the security of the space. The receptionist must question people of all types to determine whether they are authorized to enter. One trick that has been used to gain access to office buildings has been for a person to pose as a photocopier or a telephone repairperson and, after gaining entry, proceed to steal purses, billfolds, petty cash, credit cards, laptop and notebook computers, and other small valuable items left unattended in the tenant space. These criminals are aided by two common practices: businessmen often hang their suit coat or jacket, containing their billfold, on a clothes stand or behind their office door; businesswomen, similarly, sometimes drape their handbag on a chair or leave it under their desk. These items can then be easily stolen. Another trick has been for an intruder, having gained access to a tenant space, to memorize a name from a desk or a directory board. If challenged by an occupant, the intruder simply states the name to avoid detection:

“Oh, I’m looking for Mr. Searcy!”

Unfortunately, on hearing such a reply, many an unknowing occupant has escorted the person to Mr. Searcy’s desk and left the person there to continue with the deception. Such criminal behavior can occur more easily on open floors, where elevator lobbies open into corridors that, in turn, open without any form of barrier into the main floor areas (Figure 9–1).

Once it is established that a person is permitted to enter tenant space, the receptionist should arrange for entry in a manner that does not compromise security. The person may be issued a temporary “visitor” or “contractor” identification badge for the day and asked to fill in and sign the appropriate register. Then the receptionist may telephone the employee who is expecting the visitor and ask the person to come to the reception area to escort the guest. Also, some large firms and government agencies provide a corporate mail room with a separate entrance where all couriers or others who

---

*The corporate mailroom is a major gateway into any business or government agency. Each day, the typical center handles hundreds or thousands of packages—from routine letters to confidential documents, high-value parcels, and even money. Yet despite this, many managers overlook security procedures for this critical nerve center. A mailroom security program should be divided into two components. First, the security manager should develop a plan to safeguard the mailroom against theft, fraud, and other crimes. Second, mailroom employees should be trained on mail screening techniques to protect the company [or agency] against the slim possibility of a mail bomb” (Giusti C. Mail center security. Security Management. Alexandria, VA: ASIS International; November 1998.61).
are dropping off or picking up merchandise from the tenant space can be directed. This eliminates the need to escort these individuals separately.

Unwanted Solicitors
Receptionists can play an important role in building security by reporting solicitors they encounter. Solicitors may come to buildings with items for sale secreted in a bag or a briefcase. If they can obtain entry through the building lobby, once on a floor they will open up the container, take out their product, and proceed from floor to floor, tenant to tenant, selling their merchandise. Even though solicitors may be legitimate, their presence can be disruptive to tenant business; furthermore, criminals can pose as solicitors. The tenant should never buy anything the solicitor is selling. To do so provides an excuse for the solicitor to attempt to return to the building.

If a tenant receptionist detects an unwanted person such as a solicitor or someone who is behaving suspiciously, it is helpful to security staff if the receptionist can delay the person as long as possible until security assistance arrives. If possible, it is better to have a co-worker call for security personnel out of the solicitor's hearing range. Using a prearranged signal or code phrase—such as “Sarah, could you watch the telephones for me? I'm going to be busy with the flower seller for a few minutes”—may successfully delay the individual until security staff arrives. One way to detain a solicitor is to feign interest in the product and call other “interested” employees to look at the merchandise, thereby preoccupying the solicitor. Other ways for the receptionist to detain suspicious persons would be to carry on a friendly conversation, offer an employment application, or use some other deception. Simply telling the solicitor that soliciting is not permitted generally is not enough. Having left that particular tenant, the individual will often go to other tenants.

For the protection of all tenants, it is best to have security personnel escort the solicitor out of the building. If it is not possible to delay the solicitor, it is helpful if the

FIGURE 9–1 An example of an open floor viewed from near the passenger elevator lobby. Photograph by Roger Flores.
receptionist can at least notify security staff as soon as possible and supply a detailed description of the person involved, including physical characteristics and clothing details.

**Tenant Security Systems**

Some tenants have installed their own access control systems—electric locks, mechanical or electrical push-button combination locks, card-operated locks, biometric system–operated locks, or a combination of technologies—that control the operation of entry door(s) to tenant areas. Sometimes, CCTV systems, intercoms, and intrusion detection systems are used in conjunction with these devices. When considering a system, the local fire authority that has jurisdiction should be consulted to determine whether such an installation is permitted by local codes and standards—this is particularly important when the access control devices are to be installed on doors leading directly from elevator lobbies to the tenant space. These doors involve paths of egress during emergency evacuation and therefore require special locking arrangements permitted by the authority.

**After Normal Business Hours**

After normal business hours, in most office buildings, access control to all tenant areas is strict. Perimeter doors to the tenant space usually are locked when normal business is completed. Each tenant needs to establish a specific policy and procedure for access after this time. One possible solution is to furnish tenant entrance keys to all employees who require access. This approach, however, can lead to the same problems discussed earlier, under “Pedestrian Access to Buildings.” Instead, some tenants issue keys only to a few select individuals. This alleviates some key control problems but creates the need for one of these persons to be present when special after-hours access is required. In some instances, building management has permitted some tenants to leave keys with security staff for special after-hours access. The tenant’s employees must then return the keys to their representative on the next business day. Alternatively, if someone is present inside the tenant space, he or she may be telephoned by building security and notified of the request for entry; or, according to a predetermined policy, the tenant may designate an on-call manager who handles such after-hours matters.

There is no clear-cut answer to the issue—factors such as the number of employees requiring after-hours access, the frequency of after-hours access, and tenant management’s attitude toward its employees, as well as building management policies all need to be taken into consideration for a well-defined policy to be formulated. As noted previously, some tenants have installed their own access control systems to operate entry door(s) to tenant areas, possibly in conjunction with CCTV systems, intercoms, and intrusion detection systems. Other large companies who have around-the-clock operations provide security staff or receptionists to control after-hours access. Some maintain an after-hours access register or log similar to that required for the building itself (as described earlier in this chapter). If the tenant is a restaurant that is open to the public after normal business hours and on weekends and holidays, there will be the need to provide easy access for the patrons and additional measures to ensure these persons cannot stray into other building areas.

**Doors Locked**

It is important that tenants never open their doors after normal business hours for anyone they do not know personally. For example, in an office building a temporary female employee working alone after hours one night opened the door to a man who claimed to be the window washer. The intruder raped the woman, then even had the nerve to say...
goodnight to the security officer posted in the lobby. Tenants should be educated that if someone belongs in their space, either building management or tenant management would have already provided them the means of obtaining access.

Escorts of Building Users
People in office buildings are escorted for a variety of reasons. It may be to accompany individuals for the purpose of protecting them or the property that they are carrying. It may also be to show a person where to go or to ensure that the individual does not remove property. In the high-rise setting, building users can be escorted to, from, and within the building and within tenant space.

Escorts to and from the Building
Escorts to and from a building usually occur after normal business hours. Security staff generally conducts these escorts. When tenants finish business, their employees, particularly females, may request building security to escort them to unsupervised areas of the property, such as parking garages. Building policy should dictate how, when, and where the escorts are to be conducted. For liability reasons, escorting people to offsite locations, particularly across streets, is not encouraged.

Escorts within the Building
Building policy may require that persons needing access to certain maintenance spaces and areas under construction or renovation be provided with an escort to accompany them whenever they are in these areas. Building engineering or security staff may be required to provide such escorts.

Some buildings have a list of local and state agencies whose inspectors are authorized to enter, but it is absolutely critical to verify such persons’ identification and to make building management aware (if possible) of these persons’ presence before they are granted entry. It is important to escort anyone claiming to be an inspector while he or she is in the facility. On occasion, professional burglars posing as local or state inspectors have been granted entry to buildings.

Also, janitorial staff may require escorts when they are removing trash material from building floors and transporting it to trash compactors and dumpsters. The purpose of the escort is to reduce the possibility of janitors transporting stolen items along with the trash from tenant floors and depositing them in places where they can be picked up later.

Escorts within Tenant Space
It is usual for visitors, such as salespersons, tradespeople, couriers, and delivery persons, to be escorted within tenant space. This will depend on the type of business the tenant conducts, tenant policy, and staff availability. For example, a tenant may require an employee to accompany such persons at all times while they are inside tenant space or just accompany them to particular areas and leave them unsupervised to carry out the tasks they have been authorized to perform.

Property Control
There are various property acceptance and removal systems that building managers and tenants can implement to provide some control over the property that on a daily basis
is moved in and out of office buildings and tenant areas. The degree of control will vary from building to building and tenant to tenant, and it will depend largely on the policies established by building management and the tenants themselves. The effectiveness of these policies will depend on how thoroughly they are communicated to building staff, tenants, and occupants; how strictly they are enforced; and the support afforded the program. It is sometimes difficult to implement strict property control measures in a multiple-tenant/multiple-use commercial office building, primarily because each tenant may expect a different degree of security.*

**Objectives of a Property Control System**

The objectives of a property control system are threefold:  

1. **To prevent stolen property or other unauthorized items from leaving.** Stolen property may include computers (personal, laptop, and notebook), personal data assistants, mobile telephones, fax machines, calculators, and general office equipment. An unauthorized item might be a sensitive or a classified document that is not to be removed from a certain area or from the building.

2. **To prevent dangerous items entering.** Explosives are the usual concern, but other items such as cameras or firearms might be prohibited. (As a result of September 11, 2001, metal detectors and X-ray systems, although not in common use in office buildings, were deployed in some landmark facilities as a screening measure for weapons and explosive material concealed on people and contained in packages and other containers.)

3. **To prevent unnecessary or disruptive delivery traffic.** By keeping out misdirected deliveries, unnecessary traffic is avoided. By routing deliveries through proper entrances, such as loading docks and freight/service elevators, disruptive traffic is avoided and, in some cases, the building and passenger elevators are protected against damage from hand trucks and bulky crates. By intercepting deliveries at these entrances to the building, it may be possible to detect intruders posing as delivery persons.

**Property Removal Pass System**

Unauthorized removal of property from office buildings can be controlled to a degree** by requiring property removal passes for business and personal items taken through an egress point controlled by security staff. The time period when the property removal pass system is to be in effect is set by building management and then communicated to the tenants. (Some buildings only permit the checking of property removal after normal business hours.)

---

*This discussion of property control does not include the means for protecting proprietary information. However, it is appropriate to mention that document destruction either onsite using a shredder or offsite by contract companies, can be an effective means of safeguarding critical information stored in documents that needs to be destroyed.


**Small items can easily be concealed on a person or in a briefcase or a carrying bag. Also, a thief working in a building can circumvent a property control system by using commercial mail services to send stolen items out from the building. Unless electronic tracking of assets is provided, a thief can thereby bypass a building's property control system.
Building management can supply property removal passes to key tenant representatives who then supervise their distribution to tenant employees and visitors on an as-needed basis. The passes may vary both in design and in the information recorded on them.

**Required Information for a Property Pass**

For the property pass to be of value, it should address at least the following areas of information:

- Name and signature of the person authorized to remove the property
- Name and room or suite number of the tenant or company from whom the property is being removed
- Printed name and signature of the tenant representative who has authorized the property removal
- Brief description of the property, including any model, serial, or asset tag numbers
- Date property will be removed (some passes do not require this information)
- Date and time of removal of the property
- Signature of the person (usually a member of the building security staff or a receptionist) collecting the pass and permitting removal of the property.

Property passes should be sequentially numbered and a record kept of which tenants received which numbered passes. They should also be in duplicate (following the removal of the property, the original is returned by the building security staff to the tenant representative and a copy is kept on file by the building security department).

A *sample property removal pass* for an office building is shown in Figure 9–2. After the authorized tenant representative has signed the form, any blank lines on the pass should be crossed out to prevent unauthorized entries.

Whenever building security staff reviews a property removal pass, they should thoroughly examine it to ensure that it is complete and contains all the necessary information. The identity of the person actually removing the property should be confirmed by means of a valid driver’s license or other photo identification.

It is best if each tenant has already provided an authorization letter containing sample signatures of each representative authorized to sign a property removal pass. Building security staff can then compare the signature on the pass with the signature on the letter. If it matches, security will permit removal of the property. If it does not match, security personnel will keep the pass and may attempt to contact either an authorized tenant representative or building management to resolve the matter. Such a system can be effective in controlling the removal of some business and personal property. However, as previously mentioned, many computer-related items are small enough to be carried out unobserved in a carrying case or pocket.

**Permanent Property Pass**

Some office buildings permit the use of a *permanent property pass*. This pass eliminates the need to continually issue property passes for personal or company property that is frequently carried in and out of the building. The permanent property pass is similar both in design and recorded information to a regular property pass, except that it can be used repeatedly for the period of time stipulated on the pass. The card is often laminated to prevent damage and affixed at all times to the item in question. Building security staff should keep a photocopy of each pass and a log that documents their use.
As outlined in Chapter 5, small, radio frequency identification (RFID) asset tags—some of which were embedded into desktop and laptop computers at the time of manufacture—can be assigned to an asset that is permitted to leave a building. Integrated with a building's...
access control system, asset tracking can be utilized to control the movement of computer equipment and other assets from the building.

An asset tagging and tracking proximity system “allows free egress when authorized assets are removed, but prevents unauthorized removal of property. Without electronic tracking, assets can be removed by concealing them in a briefcase, package or gym bag.”

This system can also be adapted to screen assets being mailed out of a building through a central shipping area such as the loading dock.

**Dangerous or Illicit Items**

To prevent someone from entering the building on foot or in a vehicle with dangerous or illicit items is not as easy a task as it would at first appear. Items such as explosives, illegal drugs, and chemical and biological weapons might easily be secreted on a person or in a vehicle and brought into a building.

**Measures to Screen for People-Delivered Explosive Devices**

Various measures can be used to screen for persons possibly bringing explosive devices into a building, some of which are as follows:

- Search persons and items such as suitcases, briefcases, handbags, gym bags, backpacks, packages, and other containers. This practice is not common in most commercial office buildings.
- Use metal detectors and X-ray machines, explosives trace detectors, or explosives-detection trained (bomb-sniffing) dogs to screen for weapons and explosive devices concealed on people or in items they carry. Due to the perceived high-risk, some landmark buildings are deploying such measures.
- Keep doors or access ways to certain areas—mechanical rooms, mail rooms, computer rooms, data centers, and elevator machine rooms—locked at all times.
- Install intrusion detection devices at entrances to high-risk areas, and use CCTV in areas identified as likely places where a bomb may be placed. This, coupled with posting signs indicating that such measures are in place, is a good deterrent.
- Building personnel should be alert for people who act in a suspicious manner, as well as objects, items, or parcels that look out of place or suspicious.
- Security personnel should patrol potential hiding places (e.g., stairwells, restrooms, and vacant office space).
- Good housekeeping should be practiced for trash (rubbish) storage, trash compacting, and dumpster areas. (Likewise, a sometimes overlooked possibility is that when a fully loaded dumpster is replaced, one loaded with explosive

---


* A serious safety concern is that industrial trash compactors should always be locked when unattended and that their operators be thoroughly trained.

** A dumpster is “a large steel waste receptacle designed to be emptied into garbage trucks. The term is a genericized trademark of the Dumpster brand. The term is also common in Australia although Dumpster is not an established brand there. In British and Australian English, the terms wheelie bin and skip are more commonly used (although they are not perfect synonyms). In some other countries the more descriptive term frontloader container is often used, either in one or two words. In India it is called a garbage bin” (Wikipedia. <http://en.wikipedia.org/wiki/Dumpster_%28term%29>; July 19, 2008).
material could be delivered. Dumpsters should be checked upon delivery to ensure they are empty.)

- Mailboxes at buildings can be used to deposit an explosive device for later detonation. Consideration should be given to using blast-resistant mailboxes or to removing them altogether.

Measures to Screen for Vehicle-Delivered Explosive Devices

Measures to reduce the risk of explosive devices in vehicles include the following:

- Restrict or eliminate parking of vehicles adjacent to a building, and eliminate public parking in underbuilding parking garages.
- Check passenger vehicles, particularly those entering underbuilding parking garages, for bombs as they enter. For high-risk facilities, these inspections might include the use of security or parking personnel inspecting vehicles (including their trunks and boots) or using a small hand-held mirror or a CCTV camera attached to a 3-by-4-foot (0.91 by 1.21 meters) long metal pole to inspect under vehicles, undervehicle scanning systems, and the use of explosive trace detectors or explosive-detecting (bomb-sniffing) dogs.
- Require vehicles, particularly vans and trucks, to undergo on-street inspections before being permitted to enter loading dock/shipping and receiving areas. For high-risk facilities, these inspections might include performing X-rays of entire vehicles, the use of undervehicle scanning systems, and the use of explosive trace detectors or explosives-detection trained (bomb-sniffing) dogs.

Couriers and Delivery Persons

In many facilities, couriers and delivery persons, once cleared to enter, can freely move about a building to deliver and pick up letters, packages, and other items from tenants. However, there is an alternative for owners and managers who want to prevent unnecessary, disruptive, or possibly undesirable delivery traffic in their facilities. Some buildings have instituted special programs whereby outside couriers, on arrival at

---

* Also available for viewing under vehicles is an all-weather video camera fitted with a wide-angle lens. The camera is mounted on a swivel wheelbase that can be moved under a vehicle. The image can be viewed using a head-mounted video monitor (Sperry West, SpyderScope® Under-vehicle Video System, Sperry West, Inc., San Diego, CA. <www.sperrywest.com>; July 5, 2008).

** “The Under Vehicle Monitoring System SecuScan essentially comprises a scanning unit, a workstation, traffic lights and a light barrier…. Through a small slit in the scanning unit, the camera captures the entire underside of a vehicle in moving traffic…. To simplify the correlation between the underside images and the corresponding vehicles, an optional front-end capture camera as well as automatic license plate recognition can be integrated…. All the data collected or manually entered can be stored in a database under the vehicle license plate number. In case of recurring vehicles, the software provides the possibility to compare the current underside image with an already archived one of the same vehicle in order to identify potential deviations at a glance.” Signalbau Huber “Under Vehicle Monitoring System,” Signalbau Huber, Munich, Germany. <www.secuscan.com/content/prospekt/prospekt_e.pdf>; July 4, 2008.

*** MobileSearch is a noninvasive inspection system that involves the use of an X-ray source mounted in a truck. It can be used to X-ray entire vehicles, including large trucks. Such a device can be effective in screening for explosives and weapons before a vehicle is permitted entry to an underbuilding parking garage and loading dock/shipping and receiving area. MobileSearch (Information obtained at a demonstration of the American Science and Engineering [AS&E] MobileSearch system, Billerica, MA. <www.as-e.com>; June 2002).

A courier is a person or a company who delivers or picks up items such as documents, parcels, packages, or containers.
a building, are directed to a separate entrance, such as the loading dock or a central mail room. At that location, building couriers employed by a contract courier or a security company assigned to the building sign for the items and deliver them within the building by way of the freight/service elevators. When items are to leave the building, these same couriers pick up the articles from the tenants, bring them to the central location, and then outside courier companies sign for them before taking them from the facility. As a rule, major courier services that regularly do multiple deliveries in a building are permitted to perform their own pickups and deliveries. Special deliveries or pickups can be facilitated by providing temporary badges for outside couriers to enter or by providing an escort for these couriers while they are in the building.

These programs have been very successful. When dedicated building courier or security staff performs multiple deliveries and pickups from tenants, the overall number of couriers roaming throughout a building decreases: a valuable security advance when a million-square-foot office building may have 300 or more individual deliveries per normal business day. In addition, the number of couriers using elevators is reduced. Also, it can enhance security by providing an added presence in the building (particularly if security staff are used), and because these building couriers should have already been “security vetted” (i.e., a background check of these individuals has been conducted), there is less chance of possible theft or vandalism than when using outside courier services. Delivery to secured or normally “locked-off” floors is also easier because dedicated building couriers can more readily be entrusted with the access codes or cards that allow them to enter such restricted areas.

Like any well-run operation, such programs need to be meticulously documented to provide an audit trail to track deliveries and pickups and ensure that these tasks are being done in a timely manner. If there is a question about the time property was picked up or delivered or about the individual who signed for it, accurate records should be immediately available for review. Some individual tenants, particularly larger ones that occupy full floors and multiple floors, have addressed the issue of outside couriers roaming within their space by establishing a separate mail room from which only tenant messengers perform all deliveries within the tenant area.

**Package Acceptance Policy**

During normal business hours, when tenants are usually open for business, they generally accept their own packages. For those delivered after hours, their acceptance or rejection largely depends on the policy established by the building owner or manager. For security and safety reasons, most commercial office buildings do not permit after-hours acceptance of packages by security staff. The building does not want to accept the responsibility and potential liability of accepting packages (including certain legal documents) the tenant may refuse; also, these packages may contain dangerous or illicit items. Some buildings do permit the acceptance of after-hours packages on certain occasions and under special circumstances. This will usually require a written request by the tenant and an explicit understanding that the building and its agents are absolved from any liability resulting from accepting the package on behalf of the tenant.

**Lost and Found Property**

Handling lost and found property is an often-neglected but critical part of an effective security program. Most people can recall the anguish they felt on discovering that a
valuable personal possession or business item was missing. Likewise, one may remember
the exhilaration at being contacted and informed that the missing property had been
found and was available for pickup.

If property is lost in a building and is subsequently found and handed to building
security staff, the item(s) should be kept in a secure place (such as a locked cabinet or
an access-controlled room) and, if possible, expeditiously returned to its rightful owner.
Such action can considerably enhance the trust and confidence that building occupants
and visitors will have in the building security operation. Just the opposite will be true if
a tenant learns that the found item was handed to building security staff and was then
lost or went missing.

Lost and Found Property Log
Building security staff should maintain a list of lost and found items in a lost and found
property log. The log should contain details such as the following:

- A brief description of the property, including any serial or asset tag numbers
- The date, time, and place the property was lost or found
- The identity of, and means to contact, the person who lost or found the property
- If the property is claimed, the identity of, and means to contact, the claimant and
  the signature of the person who received the property
- The name(s) of the person(s) who took the report of the lost property, logged in
  the found item(s), or handled the return of the property to its rightful owner

Handing Over to Local Authorities
If the lost property is particularly valuable or sensitive, it may be necessary for the local
law enforcement agency to be contacted; if the property is subsequently handed over to
them, this fact, including the identity of the receiving law enforcement officer, should be
noted. A receipt for the property should be obtained. Local and state laws often deter-
mine the handling of lost property.*

Some jurisdictions allow found property, when its owner is unknown and its value
is below a certain amount, to be distributed to local charitable organizations. Others,
after a certain waiting period, auction the property or allow the finder to assume owner-
ship of it.

Trash Removal Control
There are a number of controls that can be placed on trash removal from tenant
space and from a building. The design and implementation of these controls largely
depend on the specific cleaning operations in effect at the building. Some operations
“gang clean” by using a team (including dusters, cleaners, waxers, polishers, and trash
removers) to clean tenant spaces and restrooms on a series of floors. Others assign
specific janitorial staff to perform all functions on particular floors. From a security

*For example, in California, Section 2080 of the California Civil Code does not require a person to take
charge of found property, but if he or she does, he or she can be sued for the negligent handling of it. The law
further provides that if the owner of lost property is known, the property must be returned to that owner.
If the owner is not known and the property has a value above ten dollars, the property, within a reasonable
period of time, must be turned over to the local police (American Protective Services. Administrative News.
Oakland, CA; 1993:4).
standpoint, the latter is preferable because regular staff members are more likely to
detect unauthorized persons who do not belong in a particular tenant space and because
investigations involving janitors are easier when the same janitors regularly work in a
particular tenant space.

Sensitive Information
Depending on the sensitivity of the business conducted, tenants may shred certain pro-
prietary documents themselves, or they may employ contract-shredding agencies that
will come to the building on a scheduled basis to remove and destroy documents. These
documents may include sensitive business data, client lists and billing information, those
that are confidential within a company, and any proprietary information that would be
useful to competitors. Depending on the sensitivity of these data, they may be passed
through a standard shredder or through a crosscut shredder.

Importance of Supervision
Routine removal of trash from a tenant floor should be carried out under constant
supervision by janitorial supervisors or building security staff. No interruption should
take place in supervision during the janitors’ passage from the tenant floor to a service
or freight elevator or to designated receptacles such as dumpsters, compactors, or holding
areas, usually located at the building loading dock. Such supervision will deter jani-
torial staff from secreting stolen articles in trash bags and then dropping the articles in
locations within the building where they or an accomplice can later retrieve them.

To make it easier to scrutinize trash, the bags themselves should be made of trans-
parent plastic. If, because of staffing limitations, direct supervision of trash removal
is not possible, then CCTV cameras in the dock areas are recommended to deter the
removal of items from trash bags before they are placed in dumpsters, compactors, or
holding areas, or for later retrieval from the receptacles themselves.

Special Trash Holding Areas
Trash holding areas can be found in office buildings, particularly where refuse from
financial institutions is being handled. To avoid accidentally discarding important doc-
uments such as negotiable instruments (checks, bank drafts, savings bonds, securities,
etc.), the trash from financial businesses often is separated and held in a secured area for
a length of time as determined by the financial institution concerned. The holding time
permits losses to surface before trash is removed for destruction and thereby facilitates
possible retrieval of the item in question.

Janitorial Staff Screening
In many buildings, janitorial staffs may be required to enter and leave the building
through an employee entrance and be subject to certain property screening procedures.
The object of the screening procedure is to observe any prohibited items being brought
into the building and to detect any stolen property being removed from the building. As
part of preemployment or preassignment agreements, janitors may be asked to submit
to a visual inspection of any items they are carrying to and from work—lunch pails,
bags, backpacks, packages, and other containers. The frequency of the inspections can
be established as part of the agreement: inspections may be conducted every time the
employee enters or leaves the building, at random, or only with cause.
Janitorial supervisors or building security staff usually conduct such inspections. They are visual only, and employees are requested to open appropriate items themselves. Under no circumstances does the inspecting person touch the items being inspected or attempt to inspect any part of the employee's person or clothing. All persons have a legal right and expectation of privacy, so items such as purses will be subject to inspection only under special circumstances, the nature of which should be established in writing beforehand. Some operations require janitorial staff to wear special clothing or smocks in which it is difficult to conceal items.

**Importance of Controlled Ingress and Egress**

The success or failure of any property control system depends largely on whether there are “controlled” exits or entries to the facility for use by building occupants and visitors. For example, if building users need to pass through one particular point to enter or leave the building, and if this point sometimes is not supervised, then the property control system can be circumvented. Similarly, if there are other unsupervised exits or entry points, persons can defeat the property control system by using these areas when they want to bring in or take out property.

Some high-rise buildings with underbuilding parking garages have passenger elevators that allow people to travel directly up from the garage to the tower and similarly for people to travel directly down from the tower to the parking garage. Such an arrangement affords no control over ingress and egress of people and property.

To address this problem, several possible solutions are as follows:

- Whenever the elevators are operating, provide security staff in the parking garage elevator lobbies. This will help control the movement of people and property but is an ongoing security expenditure.
- Install optical turnstiles in the parking garage elevator lobbies. This will control the movement of people but will not control property (and the turnstiles themselves will require some supervision by security staff).
- Install full-height security turnstiles equipped with card readers in the parking garage elevator lobbies. This will control the movement of people but will only control large property items.
- Install card readers in the elevators. This will help control the movement of people (tailgating or piggybacking of passengers will be possible) but will not control property.
- Install CCTV cameras in the elevator cars or in the parking garage elevator lobbies. If the cameras are constantly monitored or the images constantly recorded, the unauthorized movement of property might be observed either at the time it occurs or at a later stage.
- If possible, reprogram the elevators so that some exclusively service the parking garage and the building main lobby. Passengers traveling up from the parking garage will need to cross to other elevators to proceed to the tower floors. Similarly, passengers traveling down from the tower floors will need to cross over to the garage shuttle elevators to proceed to the parking garage. (Due to the limited numbers of elevators in some buildings and the pedestrian traffic load, such a measure may not be practical due to congestion and extended delays.) Even
with this arrangement, to effectively control most property, the main lobby would need to be staffed by trained security personnel.

**Key and Electronic Access Card Control**

In office buildings, keys and electronic access cards to the facility are under the control of building management, engineering, and usually security personnel. Building management personnel obviously need to have access to all areas of the facility they manage. Building engineers, because of the nature of their work, also need access to virtually all areas, including tenant spaces. Depending on how the building is managed, security staff also will need access to most areas.

**Key Control**

The decision as to whether master keys are issued to building security staff will vary from building to building. If they are not issued master keys, they will often be issued a ring of keys permitting them to enter various parts of the building. Some facilities keep tenant office keys out of the routine possession of security staff but provide a controlled, documented means for these keys to be obtained, when necessary. After the situation has been resolved, the keys are again placed under supervision, perhaps in a locked cabinet or a key cabinet secured with a key, a lock code, an access card, or a consecutively numbered seal.

Keys issued to the security staff should never be permitted to leave the facility. They should be passed from shift to shift and a receipt should be recorded each time they change hands. All security personnel should understand the importance of not permitting keys to be compromised.

**Key Points to Consider**

Keys (and access cards) should be issued only to those persons who can be entrusted with them and who have an *absolute* need for them. The status a key holder may feel by possessing certain keys should not enter into the decision-making process. The following points are important to consider:

- Tenants and residents should be issued keys that pertain to their particular area only.
- Tenants and residents should never be issued building entrance keys. (If issuing entrance keys is unavoidable, the locks should be changed periodically or when a key has been lost or taken, and new keys should be issued to the tenants authorized to have them.)
- Tenants and residents should not be allowed to duplicate keys. (Keys should be marked “Do Not Duplicate” as a deterrent to duplication. Also, keys issued to tenants may be distinctively marked to help identify unauthorized keys they may have had cut themselves.)

---

*If such staffing is not possible because of budgetary constraints, card readers may be provided in the elevators and CCTV cameras placed inside all elevators or at the parking garage elevator lobbies. By placing the elevators on card access, tenants will be required to use their cards to access floors, thereby providing some degree of access control. If the cameras are constantly monitored or the images constantly recorded, the unauthorized movement of property might be observed either at the time it occurs or at a later stage.

**For additional information on the control of keys, see Chapter 5, “Key Control.”**
• When an employee ceases to work for a tenant, all the employee’s keys should be returned to the tenant representative. Depending on the situation, locks may need to be changed.

• When a tenant or a resident moves out, all tenant or resident entry door locks should be changed.

• Janitorial staff should be issued keys only for the time they require them and for the particular areas to which they require access. Depending on the size of the janitorial staff, designated supervisors within the janitorial operation may be issued master keys that, for instance, provide access to all tenant spaces on an individual floor. In this way, the general cleaning staff does not need to be issued keys. In some buildings, no janitorial staff is issued keys, and security staff must unlock the appropriate doors and relock them after the work is completed. Procedures will vary from building to building depending on size, complexity, and the manner in which cleaning is conducted and trash is removed.

• Elevator, escalator, dumbwaiter, chute (rubbish, mail, laundry, and linen), and moving walk technicians may be permitted to carry keys that provide access to their equipment, or the building may retain possession and issue them only as needed.

In some buildings, telecommunications technicians, gas, water, and power utility workers are permitted to attach their own locking devices to areas containing their equipment. This practice is convenient because building staffs are not required to open these areas, but it compromises security because control of keys and the areas themselves has been lost. These areas could be used to store unauthorized or stolen items, and general housekeeping may become a problem. If this practice is permitted, no one should be allowed to place a lock on a door without building security or other building departments (such as engineering) having a key. In an emergency, keys must be available for access. A possible alternative is for contractors to store their equipment, including tools, in heavily reinforced, large steel boxes, chests, and cabinets that can be secured using high-security padlocks, which are protected from attack with cutting tools.

In the event of a lost or missing key, the circumstances surrounding the incident should be investigated and documented. If the key has been compromised, consideration should be given to changing the affected lock(s) or moving it to a less sensitive area of the building; in the case of a compromised master key, because the whole system is compromised, rekeying the entire building should be considered. “If rekeying becomes necessary, it can be accomplished most economically by installing new locking devices in the most critical points of the locking system and moving the locks removed from these points to less sensitive areas. Of course, it will be necessary to eventually replace all the locks in the system, but by using the method just described, the cost can be spread out over several budgeting periods.”25 Whether to immediately rekey the building or delay in this suggested manner is a risk-based decision that should only be undertaken by the building owner or manager. If delaying the rekeying can potentially affect the life safety of people or seriously impact other vital assets, then despite the costs involved, it should not be delayed.

Electronic access cards should be issued only to those persons who can be entrusted with them and who have an absolute need for them. Access cards issued to building staff, including security staff, should never be permitted to leave the facility. They should be passed from shift to shift and a receipt should be recorded each time they change hands. All personnel should understand the importance of not permitting access cards to be compromised. Also, if a card is lost or missing, as soon as possible after its reported loss, it should be deleted from the system and the circumstances surrounding the event investigated and documented.

Mobile Patrols

Mobile patrols may be conducted in office buildings for a variety of security and fire life safety purposes. “Guards [security officers] are typically highly visible thus offering something of a deterrent effect and at the same time imparting a sense of security to the building’s tenants and visitors.”

Patrolling increases this visibility. Patrols can also be used to note and quickly address anything significant or unusual affecting security or fire life safety. After conducting a risk assessment (as described in Chapter 4), the purpose, frequency, and routing of patrols can be determined by hotel management and the security department (and, if special circumstances warrant, with the cooperation of local authorities) and then carried out and thoroughly documented.

When and Where?

Patrols by security staff in office buildings may occur as follows:

- For approximately the first hour after opening the building on a regular business day, when there are usually not many occupants in the building, to provide a security presence throughout common areas and tenant floors.
- After the building is closed at the end of the business day, on tenant floors, to check for doors left unlocked or not completely closed, signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong, and so on.
- Some buildings require such patrols continuously throughout all common and maintenance areas (including stairwells outside normal business hours). The purpose is to report obstructions (particularly those blocking emergency egress routes), fire hazards, missing equipment (such as portable fire extinguishers), water or gas leaks, wet floors, holes, defects in floor coverings, tiles missing, unsecured areas, malfunctioning lighting equipment, signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong, and so on.
- Continuously in parking garages and lots to deter theft of vehicles and property within them; note parking violations and issue warnings or citations, or institute


 Violations include vehicles improperly parked, parked in a NO PARKING zone or space, parked in a RESERVED zone or space, or parked in a DISABLED/PHYSICALLY IMPAIRED designated space. When placing such a notice on a vehicle, preferably locate it in the lower corner of the driver’s window (immediately
vehicle towing actions; observe vehicle lights or engines left on, leaks from vehicles, or other unusual conditions of parked vehicles; report fire hazards, water or gas leaks, malfunctioning lighting equipment, broken vehicle windows and other signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong; and provide for the general safety of tenants and visitors. (Motor vehicles, electric carts, bicycles, tricycles, and personal transporters may be used for patrolling large parking areas with long travel distances.)

- On building floors and in parking garages, key patrol stations are often installed at each stairwell so that the patrolling officer must traverse the floor in order to complete the tour.
- Depending on a building’s usage, patrols may also be conducted in areas such as retail arcades, public parks and gardens, and other areas, with times varying according to their operating hours.
- In some buildings, patrols within tenant spaces to report security and safety hazards, including unsecured laptops and confidential information.
- To perform a fire watch when a building has exceptional hazards or the fire protection system is impaired. A fire watch is “the assignment of a person or persons to an area for the express purpose of notifying the fire department or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety dangers.”

**Patrolling Tips**

- Patrols can be conducted either on foot or using a motor vehicle, an electric cart, a bicycle, a tricycle, or a personal transporter.
- There should be reliable communication between the patrolling officer and the security department or the supervisor.

above the door handle) where it will be visible to the driver when entering the vehicle but will not obstruct his or her field of vision when driving. Also, the notice should be of a nonadhesive material that is easily removed from the glass.

- In some buildings, the patrolling officer carries a pager, a mobile telephone or a hand-held panic alarm so that tenants, particularly retailers, can summon the officer for assistance.

- Entering a tenant office may place the patrol officer in a “difficult and sensitive” situation, particularly after normal business hours. If it is necessary for a security officer to enter a tenant area after hours, another officer should accompany him or her. These officers should knock on the door before opening it and call out loudly to identify themselves and their intentions. Such actions can help avoid embarrassing and awkward situations and protect staff from unfair accusations. If entering tenant space is only permitted under special situations it may be wise to also be accompanied by a building engineer or other building staff member. Intrusions into tenant space should always be thoroughly documented.

- Whenever a building presents a hazard to life or property as a result of a fire or other emergency or when any fire protection equipment or system is malfunctioning or has been taken out of service, a fire watch will often be immediately required by the authority having jurisdiction (usually the fire department). For example, in the United States, according to NFPA 601, Standard for Security Services in Fire Loss Prevention, Chapter 3 Security Functions and Duties, “a security officer shall make rounds at intervals determined by management. When operations in the property normally are suspended, officers shall make rounds hourly or as assigned by management. Where special conditions exist, such as the presence of exceptional hazards or when fire protection equipment is impaired, management shall institute additional rounds. The first round shall begin within 30 minutes after the end of activities of the preceding work shift. During this round, the security officer shall make a thorough inspection of all buildings or spaces” (Section 3-2.1-3-3.2.2).

Whenever possible, routine patrols should be conducted in a random, unpredictable manner to avoid a fixed pattern or routine that someone planning to commit a crime can observe. Sometimes, an officer occasionally “doubling back,” or retracing steps to a previous location, can be an effective tactic; anyone observing the patrolling officer’s movements would usually not expect the officer to return quickly to an area just visited.

“Alertness, interest and thoroughness must be displayed. A suspicious mind must be cultivated and anything that appears other than normal must be looked into.”

Using a flashlight or a torch in areas where lighting is poor or nonexistent is extremely useful.

“A simple but effective patrol plan should be established in each area. Its efficiency should be regularly checked by means of [patrol management devices*], radio or telephone checks at regular intervals, etc. Failure to report, or deviation from described assignments, should immediately be investigated.” Patrol management devices “provide the security manager with a consistent record of rounds and occurrences at a facility without the need for human supervision to ensure that rounds are completed as assigned.” If an electronic patrol management device is not used, a notebook is useful for recording observations. (The patrolling officer can carry the notebook, or it can be located at designated patrol stations so the officer can record when visiting a particular area.)

Tenant Security Education

There are many ways to educate building users and tenants about the building’s security program. All building users, particularly tenants and their visitors, should be made aware of the program and how various policies and procedures impact them. If people are aware of the logic behind security regulations, they usually will be more willing to comply with them. This communication can be achieved in the following ways:

1. Explain the regulations on an informal, as-needed basis. For example, building security staff may explain the purpose of an after-hours access register to a tenant when asking him to sign it, or staff may inform a visitor leaving the building that she must have a property removal pass signed by the tenant she just visited before the computer she is carrying can be permitted to leave the building.

2. Use posted signs; written policies and procedures published in the Tenant Manual** and on the building’s website; pamphlets, leaflets, flyers, newsletters, e-mails, and video training materials supplied by building management to the tenant or by tenant management to its employees. Sometimes, information

---

*See a description of “Patrol Management Devices” in Chapter 5.


** A tenant manual (or tenant information manual) is usually supplied by building management to each tenant liaison person. The manual is “a compilation of management policies and procedures that relate to commercial tenants and the use of their leased space” (Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:171).
is displayed on in-car elevator video screens. Such elevator bulletins may, for example, provide information that reminds occupants that in the event the elevator stops running, they should immediately use the elevator emergency communication device to request assistance, or the bulletins may be used to post other appropriate emergency notifications.

Appendix 9–1 (which is on the CD-ROM provided with this book) is a Sample Tenant Security and Safety Awareness Checklist that could be revised and sent to tenants at appropriate times during the year.

3. Conduct security and safety orientation lectures, classes, briefings, workshops, and seminars. These events can be an effective medium not only for communicating to tenants what is required of them in the building security program, but also as an opportunity to educate employees about basic security and safety measures they can adopt at home. (Such measures could include being aware of their surroundings; elevator safety, securing vehicle doors and windows; not leaving valuable items in view in parked vehicles; securing desks, filing cabinets, laptop computers, computer storage devices, and personal property; and observing a “clean tabletop” policy.) The length of such events will vary, but 45 minutes to an hour is probably the maximum that busy tenants will permit. As with all effective teaching, the use of audio-visual aids—films, videotapes, DVDs, and slides—can help gain the participants’ attention and assist in effectively communicating the required message. The frequency of classes, meetings, conferences, seminars, and workshops will vary from building to building; they may be regularly scheduled or conducted when a specific need arises. Security training can be incorporated effectively into occupants’ fire life safety training classes. More will be said about the training of occupants, floor wardens, and building emergency staff in the next section, “Emergency Planning.”

The tenants themselves are an important part of any building security program. They should be educated to know that they are the eyes and ears of the building. If they see a suspicious person, particularly someone within their own tenant space, a simple “May I help you?” type of approach will reveal much about the person. Specific questions can determine if the person is an employee, a visitor (if so, who is he or she visiting?), or is delivering or picking up items (if so, where? at whose request?), and so on. Although the tenants are not expected to be trained security professionals, they are expected to be active participants in the building security program by being aware of

*For example, tenants should be made aware that when they are about to enter an elevator, if they observe a suspicious person inside the car they should not proceed but simply wait for the next elevator; or, while inside an elevator car if they similarly notice such a person they may consider exiting the elevator as soon as possible, or, if others are present, follow them when they disembark. “Never doubt your instincts. If you have a creepy feeling about a person, that’s because there’s usually a reason. Our bodies have ways of sensing danger. If you’ve ever been accosted or attacked, you will certainly understand the advantage of being proactive when it comes to elevator travel” (Fourchalk F. Peace Arch News. In: The ups and downs of elevator security. November 22, 2008. <www.bclocalnews.com/surrey_area/peacearch/news/lifestyles/34907009.html>; December 20, 2008). Standing close to the elevator control panel also affords riders the opportunity to quickly access the emergency call button, phone, or intercom to summon help. Also, “this way if someone begins to harass or threaten you, you can push all of the control buttons, which will cause the elevator to make several stops. This will now allow you many attempts to exit as the elevator stops at each floor” (Fourchalk F. Peace Arch News. In: The ups and downs of elevator security. November 22, 2008. <www.bclocalnews.com/surrey_area/peacearch/news/lifestyles/34907009.html>; December 20, 2008).
their surroundings and promptly reporting potential security problems to tenant management, building management, and building security staff.

Emergency Planning

For a building owner or manager to effectively manage an incident that constitutes an emergency in an office building, it is critical to plan ahead. Before proceeding, it is appropriate to review several key concepts.

Key Concepts

An incident is an “event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization’s operations, services, or functions—which, if not managed, can escalate into an emergency, crisis, or disaster.”

A disruption is “an event that interrupts normal business, functions, operations, or processes whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a [power] blackout, terror attack, technology failure, or earthquake).”

An emergency is “an event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response.” During an emergency there may be chaotic conditions, particularly if there is a disruption in normal communications.

A crisis is “an unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.”

Emergency management (also sometimes known as crisis management) is defined as “the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness [and] response.”

---


32 ibid, p. 46.


The combined definition stated here uses a slightly modified version of the United Nations terminology. The UN definition states that emergency management is “the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness, response and rehabilitation.” The word rehabilitation has been removed. The reason for this is that for the purposes of this book, an emergency management plan addresses preparedness and response to an emergency, and shortly thereafter. It does not deal with the rehabilitation process because, in the opinion of the author, that process is part of business continuity planning, which is “an interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption” (Business Continuity Planning. Wikipedia. <http://en.wikipedia.org/wiki/Business_continuity_planning>); July 9, 2008).
A plan is defined as “a scheme or method of acting or proceeding developed in advance.”

Combining the terms emergency management and a plan can lead to a definition of an emergency management plan as “a scheme or method of acting or proceeding developed in advance for the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness and response.”

“The objective of an [emergency management plan] should be to allow those responsible for the [facility] during an emergency to focus on the solution of major problems, not to attempt immediately to bring order out of chaos. If all predictable and routine items are considered in the plan, those responsible for actions during an emergency will be able to deal with the unpredictable or unusual situations that will surely develop.”

According to Groner,
The chaotic and dynamic nature of building emergencies requires an exceedingly rapid assessment of the situation. The timeframe is measured in seconds and minutes, not hours and days. The rapid onset of many events means that the process should be well underway before emergency responders arrive at the building.

Human factors professionals have been actively researching this problem under the generally accepted term of “situation awareness.” Endsley (1988) has provided a well-accepted definition: “The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.” As noted in the definition, it is insufficient to understand the momentary status


Sometimes an emergency management plan is referred to as a fire life safety plan or an emergency action plan (EAP). An EAP is defined by the NFPA as “designated actions that employers, employees, and other building occupants should take to ensure they are safe from fire and other emergencies” (NFPA. Glossary of Terms, National Fire Code. Quincy, MA: National Fire Protection Association; 2001). Sometimes, the term prefire plan is also used. Because an emergency management plan should encompass the types of emergencies considered likely for a building, simply designating it as a “prefire” plan can be misleading.


of the situation; projecting its development is of great importance in choosing a strategy to safeguard building occupants.

The purpose of an emergency management plan is to help building emergency staff in their efforts to achieve situation awareness and make sound decisions to provide for the safety of building occupants during emergencies, such as fire.

The value of emergency planning lies not only in the emergency management plan itself but also in the development process leading up to it and the education of building emergency staff that should occur in the process.

How to Develop a Building Emergency Management Plan

The building emergency management plan in Appendix 9–2 (which is on the CD-ROM provided with this book) is a suggested format for developing an emergency management plan for an office building. It includes actions intended to reduce the threat to the life safety of building occupants from emergencies, both fire and non-fire-related, that are likely to occur in a specific building, or in close proximity to it, until the arrival of emergency responders.

It is important that as many as possible of those who will be involved in the execution of the emergency management plan participate in the planning process. This includes the emergency staff of the building, public officials (such as those from the local fire and law enforcement agencies), and possibly building management staff from neighboring buildings (with the view to developing mutual aid agreements). Public officials may require a particular format for the plan itself.

---

*Achieving situation awareness is the primary challenge to optimizing building movement strategies, prepared for the NIST Workshop on Building Occupant Movement during Fire Emergencies June 9–10, 2004, by Groner NE, John Jay College of Criminal Justice, City University of New York, Department of Public Management; 455 West 59th Street, New York, New York. 10019, e-mail: ngroner@jjay.cuny.edu. Groner (p. 2) goes on to state in his paper that*

_Progress in helping building management and emergency responders achieve situation awareness will require a fundamental change in how we approach the design of building protection systems. At present, our buildings are not well designed to achieve the needed level of situation awareness, despite the availability of many technological tools. Addressable detection devices can pinpoint the locations of detection of hazards, but the building interfaces used to display the information [do not supply an immediately comprehensible understanding of the situation. Technological devices like CCTV cameras and smoke detectors are not deployed in ways that help building management and emergency responders understand the status of key egress systems like stairs and corridors. Research and development towards the support of situation awareness in buildings is a priority._

One of the issues being discussed in the United States is whether high-rise buildings should be required to have a video surveillance system in each exit stairway. Such a system would facilitate real-time situation awareness of activity in stairwells during an emergency. Some have even advocated installing such a system in the “elevator lobby, elevator hoistway and elevator machine room to enhance situational awareness of emergency responders” (New International Building Code address fire safety and evacuation issues for tall structures. ScienceDaily. October 3, 2008. <www.sciencedaily.com/releases/2008/10/081003122707.htm>; December 26, 2008).

**The emergency management plan presented here addresses preparedness and emergency response but does not address business continuity.**

***A mutual aid agreement is “a pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement” (ASIS Business Continuity Guideline. Alexandria, VA: ASIS International; January 2005: 8).
Summary

- From the time a vehicle enters an office building parking structure and pedestrians proceed to the building, travel in the tower elevators, and enter an individual tenant space, there is a need for access control measures that sift out unwanted persons and intruders and yet constitute a minimum of inconvenience to legitimate building users.
- In multiple-tenant commercial office buildings, the three lines of defense—the main lobby, the elevators and lobbies on each floor, and the entrances to tenant space—provide points at which access can be controlled.
- Personal and business property that is moved in and out of an office building and tenant areas must be controlled. To establish a successful property removal control system, there must be supervised egress points through which all property and trash should pass. Tenants are a vital part of security and must be educated in security awareness.
- The purpose of establishing, implementing, and maintaining a building emergency management plan is to provide for the life safety of all building occupants.

Key Terms

Area of refuge. A designated area of safety for occupants inside or outside of a building. Also known as a safe refuge area and an area of rescue assistance inside a building.

Area of rescue assistance. “An area that has direct access to an exit, where people who are unable to use stairs may remain temporarily in safety to await further instructions or assistance during emergency evacuation.” Also known as an area of refuge or a safe refuge area inside a building.

Business continuity planning. “An interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption.”

Courier. A person or a company that delivers or picks up items such as documents, parcels, packages, or containers.

Credential. Something that entitles a person to certain rights or privileges.

Crisis. “An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.”

Crisis management. See emergency management.

Defend-in-place. A strategy that “recognizes that at times it is safer for occupants to remain in place within protected zones of a building than to evacuate the building.” Sometimes known as shelter-in-place.

Delayed evacuation. This strategy “takes advantage of temporary holding places, typically known as areas of refuge or areas of rescue assistance, where occupants can remain in relative safety, albeit near the fire area, for a period before evacuating the building, either by themselves or with assistance from emergency responders or others.”

Disability. “A physical or mental impairment that substantially limits one or more of the major life activities of such individual.” “People with physical disabilities rely on a variety of artificial means for mobility. Such devices range from canes and walkers to motorized wheelchairs.”

Disabled assistance monitor. A person who locates disabled/physically impaired and nonambulatory persons and assists them to the nearest “area of rescue assistance.” See area of rescue assistance.

Disruption. “An event that interrupts normal business, functions, operations, or processes whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a [power] blackout, terror attack, technology failure, or earthquake).”

Drill. “An exercise involving a credible simulated emergency that requires personnel to perform emergency response operations for the purpose of evaluating the effectiveness of the training and education programs and the competence of personnel in performing required response duties and functions.” See also fire drill.

Dumpster. “A large steel waste receptacle designed to be emptied into garbage trucks. The term is a generalized trademark of the Dumpster brand. The term is also common in Australia although Dumpster is not an established brand there. In British and Australian English, the terms wheelie bin and skip are more commonly used (although they are not perfect synonyms). In some other countries the more descriptive term frontloader container is often used, either in one or two words. In India it is called a garbage bin.”

Elevator monitor. Person who directs all passengers who arrive at his or her floor to proceed to the nearest safe stairwell and prevents any occupants from using the elevators for evacuation during a fire emergency.

Emergency. An “event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response.”

Emergency action plan (EAP). “Designated actions that employers, employees, and other building occupants should take to ensure they are safe from fire and other emergencies.” See also emergency management plan.
Emergency management. “The organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness [and] response.” Also known as crisis management.

Emergency management plan. “A scheme or method of acting or proceeding developed in advance for the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness and response.” Sometimes referred to as a fire safety plan or an emergency action plan.

Emergency operations center (EOC). “The physical location where an organization comes together during an emergency to coordinate response and recovery actions and resources. These centers may alternatively be called command centers, situation rooms, war rooms, crisis management centers, or other similar terms. Regardless of the term, this is where the coordination of information and resources takes place.”

Fire drill. A fire drill is an exercise for a simulated fire emergency. See drill.

Fire safety director. This person establishes, implements, and maintains the building emergency management plan. Sometimes known as the life safety director, life safety manager, building evacuation controller, or emergency coordinator.

Fire safety plan. See emergency management plan.

Fire warden. See floor warden.

Fire watch. Patrols at appropriate intervals determined by the fire department may be required when a building has exceptional hazards or the fire protection equipment or system is malfunctioning or has been taken out of service. A fire watch is “the assignment of a person or persons to an area for the express purpose of notifying the fire department and/or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety dangers.”

Floor plate. The entire floor area including the public access or common areas, tenant areas, and maintenance spaces.

---

51 United Nations International Strategy for Disaster Reduction. Terminology: Basic terms of disaster risk reduction. <www.unisdr.org/eng/library/lib-terminology-eng%20home.htm31March 2004>; July 8, 2008. The combined definition stated here uses a slightly modified version of the United Nations terminology. The UN definition states that emergency management is “the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness, response and rehabilitation.” The word rehabilitation has been removed. The reason for this is that for the purposes of this book, an emergency management plan addresses preparedness and response to an emergency and shortly thereafter. It does not deal with the rehabilitation process because, in the opinion of the author, that process is part of business continuity planning, which is “an interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption” (Business Continuity Planning. Wikipedia. <http://en.wikipedia.org/wiki/Business_continuity_planning>; July 9, 2008).


Floor warden. Key individual on each floor of a building whose primary duty is to ensure a safe relocation or evacuation of occupants or visitors from that floor (or part thereof) during an emergency. See also fire warden.

Incident. “event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization’s operations, services, or functions—which, if not managed, can escalate into an emergency, crisis, or disaster.”

Landlord. A person or an organization that owns a facility and leases or rents it, or a part of it, to a tenant(s).

Landslide. “The movement of rocks, debris or earth flowing down a slope.”

Lessee. “The tenant in a lease.” See also tenant.

Mobility impaired. “People with physical disabilities rely on a variety of artificial means for mobility. Such devices range from canes and walkers to motorized wheelchairs.”

Mutual aid agreement. “A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.”

Office building. A “structure designed for the conduct of business, generally divided into individual offices and offering space for rent or lease.”

Panic. “A sudden terror often inspired by a trifling cause or a misapprehension of danger and accompanied by unreasoning or frantic efforts to secure safety.”

Partial evacuation. “Immediate, general evacuation of the areas of the building nearest the fire incident. A partial evacuation may be appropriate when the building fire protection features assure that occupants away from the evacuation zone will be protected from the effects of the fire for a reasonable time. However, evacuation of additional zones may be necessary.” Also known as zoned evacuation or staged evacuation.

Phased evacuation. This strategy “provides for immediate, general evacuation of the areas of the building nearest the fire incident with continuing, selective evacuation of all other building areas…. Phased evacuation is total evacuation but not all at once.”

Plan. “A scheme or method of acting or proceeding developed in advance.”

Portable controlled descent device. See stair descent device.

---


57 Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:94.


60 Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:120.


63 ibid., pp. 4–104, 4–105.

Rent. “Payment for the use of space or personal property owned by another. In real estate, a fixed periodic payment by a tenant to an owner for the exclusive possession and use of leased property.”

Runners/messengers. Persons who provide physical liaison in the areas normally covered by the telephone monitors when there is a failure of telephone communications.

Safe refuge area. A designated area of safety for occupants inside or outside of a building. Also known as an area of refuge and an area of rescue assistance.

Search monitor. A person who systematically and thoroughly searches all assigned floor areas in a building to ensure that all occupants leave during an emergency evacuation.

Self-evacuation. “Occupants evacuating by themselves, before emergency responders have arrived on site, using available means of evacuation, i.e. elevators and stairs.”

Shelter-in-place. See defend-in-place.

Situation awareness. “The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.”

Solicitor. A person who approaches building occupants with the intent to sell something, to ask for business for a company, to request charitable contributions, or to obtain magazine subscriptions. This definition would include people who beg or panhandle for money or food.

Stack effect. “Results from the temperature differences between two areas, usually the inside and outside temperatures, which create a pressure difference that results in natural air movements within a building. In a high-rise building, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke through the building.”

Staged evacuation. See partial evacuation or zoned evacuation.

Stair descent device. Used during emergencies to assist physically impaired persons to travel down building stairs. Such equipment includes stairway evacuation chairs and portable controlled descent devices. The latter are not to be confused with various types of harnesses, chutes, and platforms designed to evacuate occupants down the outside of a building.

Stairwell monitor. A person who lines up occupants in an orderly fashion at the entrance to the stairwell, organizes an orderly flow of persons into the stairwell when evacuation begins, and closes the stairwell door when no one is moving through it.

Suite warden. A key individual of an office suite whose primary duty is to ensure a safe relocation or evacuation of occupants or visitors from the suite during an emergency.

---

65 Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:146.


Tabletop exercise. “A test method that presents a limited simulation of an emergency or crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.”

Telephone monitor. A person who provides telephone liaison between the floor warden and floor response personnel, liaison between the floor warden and the fire safety director or the fire department, and liaison between floors.

Tenant. A person, a group of persons, or a company or firm that rents or owns, and occupies space within a building. “A legal term for one who pays rent to occupy or gain possession of real estate; the lessee in a lease. Real estate managers often limit the use of the term tenant to commercial tenants and refer to residential tenants as residents.”

See also lessee.

Tenant information manual. See tenant manual.

Tenant manual. “A compilation of management policies and procedures that relate to commercial tenants and the use of their leased space.” See also tenant information manual.

Testing. “A set of problems, questions, for evaluating abilities, aptitudes, skills, or performance. The means by which the presence, quality, or genuineness of anything is determined.”

Total evacuation. This strategy involves the simultaneous evacuation of all building occupants to an outside area of refuge or safety.

Train. “To give the discipline and instruction, drill, practice, designed to impart proficiency or efficiency.”

Visitor. In office buildings, it is a nonoccupant who spends time at the building. In hotel buildings, it is a nonguest who visits a hotel guest or uses its facilities (such as meeting rooms, conference facilities, recreational facilities, restaurants, bars, a casino, or a discotheque). In residential and apartment buildings, it is a “nonresident who spends time at the home of a resident (with that resident’s consent) but does not stay overnight.” In a mixed-use building, it could be all the preceding depending on the nature of its occupancies.

Zoned evacuation. “Immediate, general evacuation of the areas of the building nearest the fire incident. A partial evacuation may be appropriate when the building fire protection features assure that occupants away from the evacuation zone will be protected from the effects of the fire for a reasonable time. However, evacuation of additional zones may be necessary.” Also known as partial evacuation or staged evacuation.

72 ibid.
74 ibid.
75 Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:182.
Additional Reading


Broadly classified as the lodging industry, the term hotel is "an all-inclusive designation for facilities that provide comfortable lodging and generally, but not always, food, beverage, entertainment, a business environment, and other ‘away from home’ services.”

Included among these “away from home” guest room services are room cleaning; laundering of bed linen and bathroom towels (and dry cleaning of personal clothing if required); toilet and bathing facilities; telephone and network communications; bedding, furniture, and sometimes a refrigerator and cooking facilities (such as a coffee machine, a stove, a microwave, and common-area vending machines); in-room dining; and in-room entertainment in the form of radio and television.

“The hotel may be a high-rise building or part of a larger high-rise office complex.” It may also be a conference hotel with multipurpose meeting facilities designed for large-scale gatherings; a casino hotel where patrons can play slot machines, gamble on card games, dice, and roulette, and bet on sporting events; or a resort hotel with “a campus-style setting offering skiing, golf, boating, horseback riding, and other activities.” Some hotels are even attached to amusement parks.

If the hotel shares a building with other separate occupancies, such as offices and apartments or residences (including hotel-residences), it is considered to be a mixed-use building (which is addressed in Chapter 12).

This chapter addresses high-rise hotel buildings. To systematically examine the security and fire life safety of such buildings, this discussion addresses the following areas: occupancy characteristics; assets, threats, vulnerabilities, and countermeasures; security programs; and emergency planning.
Occupancy Characteristics

“Today’s hotels may offer a variety of services and activities for their transient and permanent guests. A traveler who is staying at a hotel for a limited period of time is commonly described as a guest. Besides providing for lodging and meals, hotels usually have newsstands, retail shops [such as boutiques], restaurants, cocktail lounges, [coffee bars,] health clubs, concierges, and other quality services [which may include laundry and dry cleaning services and business centers with high-speed Internet connections]. Generally, parking facilities are available [many of which include self-park and valet service]. Some have recreational facilities, such as saunas [spas/hot tubs,] and swimming pools, while others may offer tennis and racquetball courts, gyms, and exercise rooms.”

According to Bell,

[Hotels] are unique in that they almost always combine several different occupancies under one roof. In addition to guest rooms or guest suites, which are residential occupancies, hotels usually provide space for assembly occupancies such as ballrooms, meeting rooms, exhibition halls, and restaurants; or mercantile * occupancies such as shopping areas, gift shops, and other retail areas; and offices and commercial establishments, or business ** occupancies.

...Many large hotels also contain industrial-type laundries and dry cleaning facilities, as well as kitchens, which use large broilers, ovens, and deep-fat fryers.

Larger-scale hotel building configurations often have atria two or three stories high and sometimes up to sixty stories high, which are often the focal point of building design. Atrium areas themselves may include several occupancies or mixed functions associated with hotel operations [on lower floors these consist of restaurants and retail establishments (and possibly the main reception area), and on upper floors they consist of guest rooms located on corridors that face the open space of the atrium].

Some structures also may include parking facilities which may be open, enclosed, above- or below-ground, and often directly beneath or adjacent to the hotel itself. These arrangements may require special types of fire protection, and the building codes may require fire separations.

“Limited-service hotels are free-standing properties that do not have on-site restaurants or most other amenities that must be provided by a staff other than the front desk or housekeeping. They usually offer continental breakfasts, vending machines or small packaged items, Internet access, and sometimes unattended game rooms or swimming pools in addition to daily housekeeping services.”

---

4 ibid.


**A business occupancy is “an occupancy used for the transaction of business (other than those covered under ‘mercantile’) for the keeping of accounts and records and for similar purposes.” ibid.


The number of occupants in hotels will vary according to the day of the week (including whether it is a weekend or holiday), time of the day, and the season or time of the year. Early in the day, because most guests are generally required to check out by approximately noon each day, there may be higher numbers of people in the reception area around that time. If the hotel caters to a large number of businesspeople, there may be more guests checking in at the reception areas late in the afternoon and early in the evening, particularly on Sundays through Thursdays. The types of amenities and services offered by the hotel will also affect the number of persons in hotel common areas. For example, if there are restaurants, bar facilities, function rooms, banquet rooms, and exhibition halls, there may be high concentrations of people around break times, meal times, evening hours, or when meetings and special events are being held. Of course, during the early hours of the morning, when these facilities are usually closed and many guests are sleeping, the number of people in hotel common areas will be much lower.*

Generally speaking, individual hotel buildings are managed by one group; this will consist of a general manager, assistant managers, department heads, and administrative staff, plus support staff such as PBX operators,** receptionists, bell captains, concierge staff, valet parking attendants, hotel limousine drivers, housekeepers, laundry staff, engineers, security personnel, and, particularly in larger facilities, kitchen and catering personnel, gardeners, electricians, plumbers, carpenters, painters, elevator technicians, and others associated with hotel operations. The actual number of staff members will vary according to the size of the hotel, the services that it offers, the complexity of its operations, and the security needs of each individual facility.

During normal business hours (i.e., Monday to Friday, during the daytime), usually the general manager will be on duty; after hours (i.e., Monday to Friday, late afternoon until the next morning; weekends and holidays), an on-duty manager will usually be present.

During the daytime hours (particularly from morning to early to mid-afternoon) when guest rooms are being cleaned and refurbished with supplies, usually there is a higher concentration of housekeeping staff. After hours, most hotels (except large ones, such as those that provide special facilities such as ballrooms, meeting rooms, exhibition halls, restaurants, and gambling casinos) have fewer engineers, maintenance personnel, and other support staff on duty; although, the number of security staff members may increase (again, staffing needs will vary according to the size of the hotel, the services that it offers, the complexity of its operations, and the security needs of the facility).

### Assets, Threats, Vulnerabilities, and Countermeasures

A risk assessment (as detailed in Chapter 4) is an important tool for developing an appropriate security and fire life safety program for a hotel. A “risk assessment analyzes

---

* A notable exception will be where gambling casinos are situated on the premises. In this case, there may be large numbers of patrons in these areas at all hours of the night, particularly on weekends and public holidays.

** A PBX operator, sometimes called a switchboard operator, greets people telephoning a hotel. These operators answer callers’ questions, provide guidance, and direct calls to various hotel departments. Also, they handle guest inquiries and arrange wakeup calls. As well as these communications services, they may also be responsible for monitoring the hotel’s fire life system. (“So, you want to be a PBX operator?” by Jenifyr Bedard interviewing Donna Bigerton, PBX Operator, The Ritz-Carlton-Palm Beach, Manalapan, FL. <www.PalmBeachPost.com>; June 29, 2008).
the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require mitigation measures [countermeasures], but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with identified vulnerability, allow prioritization of resources to implement mitigation measures."

Key steps in the process involve examining the assets, the threats against the assets, the vulnerabilities of the assets, and the countermeasures or mitigation measures that can be used to address identified vulnerabilities of the assets (within the confines of risk management). These areas are now examined for hotel buildings. (Although it addresses many areas, the scope of this chapter does not include accounting measures such as credit and billing procedures, inventory controls of items such as guest towels and sheets, alcohol and food, or detailed lodging property’s rights and duties, liability, and insurance matters.)

Assets

Tangible assets in hotels include the lives of guests, visitors, contractors, vendors, and the hotel staff; guest’s personal property; and the building itself, its fittings, and its equipment. Building equipment includes the electrical, water, gas, mechanical, heating, ventilating, air-conditioning, lighting, elevator, escalator, communication, security, and fire life safety systems. In addition, there are other types of assets that may include telephones, computers, printers, fax machines, photocopiers, and audio-visual equipment (including radios and televisions in guest rooms, foyers, restaurants, and bars), equipment in meeting rooms and business and conference centers, housekeeping supplies, and general-use items (refrigerators, coffee machines, stoves, microwaves, furniture, and common area vending machines), and sometimes antiques and works of art, cash and negotiable instruments (particularly in the reception area, restaurant, bar, retail shops, and shop inventory warehouse), and high-value merchandise (such as liquor in the hotel liquor vault and silverware in storage rooms). In addition, there may be assets in kitchens, laundries, dry cleaning facilities, fitness centers, saunas, swimming pools, spas/hot tubs, tennis and racquetball courts, dining areas, restaurants, retail shops, newsstands, business centers, and other facilities for guest services, as well as vehicles parked in the facility’s parking garage.

Intangible assets include the livelihood of hotel guests, visitors, contractors, vendors, and the hotel staff; intellectual property and information stored in paper files, reference books, and within computer systems and peripherals; and the reputation and status of the hotel.

Threats

The types of security and fire life safety threats to hotel building assets are outlined in Chapter 3. Briefly they include the following:

- **Security threats to people**: assault, assault and battery, kidnapping, manslaughter, mayhem, murder, robbery, sex offenses (including rape, sexual harassment, and lewd behavior), and stalking.

---

• **Security threats to property and information:** aberrant behavior, arson, burglary, cyberattack, disorderly conduct, espionage, larceny, sabotage, theft, trespass, and vandalism. In addition, there may be the disruption of building utilities such as water; electrical power; natural gas; sewer; heating, ventilation, and air-conditioning (HVAC); telecommunications; security; and fire life safety systems. Some security threats may involve terrorism.

• **Security threats to people and property:** bombs, chemical and biological weapons, civil disturbance, fires, hazardous materials, natural disasters, and nuclear attack.

• **Life safety threats:** aircraft collisions; bombs and bomb threats; daredevils, protesters, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstrations, and civil disorder; medical emergencies; natural disasters (earthquakes, tsunamis, volcanoes, heat waves, storms, and floods and landslides); contractible diseases (pandemic influenza, severe acute respiratory syndrome, and tuberculosis); power failures; slip-and-falls; stalking and workplace violence; traffic accidents; and water leaks.

**Threats to Guests**

“Providing security in a hotel or motel is the broad task of protecting people—guests, employees, and others—and assets. Crimes involving the theft of assets usually result in greater losses to lodging properties than crimes against persons, but crimes against persons have a greater effect on public relations (and therefore occupancy) and may generate high legal expenses.”

According to Kaminsky,

> Innkeepers are held to the highest standard of care of all landlords…. Hence, when a guest at a hotel or motel is the victim of a crime, the landowner is confronted with a very difficult lawsuit. Aside from the elevated standard of care issue, there is something inherently frightening about crimes committed in a hotel or motel; victims are often hundreds of miles from home—often on business trips to an unfamiliar city—and they have to put their safety in the hands of the innkeeper. Jurors can easily relate to this scenario, and the defense should expect that jurors will have little tolerance for crimes committed in hotels or motels.  

---


* An innkeeper is the landlord of an inn or a lodging facility.

** In law of negligence, [standard of care is] that degree of care which a reasonably prudent person should exercise in same or similar circumstances. If a person’s conduct falls below such standard, he may be liable in damages for injuries or damages resulting from his conduct” (Publisher’s Editorial Staff. *Black’s Law Dictionary.* 6th ed. [Nolan JR, Nolan-Haley JM, co-authors] St. Paul, MN: West Publishing; 1990:1404, 1405).

According to Callaghan,

_The lodging industry is somewhat different from other businesses in that customers are present 24 hours per day, seven days a week, in effect living with hotel proprietors. The close proximity of customers, as well sometimes-informal situations in which they find themselves, can lead to problems. These include a myriad of incidents that can be referred to as acquaintance assaults. Examples are two people sharing a room who are fighting with one another, people meeting and getting into an argument in a lounge area, and incidents where one guest reports that he or she was sexually assaulted by another. These crimes often occur without witnesses._

“There is the possibility that an assailant who victimized a guest followed the victim back to the [guest] room after encountering him or her elsewhere. There will be many instances when criminals readily spot out-of-state visitors, either in tourist areas or other locations, and target them at that time.” Such crimes may lead to attacks in hotel parking garages, as well as in the hotel itself.

Also, “crimes of opportunity” such as confidence tricks may occur against guests and patrons in hotel lobbies, restaurants, bars, casinos, and other facilities.

**Threats from Guests and Employees**

“While recognizing the need for the protection of the guests, the employees, and the assets of each, management must also recognize that guests and employees may themselves create security problems by stealing property and services from the hotel.” For example, thefts and check and credit card fraud may occur at the front desk, in bars, restaurants, retail stores, casinos, recreation facilities, and any other hotel facilities that handle money transactions. As Beaudry commented,

*Incidents involving “walk-outs” are common when nonpaying customers enjoy a meal and/or drinks in a hotel and then proceed to leave without offering to*

---


“[S]uch cases, where the assailant targets the guest at a different location through no fault of the hotel or motel and simply follows the target back to the premises, [may be used by the defense in a premises security action to] raise the issue of causation. Many jurisdictions deem such directed attacks as intervening and/or superseding events that break the causal chain between the landowner’s alleged—and often actual—negligence and the attack on the victim” (Kaminsky A. A Complete Guide to Premises Security Litigation. 2nd ed. Chicago, IL: American Bar Association; 2001:71). Causation is “the fact of being the cause of something produced or of happening” (Publisher’s Editorial Staff. Black’s Law Dictionary. 6th ed. [Nolan JR, Nolan-Haley JM, co-authors] St. Paul, MN: West Publishing; 1990:221).

AA confidence trick “or confidence game, more often known as a con, scam, swindle, grift, gaffle, bunko, flim flam, stratagem, or scheme, is an attempt to swindle a person or people (known as the ‘mark’ or sometimes ‘griftee’) which involves gaining his or her confidence” (Wikipedia. <http://en.wikipedia.org/wiki/Confidence_trick>; August 4, 2008).

pay for items consumed.... Frequently, if the patron is caught leaving, they can be confronted and—if they refuse to pay—be held long enough for security or the public police to arrive. The thief then can be identified for future reference or prosecution. The amount of loss is usually not worth the time required to prosecute, so it is recommended that the name and description of the individual be recorded and distributed to all outlets in the hotel. You may also try alternate means of payment (e.g., having a family member pay, or requesting [a] form of payment like cash). If the person tries to obtain food or drink again, they can be refused until they pay for the previous bill....

The security department must face problems ranging from guests using stolen credit cards and cards over their allowable limit to dishonest employees inflating gratuities or even writing in gratuities. The best means of avoiding these and other scams is to develop detailed policies and procedures for authorization of use, and to train employees to follow the procedures. Charging store merchandise [and meals in hotel restaurants and services in recreation facilities] to a guest room, for example, must somehow be verified first [by, say, requesting photo identification and the room key or keycard itself]. Management must then follow up to ensure compliance with the rules, and violators should be dealt with appropriately.13

In addition, guests may steal items from their room (such as alcohol and food items from in-room containers, bathing towels, bed linen, bathing robes, hair dryers, coffee pots, television sets, clock radios, computer peripherals, artwork, light fixtures, and, as unlikely as it may seem, even furniture), cutlery and china from in-room dining carts (particularly those left in the corridors outside of guest rooms), tableware from hotel dining areas, and various items left unsecured in meeting and banquet rooms, exhibition halls, recreational areas, and other facilities.

In addition, there may be other security- or crime-related incidents—such as illegal gambling and prostitution—that occur in guest rooms. These crimes involve the guest knowingly inviting the participant to his or her hotel room. In the case of the latter, prostitution, Beaudry noted,

Some of the comments frequently heard about prostitution [are] that it is a victimless crime and that society should not care what consenting adults do in privacy. However, prostitution is a problem that, if not controlled, can ruin a hotel's reputation. The word controlled was used intentionally, for prostitution cannot and will not be eliminated. The security objective should be to reduce such activity to an absolute minimum. A hotel's reputation is, without doubt, its single most important asset. No matter how professional the hotel's services may be or how good a value may be offered, no one respectable will stay at your hotel if this type of activity is allowed to take place openly.

It is not the prostitutes (both males and females) that are in and of themselves a concern, but rather the peripheral activity that frequently accompanies prostitution. Theft of the guest's property, assaults on the guests, and

drugs are only a sample of the concerns associated with this crime. It is in the best interest of the hotel operator and guest alike to control prostitution.

There are a number of simple control methods a hotel can employ. First, guest registration procedures must be established and followed closely. All guests must be required to show valid photo identification such as a driver’s license and preferably a credit card when checking in, even if they are paying cash in advance for their stay. The reason for the tight registration process is that most streetwalkers will not carry identification. The more sophisticated “call girl” or “escort” type of prostitute will have identification, but he or she also represents less of a threat to the innkeeper.

The second method of control can be utilized in properties that have computerized front desk procedures and can print out a complete list of all guests by room as well as list the number of occupants registered in that particular room. Once given that list, particularly at night when guests are returning to their rooms with visitors they may have just met in a local bar, the security officer can screen all incoming guests at the front door. (This works very well when hotel policy regarding visitor access after a certain hour is implemented.) This method has two benefits. First, the innkeeper [may be] entitled as a matter of law to additional revenue if a second person is staying in the room. Second, if in fact the “visitor” is a streetwalker, not only will she or he not have identification as noted above, but the guest may or may not want to risk having a second person listed on the registration folio.

The final two methods of prevention include employee cooperation. The housekeeping department will know if a certain guest room has heavy traffic going to and from it and can alert security. Secondly, hotel managers must maintain a no-tolerance attitude towards prostitution while supporting security in its efforts to deal with the problem. Common meeting places for prostitutes are lobby pay telephones [now less frequent due to the advent of mobile telephones], bars, and easily recognized hotel fixtures such as chairs, plants, and the like.

Sometimes, hotel staff may even be involved in the prostitution activities. “In some cases, employees working in collusion with the front desk or even with security staff members have provided prostitutes to guests.” If the problem cannot be adequately dealt with, hotel management, in consultation with legal counsel, may want to seek the cooperation of local law enforcement.

*Of course, the tight registration process requiring photo identification and a valid credit card is for purposes other than that of prostitution. For example, if the guest is a victim of an accident, a crime, or a medical incident that renders him or her unconscious, dead, or missing, such information will be crucial in contacting next of kin, reporting to law enforcement and medical authorities, and so on. Also, it will assist in investigation of the guest not paying the hotel bill, including guest services, or may provide information if he or she is suspected of committing a crime.


The sale and use of illegal drugs by guests can also occur in hotels. According to Beaudry,

_It is very unlikely that a hotel manager will be able to prevent a guest from using drugs in the privacy of his or her room. If, however, the manager becomes aware of such use, action should be taken. Limited use (e.g., smoking a marijuana cigarette) may best be handled by warning the guest that repeated activity will result in removal from the hotel. However, evidence of a more serious use (such as large parties with cocaine left out in the open) may require assistance from the local police. It is common for drug dealers to use large urban hotels to conduct their drug deals, for the size of the hotel usually will ensure their anonymity._

In addition, the potential also exists for a guest room to be set up as a temporary, mobile laboratory manufacturing illicit drugs such as methamphetamine.*

A room can even be used for “surreptitious meetings among dangerous persons such as [gangsters,] terrorists, and drug dealers.” Of course, due to the openness of hotels, this is difficult to prevent.

“Large hotels host large parties, weddings, reunions, conventions, conferences, [exhibits], seminars, sales meetings, and the like. Employees, especially the event planner, regularly face a myriad of crime- and security-related incidents.” Sometimes, problems arise when large groups that are traditionally antagonistic to each other have events at the hotel at the same time. Often, the excessive use of alcohol or drugs can be the trigger for incidents to occur.

“Depending on the size and location of a hotel, certain types of public figures are likely to stay as guests on occasion. In larger, convention-class hotels, political figures are often in attendance for social events. Public figures, whether they are politicians or people such as rock stars or sports teams, often will draw crowds. These crowds may be admirers, or they may be demonstrators protesting the appearance of the individual…. [T]he security manager should be prepared to work with the authorities in planning for the person’s arrival, stay, and departure.” Additional hotel security staff will often be required to handle these occasions.

---

*According to Ruda Maxa for Marketplace, “If you happen to get a whiff of ammonia in the hallway of a long-term-stay hotel, you might want to pick up the phone and make a few calls. That’s because over the past several years, in states including Arkansas, Texas and California, bad guys have used these hotels for makeshift methamphetamine [meth] labs. Last August, just such a lab blew up at a Quality Inn and Suites in Arlington, Texas, demolishing 60 of its 100 rooms and causing more than $1 million in damage. If you happen to be the next guest in a hotel room used to make meth, just touching an ammonia-saturated bedspread, curtain or carpet can burn your skin, eyes or respiratory tract…. Hotels can shell out thousands just to clean carpeting, bedding, curtains and even drywall before throwing it all away. That’s why hotels are training staffs to recognize suspicious guests, especially ones who decline regular housekeeping service” (“Is the hotel room next door a meth lab?” January 12, 2005. <www.rudymaxa.com/radio.php?CommentaryID=19>; August 2, 2008).


18 Ibid.

Notable Incidents
Some notable incidents\(^20\) that have occurred in high-rise hotels are shown in Table 10–1.

Fire Risk in Hotel Buildings
Fire is a constant risk in high-rise hotel buildings. “Since hotel guests are [primarily] transients, special consideration must be given to the potential threat to their life safety from fire. For example, occupants of the residential portion of a hotel sleep in unfamiliar surroundings and could possibly become disoriented when trying to evacuate under heavy smoke conditions. Likewise, persons in ballrooms, lounges, [casinos,] and restaurants could become disoriented due to low-level lighting, crowd size, and unfamiliarity with evacuation routes.”\(^21\)

In discussing fire risk,\(^*\) it is helpful to analyze fire incident data\(^**\) for the four property classes—office buildings, hotels and motels,\(^***\) apartment buildings, and hospitals (and other facilities that care for the sick)—that account for the majority of high-rise building fires.\(^22\) Even though this data pertains only to the United States, it is worth considering because it includes the types of commercial buildings that are addressed in this book (namely, office, hotel, residential and apartment, and mixed-use buildings).

A study by Dr. John Hall, Jr., of the National Fire Protection Association’s (NFPA) Fire Analysis and Research Division, using statistics from the U.S. Fire Administration’s National Fire Incident Reporting System (NFIRS), stated that from 1987 to 1991, office buildings, hotels and motels, apartment buildings, and facilities that care for the sick...
According to the New York Times, “No precise number of casualties for the Marriott exists, but it is likely, based on eyewitness accounts analyzed by the New York Times, that no fewer than 50 people inside the hotel were killed. At least 41 of those were firefighters, and the number could be much higher. Besides Mr. Keller [Joseph Keller, the executive housekeeper], another Marriott employee, Abdu A. Malahi, was killed. As for guests, 11 of the 940 registered guests that day were ‘unaccounted for,’ said Cathy Duffy, a spokeswoman for Marriott. It is not known if they died in the building or were elsewhere in the complex” (Dwyer J, Fessenden F. One hotel’s fight to the finish; At the Marriott, a portal to safety as the Towers fell. The New York Times, September 11, 2002. <http://query.nytimes.com/gst/fullpage.html?res=9B07EFD81431F932AC0A9649C8B63> • March 16, 2009).

Such a coordinated attack on a hotel is difficult to protect against due to the open access of most hotels throughout the world.

<table>
<thead>
<tr>
<th>Date</th>
<th>Building</th>
<th>Incident</th>
<th>Persons Killed/ Injured</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 7, 1946</td>
<td>Winecoff Hotel, Atlanta, Georgia</td>
<td>Fire</td>
<td>119 killed, 91 injured</td>
</tr>
<tr>
<td>January 26, 1969</td>
<td>Victoria Hotel, Dunnville, Ontario, Canada</td>
<td>Fire</td>
<td>13 killed</td>
</tr>
<tr>
<td>December 25, 1971</td>
<td>Taе Yon Kak Hotel, Seoul, South Korea</td>
<td>Fire</td>
<td>163 killed (greatest loss of life in a hotel building fire)</td>
</tr>
<tr>
<td>September 1, 1973</td>
<td>Copenhagen Hotel, Denmark</td>
<td>Fire</td>
<td>35 killed</td>
</tr>
<tr>
<td>November 21, 1980</td>
<td>MGM Grand Hotel, Las Vegas, Nevada</td>
<td>Fire</td>
<td>85 guests and hotel employees killed, approximately 600 injured</td>
</tr>
<tr>
<td>December 31, 1980</td>
<td>Dupont Plaza Hotel &amp; Casino, Puerto Rico</td>
<td>Fire</td>
<td>97 killed (84 in the casino), more than 140 injured</td>
</tr>
<tr>
<td>February 10, 1981</td>
<td>Las Vegas Hilton Hotel, Las Vegas, Nevada</td>
<td>Fire</td>
<td>8 killed, 350 injured</td>
</tr>
<tr>
<td>October 18, 1984</td>
<td>Alexander Hamilton Hotel, Paterson, New Jersey</td>
<td>Fire</td>
<td>15 killed, more than 50 injured</td>
</tr>
<tr>
<td>July 11, 1997</td>
<td>Royal Jomtien Resort, Pattaya, Thailand</td>
<td>Fire</td>
<td>91 hotel guests and staff killed, 51 injured</td>
</tr>
<tr>
<td>September 11, 2001</td>
<td>Marriott World Trade Center Hotel (WTC 3) at New York World Trade Center, New York</td>
<td>Collapse of New York WTC Twin Towers</td>
<td>2 hotel employees killed</td>
</tr>
<tr>
<td>May 8, 2002</td>
<td>Sheraton Hotel, Karachi, Pakistan</td>
<td>Car bomb</td>
<td>14 killed (including 11 French engineers, 3 Pakistanis)</td>
</tr>
<tr>
<td>November 28, 2002</td>
<td>Hotel Mombassa, Kenya</td>
<td>Car bomb</td>
<td>13 killed (including 3 Israelis)</td>
</tr>
<tr>
<td>August 5, 2003</td>
<td>JW Marriott Hotel, Jakarta, Indonesia</td>
<td>Car bomb</td>
<td>11 killed (including 2 Americans), 144 injured</td>
</tr>
<tr>
<td>September 20, 2008</td>
<td>Marriott Hotel, Islamabad, Pakistan</td>
<td>Truck bomb</td>
<td>53 killed, more than 250 injured</td>
</tr>
<tr>
<td>November 26, 2008</td>
<td>Taj Mahal Palace and Tower Hotel and the Oberoi Hotel, ** a train station, a Jewish Center, a movie theater, and a hospital, Mumbai, India</td>
<td>Machine guns, hand grenades, and military-grade explosives</td>
<td>171 killed (including 6 foreigners), and more than 300 injured</td>
</tr>
</tbody>
</table>
averaged 13,800 high-rise building fires per year and associated annual losses of 74 civilian deaths, nearly 720 civilian injuries, and $79 million in direct property damage. However, “most of these high-rise building fires and associated losses occurred in apartment buildings.”

Hall added that for this period,

- Only a small share of high-rise building fires spread beyond the room of origin, let alone the floor of origin.
- In high-rise buildings [office buildings and hotels and motels], electrical distribution system fires rank first in causes of fire-related property damage.

The most recent published study by Hall shows that “in 2002, high-rise buildings in these four property classes combined had 7,300 reported structure fires and associated losses of 15 civilian deaths, 300 civilian injuries, and $26 million in direct property damage.” He concluded that “these statistics generally show a declining fire problem over the nearly two decades covered” and, similar to his previous findings, “most high-rise building fires and associated losses occur in apartment buildings.”

However, Hall did caution that, due to a number of factors (one being lower participation in national fire incident reporting in recent years), “the patterns shown in data available so far should be given limited weight.”

It is worth noting here that, as previously mentioned, some buildings, particularly “larger-scale hotel building configurations often have atria two or three stories high and sometimes up to sixty stories high, which are often the focal point of building design. Atrium areas themselves may include several occupancies or mixed functions associated with hotel operations.”

The presence of an atrium constitutes a fire risk. If a fire occurs on the lower floors of the atrium (for example, in a restaurant or a retail space), then the resulting smoke and heat can rise up through the atrium and possibly reach guest rooms on upper floors located on corridors that face toward the atrium). To reduce this risk, according to Brannigan and Corbett,

Building codes specify numerous requirements for atria: full sprinkler protection throughout the building (with the exception of the top of the atrium itself if it is more than 55 feet [16.8 meters] above the floor because it is felt that sprinklers will not activate so high above the floor), a smoke control system to minimize the movement of smoke onto the adjacent floors to the atrium and to move the smoke out of the building, and standby power for the building.

---


24 Ibid., p. 53.

25 2002 is the most recent year for which data was available for this report.


27 Ibid.

28 Ibid., p. 4.

29 Ibid., p. 3.

30 Ibid., p. 4.

In addition, the fire code requires that the floor of the atrium be limited to “low” fire hazards. Author Corbett has seen this violated many times with moderate and high fire hazards such as live, cut Christmas trees; propane grills in food kiosks; and large plastic displays. This provision is difficult to enforce (hence the desire for sprinklers at the top of tall atria).\(^\text{32}\)

It is worth noting here that in his book, *High Rise/Fire and Life Safety*, O’Hagan stated that high-rise residential building fires, including those in hotel rooms, to some extent are different in nature and not as severe as fires in high-rise office buildings (see earlier discussion in Chapter 2). Two of his stated reasons for this position are (1) high-rise residential buildings are typically of masonry construction and lack the empty spaces between the interior of their exterior walls and the outer edges of their floors (that typify the curtain walls of steel-framed [core construction] buildings) and (2) for privacy and usage reasons, residential buildings are typically compartmentalized with walls and partitions that have adequate fire resistance to withstand the fire until the arrival of the fire department; as a result, individual fires are considerably smaller in area.\(^\text{33}\)

### Vulnerabilities

Weaknesses that can make an asset (in this case, a hotel building and its operations) susceptible to loss or damage\(^\text{34}\) will largely depend on the building itself and the nature of its operations. A vulnerability assessment is required to “evaluate the potential vulnerability of the critical assets against a broad range of identified threats/hazards.”\(^\text{35}\) (See Chapter 4.)

“Lodging property security efforts may involve such areas of concern as guestroom security, key control, locks, access control, perimeter control, alarm systems, communication systems, lighting, closed-circuit television, safe deposit boxes, inventory control, credit and billing procedures, computer security, staffing, pre-employment screening, employee training, responsible service of alcoholic beverages, emergency procedures, safety procedures, record keeping, and more.”\(^\text{36}\)

### Countermeasures

Mitigation measures to counteract the identified vulnerabilities of an asset to a threat may consist of security systems and equipment (see Chapter 5), fire life safety systems and equipment (see Chapter 6), security personnel (see Chapter 7), security policies and procedures (see the next section, “Security Programs”), and emergency management (see the later section, “Emergency Planning”). These countermeasures need to be looked

---


at in terms of security design. “Security design involves the systematic integration of design, technology, and operation…. The process of designing security into architecture is known as Crime Prevention Through Environmental Design (CPTED).” As mentioned previously, the key to selecting appropriate countermeasures for a particular facility is for a risk assessment to be conducted. (See Chapter 4.)

According to Kaminsky,

Though hotels and motels have a duty to provide security, innkeepers cannot prevent all crimes from occurring on their premises, despite their best efforts. Neither are they ensurers of the safety of people on their premises. If there is adequate lighting, working locks, properly trained and deployed security officers, video surveillance, and other security measures or some combination of these in place, the chances of a favorable defense verdict in a premises security case are significantly increased. On the other hand, if any of these security measures are lacking or improperly implemented, the chances of an adverse outcome are heightened.

Because fire is a risk in high-rise buildings, the following is noted regarding their fire protection features: hotel buildings that have properly designed, installed, operated, tested, and maintained automatic fire detection and suppression systems and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes and automatic smoke control systems to restrict the spread of smoke—do have the necessary early warning systems to quickly detect fires and warn occupants (including guests and visitors) of their presence; they also have the necessary automated sprinkler systems to quickly extinguish a fire in its early stages. One of the key issues here is the presence or absence of sprinklers.

In the study mentioned in the previous section, “Threats,” Hall commented on fire protection in high-rise buildings by stating,

In several instances, the value of these fire protection features [i.e., automatic extinguishing systems (primarily sprinklers), fire detection equipment, and fire-resistive construction] may be seen clearly in a statistical analysis of 1994–1998 loss per fire averages, with and without the protection. For high-rise buildings, automatic extinguishing systems are associated with a reduction of at least 88% in the rate of deaths per 1,000 fires for each of the three property classes (excluding office buildings, which had no deaths recorded in NFIRS [National Fire Incident Reporting System] in high-rise buildings) and at least 44% in the average dollar loss per fire for each of the four property classes....

---


Automatic extinguishing systems and fire detection equipment and the compartmentation features associated with fire-resistive construction all contribute to fire protection by helping to keep fires small, with extinguishing and construction doing so directly and detection doing so by providing early warning that can lead to earlier manual suppression.  

Security Programs

Security programs for hotels and for individual guests and patrons involve policies, rules and regulations, and procedures designed “to prevent unauthorized persons from entering, to prevent the unauthorized removal of property, and to prevent crime, violence, and other disruptive behavior.” Security’s overall purpose is to protect life and property. “Because hotels offer such diversity of facilities and activities, no one security program will fit all properties. The security program must be designed to fit the needs and characteristics of the individual hotel. While crime is not always preventable, certain policies and procedures, properly implemented, may deter or discourage criminal activity.”

“Every establishment has to find the right balance for its environment—weighing the benefits of security against the extent to which each measure will inconvenience guests.”

Hotel Building Access Control

There are many different people who may, at any one time, wish to enter a hotel building. They include hotel owners and management staff, hotel contractors (such as elevator technicians and engineering, maintenance, security, janitorial, and parking personnel), guests, visitors, salespersons, tradespeople (including construction workers, electricians, plumbers, carpenters, gardeners, telecommunications repair persons, persons replenishing vending machines, and others who service equipment within the hotel), building inspectors, couriers, delivery persons, solicitors,* sightseers, people who are lost, vagrants or homeless people, mentally disturbed individuals, vandals, suicidal persons, protestors, and daredevils. There may also be others who try to enter hotel parking areas, retail shops, restaurants, cocktail lounges, health clubs, business centers, recreational facilities, gyms, exercise rooms, function rooms, meeting rooms, or an individual guest room, with the sole purpose of committing a crime.

It is primarily the hotel owner and operator who determine the access control measures for this wide spectrum of persons. These measures aim to screen out unwanted persons or intruders and at the same time provide a minimum of inconvenience to hotel guests and legitimate visitors. Varying degrees of access control can be achieved using security staff—in some hotels known as a security officer, a security guard, a doorman, a concierge, or by another title that differs according to the respective duties and responsibilities—and various security measures.

---

42 "Lodging no complaints" by Chad Callaghan, CPP, CLSD, vice president of loss prevention for Marriott International (Security Management, Alexandria, VA, June 2001:73).

*In this context, a solicitor is a person who approaches building occupants with the intent to sell something, to ask for business for a company, to request charitable contributions, or to obtain magazine subscriptions. This definition would include people who beg or panhandle for money or food.
Building access controls include vehicle access to parking lots, garages, and loading dock/shipping and receiving areas; pedestrian access to building lobbies, elevator lobbies, and passenger and freight/service elevators; and access routes to retail spaces, restaurants, promenades, mezzanines, atria, and maintenance areas. Measures for controlling access to these areas vary from hotel to hotel, depending on the hotel management’s policy, but generally they incorporate some or all of those described in the following sections.

Parking of Hotel Guest and Patron Vehicles
Handling of hotel guest and patron vehicles will vary from hotel to hotel and will often include the following:

1. A hotel valet or parking attendant stationed at the front entrance of the hotel to take control of hotel guest and patron vehicles and park them in a parking structure located adjacent to or underneath the hotel or in a surface parking lot outside of the hotel.

2. Hotel guests and patrons self-park their vehicles in a parking structure located adjacent to or underneath the hotel or in a surface parking lot outside of the hotel. Either
   a. there are no controls on the entry of vehicles to structures (apart from vehicle height restrictions at the point of entry to any structure). Many hotels allow such free access. Some require the guests, once they have registered at the reception desk, to display a sheet of paper, placard or sign on their vehicle dash indicating their authorization to park, or
   b. a ticket (imprinted with the date and time of entry) is dispensed by a machine at the point of entry, which when withdrawn from the control unit automatically opens an entry gate or raises a gate arm. (There will be vehicle height restrictions at the point of entry to any structure.) When exiting a controlled-access parking structure or lot, the driver may be required to make a monetary payment, to present a hotel-validated ticket to a parking attendant, to present the ticket to a pay-on-exit machine and either pay in cash or with a credit card, or to present a token issued by the hotel to a controller that can operate the parking exit barrier.
   c. the guest room electronic access card provided to guests when they check into the hotel also provides access for their vehicle to the hotel parking areas (both for ingress and egress).

Parking of Hotel Staff and Vendor Vehicles
Requiring hotel staff, vendors, and other hotel workers to park in designated safe areas far from the hotel building is a sound security policy. Adherence to this rule frees up available parking spaces closer to the hotel for hotel guests and patrons to use. Not only is this appropriate from a customer service standpoint, but it also keeps hotel staff from parking in specific areas—such as near hotel loading dock/shipping and receiving areas, kitchens, food and alcohol storage areas, and building stairwells—and makes it more difficult (or at least increases the chance of detection) for hotel staff to carry unauthorized items from the hotel to a parked vehicle.

Vehicle Access to Loading Dock/Shipping and Receiving Areas
Vehicles entering loading dock/shipping and receiving areas either may do so at will and park at whatever loading bays or docks are available, or they may be permitted to...
enter and be directed to park in certain areas by a loading dock attendant who will then supervise subsequent loading or unloading. Also, docks that are normally unattended may have an intercom or buzzer system, possibly in conjunction with closed-circuit television (CCTV), to allow drivers to remotely summon hotel staff for assistance.

For security purposes, the dock attendant normally will maintain a log or record of the vehicle license plate number, the driver’s name and company, the time in, and the time out. Depending on building policy, vehicle keys may remain in the vehicle or be given to the dock attendant for safekeeping and to permit the attendant to move the vehicle if necessary.

The activity of drivers and delivery persons usually will be confined to the loading dock/shipping and receiving areas, unless they need to proceed into the hotel for deliveries or pickups. For this reason, rest areas, toilet facilities, and pay phones may be provided in these areas. If drivers and delivery persons enter the hotel, they are usually required to notify the dock attendant of the specific area they will be visiting and the approximate duration of their stay. They may also be issued special identification badges and required to leave some form of personal identification (such as a driver's license) with the attendant.

Pedestrian Access to Hotels
Security officers or doormen are often present at a larger hotel’s main entrances (for major facilities they will be present 24 hours per day, 7 days per week). These individuals (and others such as bellhops and valet parking attendants) can observe both incoming and outgoing pedestrian traffic and assist hotel guests, patrons, and visitors with information and directions. (Some smaller hotels may rely on hotel reception staff to monitor pedestrian traffic at the hotel's main entrance, if visibility affords it. Such surveillance is not always reliable because staff may be distracted when carrying out other reception duties such as handling guests, answering telephones, etc.) They can also direct persons delivering or picking up items to the appropriate hotel service entrances, assist other legitimate hotel users, and, by being trained observers and asking probing questions, they can help screen out intruders who have no legitimate reason for entering the premises.

During Normal Business Hours
During business hours (or at least during daytime hours, 7 days per week), pedestrians entering hotel buildings may simply enter the facility at will and proceed to whatever area they desire, including freely using elevators to access guest room floors, or they may be asked to submit to some form of credentialing process before they are permitted to enter.

*A bellhop, “also bellboy or bellman, is a hotel porter, who helps patrons with their luggage while checking in or out. They often wear a uniform like certain other page boys or doormen. The job’s name is derived from the fact that the hotel’s front desk would ring a bell to summon an available employee, who would ‘hop’ (jump) to attention at the desk in order to receive instructions... Duties that are often included in this job are opening the front door, moving luggage, valeting cars, calling cabs, transporting guests, giving directions, basic concierge work, and responding to any of the guest needs.” (Wikipedia. “Bellboy.” <http://en.wikipedia.org/wiki/Bellhop>; August 4, 2008). Bellboys are usually supervised by a bell captain.

**Some hotels only permit guests to enter exterior hotel doors, other than those at the main entrance, by presenting their guest room access card to electronic card readers positioned at these ingress points.
enter the hotel and proceed to interior locations (such as guest room floors, penthouse or presidential suites, concierge floors, and recreational facilities, function rooms, dining areas, and restaurants). Sometimes the process will involve the hotel guests being required to use their room access cards either on the elevator bank wall or at an elevator kiosk before proceeding to an elevator car (as is the case with destination dispatch elevators) or inside the elevator car itself to access their floors or a specific location.

After Normal Business Hours
After hours (or at least from early to late evening until the next morning, 7 days per week), the procedures may vary. Some hotels may lock all entrances except the main entrance door(s). For entry to interior areas of the hotel, some hotels do not control access to guest floors during normal business hours but do require it after hours. Hotel guests may be required to use their room access cards either on the elevator bank wall or at an elevator kiosk before proceeding to an elevator car (as is the case with destination dispatch elevators) or inside the elevator car itself to access their floors or a specific location; or for hotels that do not have card-access controlled elevators, a temporary kiosk may be set up at the entrance to each guest elevator lobby, and a security officer or a doorman requires guests to produce their room access cards before proceeding to use the elevators.

The degree of access control imposed by a hotel determines the percentage of unwanted persons successfully screened out. “The security program should be designed just tight enough to screen out as many intruders as it takes to reduce problems to the level that can be accepted. This means that a useful security program will rarely screen out all intruders.” Because hotels desire to create a warm, welcoming atmosphere, often access control measures will not be tight due to the fear of driving away guests, patrons, and legitimate users of the hotel’s facilities.

Right to Pass Signs or Plates
Signs or sidewalk plates, generally located outside the hotel, may state the following:

“RIGHT TO PASS BY PERMISSION, AND SUBJECT TO CONTROL, OF OWNERS” or “PERMISSION TO PASS REVOCABLE AT ANY TIME.”

If a person who does not have a legitimate reason for being in the hotel is discovered, then the hotel owner, manager, or agent acting on behalf of the hotel may revoke the person’s right to remain. Due to the limited authority of security staff, “any activities which limit the freedom of movement of any person or persons in the lodging..."
facility be undertaken by the property’s staff with the utmost discretion. Such actions should always be reasonable and appropriate.⁴⁴ As Ellis and Stipanuk further cautioned,

Unauthorized or undesirable persons (as determined by management for each individual property) should be discouraged from visiting the property, but again, extreme discretion and tact should be used. When deciding whether to evict persons from the premises, great care should be taken to react to what they actually do as opposed to who they are or seem to be. For example, persons suspected of being prostitutes should be evicted with great care. It can be a costly and embarrassing error to question the character or reputation of an individual. Such questioning, if unfounded, can serve as basis for legal action for slander.⁴⁵ The eviction of persons from public space (such as the lobby and any restaurants) is governed by laws applicable to places of public accommodation. Management should review the statutes applicable to its location.

On the other hand, guestrooms, and guest corridors are not deemed open to the public. No one other than guests, legitimate visitors of guests, and the property’s employees should be in these areas. The normal laws of trespass apply in these areas and should be consulted. If employees see a suspicious person on a floor or in an elevator, they have the right to ask if he or she is a guest or a visitor. They can also ask to see the person’s room key [or a keycard] or accompany the person to the room he or she intends to visit. Unauthorized persons may be asked to leave the property and warned not to return.⁴⁵

After being told to depart the premises, those who refuse to leave may be subject to arrest by law enforcement. Also, anyone reentering a hotel after having been warned that he or she is not authorized to enter may be treated as a trespasser. These actions should be thoroughly documented.

Stairwell Access

Doors leading to stairwell doors are unlocked from the floor side (as required by life safety codes as a means of egress during an emergency) and are also usually unlocked from the stairwell side leading onto the floor, including on all guest room floors (with the possible exceptions of the concierge floor and hotel service floors).

Access to Maintenance and Storage Areas

Access to maintenance areas (mechanical rooms and floors, air-conditioning rooms, telecommunications and utilities access points, and elevator machine rooms), storage closets, and areas under construction or renovation usually will be tight. Depending on hotel


policy, persons accessing these areas may be logged in and out, required to wear special identification badges, given keys (although issuing keys to vendors or visitors can be a security risk) or an access card (if the card is not returned, it can be immediately deactivated) to a particular area, or provided an escort. Some contractors servicing certain types of equipment in specific hotel areas may be permitted to install their own locking devices at access points leading to this equipment (see further comments in the “Key Points to Consider” section presented later in this chapter). Main electrical switchgear and power transformer rooms are usually deemed such a life safety risk that no hotel personnel are issued keys to these areas.

Access to Guest Rooms

On checking into many hotels and providing appropriate photo identification, a guest is often given a paper folder containing an electronic access card that can be presented to a card reader located on the entrance door to the guest’s room or suite. This card is programmed with its own unique identification number and is valid only for the scheduled period of stay. Presenting of a valid card to the door reader will permit entry and record each individual transaction. (Each individual card reader is usually battery powered and will continue to operate during a power failure.)

The access card does not have the guest’s room number recorded on it. Handwritten inside the folder is the guest’s room number, plus possibly some simple security and safety information printed on the folder. “The guest should be reminded to keep the room number identifier separate from the key or keycard or the identification of the keycard will be compromised.” Unless the guest is visually impaired, the staff checking in the guest usually does not speak the room number out loud. This is done to ensure that no one else in close proximity can hear the conversation and thereby know where the guest will be staying. (A guest’s room number should never be revealed to outsiders other than the guest.) If the hotel has its elevators on access control, a guest can present this same card to the elevator system to gain access to the floor on which her or his room is located.

If there is a problem using an access card, the guest loses their card, or the guest inadvertently leaves their card in their room when they exit the room, the guest can speak to any available hotel security staff or request housekeeping staff to contact hotel security, use a house telephone (usually located on guest floors in each elevator lobby) or a mobile telephone to contact the lobby reception desk, or return in person to the front reception desk. If the guest goes to the reception desk with their photo identification, hotel reception staff can simply program another card for the guest. If the guest has left their personal identification in their room, hotel security or other hotel staff can accompany the person to the room in question, use their own access card to permit the guest entry to the room, and observe the guest retrieving their identification for confirmation of identity. In the case of the guest having left their access card in the room, the guest can then retrieve it; in the case where the card is not working properly, or has been lost, a replacement card can be made for the guest by the hotel.

In the past, keys were commonly issued to hotel guests to access and secure their rooms. However, keys can be fairly easily duplicated and present problems if they are lost or stolen. Today, throughout the world, most hotels issue electronic access cards—sometimes simply called keycards—that operate guest room electronic door locks. Ellis Jr RC, Stipanuk DM. Security and Loss Prevention Management. 2nd ed. Lansing, MI: Educational Institute of the American Hotel & Motel Association; 1999:166, 167. Unless there are special circumstances, such as an authorized request from law enforcement.
For security reasons, most hotel access cards will display no identifying marks (such as the hotel’s trademark, its name, or its address) that indicate where it might be used. Then, if a card is lost, there are no identifiers to indicate from which hotel it came. If used with an insertion or a swipe-type card reader, there may be an arrow depicting the correct way to insert or swipe the card (or other simple step-by-step instructions on its use). An advantage of an electronic access card is that if it is missing (either lost or stolen) or when a guest leaves the hotel, the card can be immediately deactivated at a hotel computer without the need to retrieve the card itself. (Some hotels allow guests to keep the card as a memento of their stay. However, if the card does not contain identifying information, then much of the appeal for keeping the card is diminished.) Regarding the value of access card-controlled door locks, Lauer stated,

Since the introduction of the recodable electronic door lock in the late 1970’s, hotel security has been virtually transformed. The focus at the time of inception was increased guest security, but the benefit to the property was quickly realized. Hotel security experts, along with media pundits, the courts, and the insurance industry all agree—keycard locks, which can be easily changed so that every guest gets a new key, are the best way to boost security....

Employee access control was one of the first system enhancements to increase the level of internal technology. In order for a property to be maintained efficiently, hotel personnel require their own means of entry to rooms in which they must perform daily routines or tasks. In the past, distribution of conventional keys to housekeepers, room service attendants, and maintenance personnel compromised guest belongings and increased the liability of the hotel. In some instances of theft, the victim was often the hotel (where even the negligent customer is king), and claims went unchallenged. The “burden of proof” is welcome by a hotel equipped with modern electronic locks, for the actual lock serves as a log, monitoring and recording up to 1,000 entries (about 100 days worth). Many reputations have been restored and many a thankful employee has been cleared of suspicion due to the success of these products. Employee key cards can be coded to allow access only to their assigned units of responsibility and only during the hours of their shift. Knowledge of these system capabilities may also serve as a deterrent to those less ethical. 47

In the case of a reported theft from a guest’s room, the event history of cards used to enter the room and when entries occurred can be determined by interrogating* the lock at the door itself (using a small hand-held device); or if the lock uses a hardwired or a wireless system, ** this information can be determined with the use of an online central computer at the front reception desk or the security command center, eliminating the

---


*In this context, interrogate means to examine the audit trail of events when access cards were used to operate an electronic lock.

** For example, the Saflok Messenger Wireless Lock Access Network has the capability for the Messenger module in each lock to report to the central computer all keys used in the lock. Also, it can notify the central computer when a door has not been fully closed for a specified period of time and when the battery power operating the lock is low (Saflok Messenger Wireless Lock Access Network brochure [Saflok, a member of the Kaba Group. <www.saflok.com>]).
need to go to each individual lock. This information can be vital in such an investigation, particularly if there were no visible signs of a forced entry. Technology is also available to determine whether a door was opened from the inside of the room (such a feature is invaluable in investigations to determine when a door was opened and whether an access card was used in the process).

For hotels that do not have a guest room locking system connected to a central computer, when a guest checks out of their room the access card to that room usually remains active until the next guest assigned to that room presents their card to the door reader or the scheduled time of stay expires. When the next guest to that room uses their card it will automatically delete the previous guest’s access privileges. Therefore, until the new guest arrives, the possibility exists that the previous guest could continue to access their room until their scheduled time of stay expires. This issue does not exist with a centralized, online computer-controlled card system since the card’s access privileges can be immediately deleted at the reception desk’s central computer when the guest checks out.

**Guest Room Security**

In addition to completely closing the door when entering the hotel room (and leaving it closed while in the room), guests may improve their room security by engaging any secondary locking mechanism, such as a deadbolt lock, a door swing arm security restraint, or a safety chain. Also, if there is a connecting room, guests should check that the door leading to it is locked.

It is important that guests *never* open their doors for anyone that they do not know personally or for room service or hotel maintenance that they did not request, even if the person is wearing a name tag, as most hotel employees are required to do. Any guest who is in any doubt as to the identity of anyone requesting entry should immediately telephone the hotel reception desk to report the matter or to verify the identity of the person in question and determine the purpose for allowing the person to enter the room.

In many hotel guest rooms, the main entrance door is equipped with a conventional door viewer (sometimes called a view port) to provide a clear view of the other side of the door (using a hollow end or peephole to look through and a lens at the other end to give a wide viewing angle) and of anyone requesting entry. (Some hotels have a small box housing the view port. A printed sign informs the guest to “LIFT THE LEVER FOR VIEWING. VIEW THE CALLER BEFORE OPENING THE DOOR.”) Also, digital door viewers are available. Such a device “includes an LCD monitor that mounts on the inside of the guest room door with a digital camera on the outside to

---


*This same time control feature also can be utilized to issue housekeepers with keycards that only work during their shifts (Channell, WT. Electronic locks finding the right fit. Alexandria, VA: *Security Management*: January 1996:61).

**Although a guest who is entertaining a visitor may decide for appearances sake to leave the door ajar while in the room. However, if there is such a concern, it may be more appropriate to meet the person in a public area such as the hotel lobby or a restaurant.

***Some hotels use spring-activated deadbolts, which automatically engage when the door is closed without requiring the guest to manually engage the deadbolt in order to double lock the door.

****Usually located at the height of an average person’s eye level, sometimes an additional viewer is installed in the door at a lower height for physically disabled guests who may be wheelchair bound (Ellis Jr RC, Stipanuk DM. *Security and Loss Prevention Management*. 2nd ed. Lansing, MI: Educational Institute of the American Hotel & Motel Association; 1999:145).
provide a clear and effortless view." The guest should use these viewing devices to see the person requesting entry before granting or denying access.

If a hotel guest in-room safe is provided, a guest should secure in it any valuables (such as money, credit cards, jewelry, documents, airline tickets, clothing, or other items of considerable value, and, if the safe is large enough, any laptop computer). If the safe uses a security key that can be removed from the safe only after the door is closed and locked, the guest should keep the key safely in her or his possession at all times. If the safe has a digital keypad system, the guest should record the combination selected for the safe but make sure not to leave it lying around in the room.

If no guest in-room safe is available, the guest should consider using any safe deposit boxes located at the hotel’s main reception desk. (If neither is available and the hotel offers to take possession of valuables, the guest should request to see where the items are being secured. If there is a concern they are not being adequately protected, the guest should not leave such items in the hotel’s possession.)

If the guest decides to leave valuable items in the room, they should be secured in the room (for example, the guest can anchor a laptop with an appropriate cable and lock it to an immovable room fixture) or hidden from view as much as possible (such items are still at considerable risk for an experienced thief to search for and find, even if extremely well hidden). Also, leaving valuable items in vehicles parked in the hotel’s parking garage is a risk. If a guest does so, these items should always be out of sight and secured in the vehicle’s trunk (boot) or locked glove box compartment. Using a valet service may potentially increase the chance of such items being taken from the vehicle.

Guests should familiarize themselves with the telephone in their guest rooms to ensure they know how to dial the main reception desk or any other emergency services. They should also pay attention to security and safety information—usually in the form of listed security and safety awareness tips—provided to them at check-in (for example, printed on the paper folder containing the room key or keycard), contained in any guest information book or brochure provided in the guest room, posted on the back of the guest room main entrance door (including information on steps to take if a fire emergency occurs, including a plan depicting the emergency exits on the floor in question and possibly the location of manual fire alarm stations on the floor), or displayed in a program on any hotel television channel. Guests can play an important part in any hotel security and life safety program by promptly reporting things such as suspicious persons or activities, safety hazards, or the smell of smoke to hotel management and security staff.

• Such items, particularly laptops, should not be left in hotel storage rooms that do not have adequate access control measures. Also, a receipt for any item should always be obtained from the hotel.
•• In hotel meeting rooms, a similar security precaution can be taken by securing the laptop to a meeting room table. “In addition, some hotels have provided roll-in safes for meeting rooms, with newer models outfitted with electrical outlets so that the laptop can be charged while secured” (“Lodging no complaints” by Chad Callaghan, CPP, CLSD, vice president of loss prevention for Marriott International [Security Management. Alexandria, VA; June 2001:76]).

Of course, this is no guarantee that a physically secured laptop will not be interfered with or the information within it compromised. Encrypted software may be used to protect information stored in a laptop computer.

•••• However, because many guests are transients they are somewhat at a disadvantage, as compared with residents of apartment buildings, in recognizing persons who do not belong (Ellis Jr RC, Stipanuk DM. Security and Loss Prevention Management. 2nd ed. Lansing, MI: Educational Institute of the American Hotel & Motel Association; 1999:104).
As part of guest room security, when a hotel operator receives a call from an outside telephone line or an internal house phone requesting connection to a guest room, the operator should never forward such a call unless the caller is able to provide the guest’s name and, depending on hotel policy, possibly the guest’s room number.

The hotel operator and receptionists should never reveal the room number of a guest to anyone other than the guest. As mentioned previously, when checking in a guest and handing the person the guest room access card, the receptionist should never loudly announce the room number (to prevent someone standing close by from hearing this information). Instead they should speak softly or indicate the room number by pointing to it written on the folder containing the card.

When leaving the room, the guest should make sure any exterior sliding glass doors and all windows are closed and locked and should engage any additional devices (such as added locking mechanisms or material that can be placed in the channel in which a sliding door or window is designed to glide along) that limit the distance the door(s) or the window(s) can open; and on exiting the hotel room door, the guest should make sure it is completely closed and locked, testing it by trying to open it again without using a key or access card (some opportunists may methodically walk hotel corridors to locate an unsecured room; such activity may be for criminal purposes or simply to find a vacant room to use). Also, when not in the room, leaving the “Do Not Disturb” notice on the door and a television set on may be a deterrent to a would-be-thief. While out of the room, guests should keep the room access card in their possession at all times, particularly if it is housed in a paper wallet on which the room number is written. On leaving the room, guests should make sure they take the room access card with them.

When returning to the hotel after dark, guests consciously pay attention to their surroundings, keep to well-lighted areas, and use the main entrance of the hotel.

**High-Profile VIP Guests**

According to Ellis and Stipanuk,

> VIP [very important person] guests may require additional security personnel. Some well-known figures may wish to keep a very low profile, and all staff [hotel management, security, front desk, room service, housekeeping, and engineering] should be instructed on how to appropriately respond to inquiring media and the general public. If the guest has a personal security staff, armed or otherwise, arrangements and accommodations may need to be made by the property and the local police. If the individual is controversial, the property may wish to request the assistance of the local police ... or some other authority. Properties expecting the arrival of a controversial guest

---

*A guest with vision impairment should be taken aside, out of the hearing of others, to be told the room number. Hotel room doors should be equipped with Braille numbers or raised numerals for blind persons to find their designated room, or they should be escorted to their room by hotel security or other hotel staff. Depending on local laws or a hotel’s policy, some facilities may have specially designated guest rooms for persons with impairments.*

---

may also want to review emergency evacuation and bomb threat procedures with their employees before the guest arrives.51

Intoxicated Guests and Patrons

According to Beaudry,

Alcohol liability problems generally do not involve security staff initially, for it is usually food and beverage department employees such as bartenders, waitresses, and managers who are directly in control of and responsible for alcohol consumption. Security does have a function to perform, however, in helping to prevent intoxicated patrons from driving a vehicle or becoming injured while walking around the hotel property. Not all alcohol liability cases are limited to motor vehicle accidents. Guests can become injured by falling down due to intoxication in an otherwise safe area. Unfortunately, in such cases the innkeeper is not able to claim the defense that it was the guest’s intoxication that caused the injury, if it was the innkeeper who allowed the individual to get drunk in the first place.

The greatest risk of alcohol liability arises when the guest attempts to leave the hotel and drive a car. If a security officer is called for assistance in such circumstances, everything possible should be done to discourage the guest from driving. A hotel’s management may even want to consider the extreme measures of refusing to return the guest’s keys or calling the local police department. This action may cause other problems (such as difficulties regarding the appropriateness of refusing to give a person back his or her property), but the hotel operator must weigh the risks and decide on the safest option.52

Guest Evictions

According to Beaudry,

The hotel may make reasonable regulations governing the conduct of guests, provided such regulations are applied to all persons, without discrimination. These regulations can be designed to prevent immorality, drunkenness, or any form of willful misconduct, e.g., loud obnoxious behavior, drug activity, etc., that may offend other guests, may bring the hotel into disrepute, or may be inconsistent with the generally recognized properties of life. The hotel has the right to evict any guest who willfully violates these rules....

Obviously, the eviction must be done in a reasonable manner. If guests refuse to leave the hotel after their attention has been called to the violation and they have been requested to leave and given a reasonable opportunity to do so, the hotel may forcibly evict them. The hotel may use only such force as is reasonably necessary to accomplish this goal. Management personnel


Sometimes large groups, such as visiting sporting teams, exhibit uncontrolled, boisterous behavior that is extremely noisy and disruptive to other guests and can result in damage to the hotel itself.
and security officers should be carefully instructed on this point and the hotel should obtain the assistance of the local police [if required].

When a hotel guest becomes ill with a contagious disease, the hotel management, after notifying the guest that he or she must leave, has the right to remove the guest in a careful manner and at an appropriate time to a hospital or other place of safety, provided this does not imperil the guest’s life. As a practical matter, however, it is preferable to consult with an attorney and report these matters to the proper local authorities. Usually the local authorities will take charge and remove the sick guest. The illness of an indigent guest should be reported to the local department of welfare, communicable diseases should be reported to the local health authorities, and psychiatric cases should be reported to police.\textsuperscript{53}

\textbf{Escorts of Hotel Users}

In hotels, people may be escorted for a variety of reasons. It may be to protect individuals or the property that they are carrying. It may also be to show a person, unfamiliar with a site or facility, to a particular location.

\textit{Escorts to and from the Hotel}

Escorts to and from a hotel usually occur after normal business hours. Security staff members generally conduct these escorts. Hotel guests, particularly older residents or females, may request hotel security to escort them to areas of the property such as parking garages. Hotel policy should dictate how, when, and where the escorts are to be conducted.

\textit{Escorts within the Hotel}

Some guests may require escorts to their rooms, and hotel staff such as cashiers may require escorts to areas where monies are secured. Also, hotel policy may require that persons needing access to certain maintenance spaces and areas under construction or renovation be provided with an escort to accompany them whenever they are in these areas. Building engineering or security staff may be required to provide such escorts.

Some hotels have a list of local and state agencies whose inspectors are authorized to enter, but it is absolutely critical to verify the identification of these individuals and to make hotel management aware of their presence before they are granted entry. It is important to escort anyone claiming to be an inspector while he or she is in the facility.

\textbf{Property Control}

Most hotels allow the free movement of guest’s luggage and possessions into and out of the facility. This makes the control of property extremely difficult, if not impossible.

\textbf{Objectives of a Property Control System}

The objectives of a property control system are threefold:\textsuperscript{54}

- \textit{To prevent stolen property or other unauthorized items from leaving}. Stolen property may include furniture and furnishings, entertainment equipment, antiques and works


of art from hotel guest rooms, function rooms, convention facilities, restaurants, and dining areas; cash and negotiable instruments from reception and restaurant areas, retail shops, and other areas handling such items; computers and printers from administrative offices and business centers; equipment from recreation areas, kitchens, dining areas, restaurants, retail shops, newsstands, entertainment centers, kitchens, and laundries; equipment and exhibits from exhibit areas; and property from inside vehicles parked in the hotel’s parking garage.

- **To prevent dangerous items entering.** Items such as explosives, illegal drugs, and hazardous materials might easily be secreted on a person, in that person’s luggage, or in a vehicle and brought into a hotel.
- **To prevent unnecessary or disruptive delivery traffic.** By keeping out misdirected deliveries, unnecessary traffic is avoided. By routing deliveries through proper entrances, such as loading docks and freight/service elevators, disruptive traffic is avoided and the guest elevators are protected against damage from hand trucks and bulky crates.

The use of property control systems for guests and patrons is usually not appropriate in the hotel setting. However, guests and patrons may hand over certain property to hotel staff for temporary safe keeping (for example, items placed in safe deposit boxes, coats and hats checked in at restaurants, and luggage stored after a guest has checked out of the hotel but has not yet left the facility). Also, during special events, such as those involving valuable exhibits, strict property removal control may be required to protect the exhibits; and the hotel, particularly a larger one, may require hotel staff and workers to enter and leave the hotel through an employee entrance and be subject to periodic inspections of bags, containers, and packages. However, it is unusual for vehicles, even those entering under-building hotel parking garages and loading dock areas, to be inspected.

Good housekeeping should always be practiced for trash (rubbish) storage, trash compacting, and dumpster areas. Hotel staff, including security and housekeeping staff, should be alert for objects, items, materials, or parcels that look out of place or suspicious, and for large items being removed from the facility.

**Couriers and Delivery Persons**

Hotels receive deliveries of assorted items for guests (for example, delayed airline luggage). Also, couriers sometimes come to a hotel to pick up packages and sundry other items. The entry of delivery persons and couriers needs to be strictly controlled. Depending on the size of the hotel, such items will be handled inside the hotel by bellhops and possibly a business center where shipping and receiving services are offered. Like any well-run operation, these programs need to be meticulously documented to provide an audit trail to track deliveries and pickups and ensure that these tasks are being done in a timely manner.

**Special Exhibits**

Special events where exhibits of various items, some of which may be of high value, that are held in the hotel require special security measures. When the exhibitors are

---

*However, since the 2008 Mumbai bombing incident, some hotels are searching guest’s bags, deploying X-ray machines at entrances, scanning guest luggage upon arrival, and, in future, may not permit luggage storage or packages or luggage to be accepted prior to the guest’s arrival (Conde Nast Traveler. Brady S. Wake up call: Lessons learned from Mumbai. March 9, 2009. <http://www.concierge.com/cntraveler/articles/500281>); March 20, 2009.*
present, responsibility for these items is generally theirs. However, when the exhibition hall or room is closed (and particularly if the exhibits are left overnight), the exhibitors will need to make special arrangements, in conjunction with hotel management, to protect these items. Protective measures may involve the use of hotel security or contract security staff, video surveillance, or intrusion detection systems in the area where the exhibits are located. It is critical that all arrangements be thoroughly documented, contracts and insurance policies be in place, and that there is a clear understanding of any liability burdens that the hotel may be assuming while the exhibits are in the hotel, including the time periods when the exhibition is being set up or dismantled.

Construction and Remodel Activities
When a hotel is being constructed or remodeled, the security department needs to be a critical part of the operation. It is particularly important that access control measures are in place to prevent the unauthorized removal of property from the hotel, including hotel fixtures and equipment.

Lost and Found Property
Handling lost and found property is an important part of an effective security program. Most people can recall the anguish they felt on discovering that a valuable personal possession or business item was missing. Likewise, one may remember the exhilaration at being contacted and informed that the missing property had been found and was available for pickup.

If property is lost in a hotel and is subsequently found and handed to hotel staff, the item should be kept in a secure place (including a safe deposit box for items such as cash, credit cards, traveler's checks, jewelry, etc.) and, if possible, expeditiously returned to its rightful owner. This can considerably enhance the trust and confidence that hotel guests and patrons will have in the hotel's operations. Just the opposite will be true if a guest or patron learns that the found item was handed to hotel security and was then lost or went missing.

Lost and Found Property Log
Hotel staff should maintain a list of lost and found items in a *lost and found property log*. The log should contain details such as the following:

- A brief description of the property, including any serial or asset tag numbers
- The date, time, and place the property was lost or found
- The identity of, and means to contact, the person who lost or found the property
- If the property is claimed, the identity of, and means to contact, the claimant and the signature of the person who received the property
- The names of the person who took the report of the lost property, logged in the found item, or handled the return of the property to its rightful owner

Handing Over to Local Authorities
If the lost property is particularly valuable or sensitive, it may be necessary for the local law enforcement agency to be contacted; if the property is subsequently handed over to local authorities, this fact, including the identity of the receiving law enforcement officer,
should be noted. A receipt for the property should be obtained. Local and state laws often determine the handling of lost property.

Some jurisdictions allow found property, when its owner is unknown and its value is below a certain amount, to be distributed to local charitable organizations. Others, after a certain waiting period, auction the property or allow the finder to assume ownership of it.

**Handling Property of Sick, Injured, or Deceased Guests**

If a guest staying alone at the hotel is sick or injured and needs to be transported for medical help or dies while on the premises, a member of the hotel’s staff, in the presence of another staff member, will need to itemize the guest’s personal property and store it in a safe location until the guest or an authorized representative can take possession of it. Of course, the handling of a deceased guest’s property will depend on whether law enforcement is involved as part of a criminal investigation. In this case, if a suspicious death has occurred in the guest room, the room may be considered a crime scene that needs to be protected (see a discussion of crime scenes in Appendix 9–2 on the CD-ROM provided with this book). If a similar type of death occurs in a public area, the scene will need to be protected accordingly.

**Housekeeping Operations**

Housekeeping staff (who wear uniforms and usually name or photograph identification cards) are assigned to clean and replenish the supplies of designated guest rooms on a floor. Because they often work alone in guest rooms there is the opportunity for them to steal a guest’s property or copy information from confidential documents or a laptop computer or other electronic media left in the room.

Because housekeeping staff are assigned rooms, this can make investigations involving housekeeping staff easier as management will know which housekeeper handled which rooms on a particular day. In itself, this can be a strong deterrent to dishonest behavior.

**Housekeeping Staff Screening**

During the hiring process, housekeeping staff should be carefully screened, including conducting a thorough background investigation. As part of preemployment or preassignment agreements, housekeeping staff may be asked to submit to a visual inspection of any items they are carrying to and from work—lunch pails, bags, backpacks, packages, and so on. The frequency of the inspections can be established as part of the agreement: inspections may be conducted every time the employee enters or leaves the hotel, at random, or only with cause.

Housekeeping supervisors or hotel security staff members usually conduct such inspections. They are visual only, and employees are requested to open appropriate items themselves. Under no circumstances does the inspecting person touch the items being inspected or attempt to inspect any part of the employee’s person or clothing.

---

*For example, in California, Section 2080 of the California Civil Code does not require a person to take charge of found property, but if the person does, she or he can be sued for the negligent handling of it. The law further provides that if the owner of lost property is known, the property must be returned to that owner. If the owner is not known and the property has a value above ten dollars, the property must be turned over to the local police within a reasonable period of time (American Protective Services. Administrative News: Oakland, CA; 1993:4).*
All persons have a legal right and expectation of privacy, so items such as purses will be subject to inspection only under special circumstances, the nature of which should be established in writing beforehand.

**Important Part of Security**

The housekeeping staff constitutes an important part of a hotel’s security program. Some of the ways these employees can impact security are as follows:

1. When cleaning guest rooms, either taking their cleaning and supplies cart inside the room and locking the room door while servicing the room, or leaving the room entrance door open, with the cart immediately outside to partially block the entrance. They should not allow persons, other than the room guest, to enter the room while they are working (unless the room guest authorizes others to enter).
2. Recognizing potential security hazards (such as malfunctioning door locking mechanisms) and safety hazards (such as potential slip-and-fall hazards like a water leak, broken flooring, slippery floor mats or damaged carpeting).
3. Being alert for people who act in a suspicious manner (including guests who decline regular housekeeping service, particularly for more than one day), as well as for objects, items, materials or parcels that look out of place or suspicious—including plastic tubes, glass containers, and supplies of household chemicals—and strong odors that may indicate a clandestine drug laboratory.
4. Reporting missing signs and notices displaying security and safety information and hotel liability notices that should be securely attached to the back of guest room doors, and similar information contained in guest information books or brochures provided in the guest rooms.

**Key and Electronic Access Card Control**

In hotel buildings, keys and electronic access cards to various parts of the facility are under the control of hotel management and departments that include security, engineering, and housekeeping. Hotel management personnel obviously need to have access to all areas of the hotel they manage. Depending on how the hotel is managed and how security staff is utilized, security personnel also will need access to certain areas. Building engineers, because of the nature of their work, need access to virtually all areas, including guest rooms. Housekeeping personnel will need access to guest rooms and rooms where cleaning and supplies are kept. Depending on the size of the hotel and the services provided, various other department heads, including those overseeing function rooms, business and conference centers, restaurants, kitchens, and recreational facilities, will need keys and access cards pertaining to their areas of responsibility.

---

*All staff members are an important part of a hotel's operations. In numerous ways they are the eyes and ears of the hotel's security and fire life safety program. “Nonsecurity staff should also be concerned about security…. By training the entire hotel security staff to report security and safety concerns, security departments can cost-effectively improve site safety, thus enhancing customer’s overall perceptions of the facility” ( “Lodging no complaints” by Chad Callaghan, CPP, CLSD, vice president of loss prevention for Marriott International [Security Management. Alexandria, VA; June 2001:72, 73]).

**In some hotels, telecommunications technicians, gas, water, and power utility workers are permitted to attach their own locking devices to areas containing their equipment. This practice is convenient because hotel staffs are not required to open these areas, but it compromises security because control of keys and the areas...*
special circumstances (such as during medical emergencies or when a guest has died), there will be the need for designated hotel personnel (possibly security and engineering or hotel management staff) to override the locking systems to enter a guest room.

**Key Points to Consider**

Keys and access cards should be issued only to those persons who can be entrusted with them and who have an *absolute* need for them. The status a person may feel by possessing certain keys and access cards should not enter into the decision-making process.

Most lodging properties use at least three levels of keying. These levels typically include emergency keys, master keys, and guestroom keys. The *emergency key* opens all guestroom doors, even when they are double locked. It can be used, for example, to enter a room when the guest needs aid and is unable to reach or open the door. The emergency key should be highly protected and its use strictly controlled and recorded; it should never leave the property. One procedure for emergency keys is to have them locked in a safe or safe deposit box [or in a locked or sealed key cabinet with the cabinet’s key, lock code, access card, or replacement seal in strict custody] and signed out by the individual needing one. The log should be dated and signed by the individual taking the key.

A *master key* opens all guestrooms that are not double locked. Depending upon the need, the master key or keycard [access card] may be further established as a section master, a floor master, or a grand master. For example, the section master may be used by a housekeeping supervisor who is providing a quality check on service of the room by the room attendant. If it is more practical for the entire floor to be supervised by one person, that individual would be provided with a floor master. The executive housekeeper and assistant housekeeper would have a grand master, permitting access to any guestroom. Similarly, the management should establish protocol on use of these levels of master keys or keycards [access cards] for engineering and maintenance, room service, mini-bar replenishment and service, front and bell service, [technology personnel;***] and security....

The *guestroom key* opens a single guestroom if the door is not double locked. Guestroom keys should be controlled by front desk personnel, who should always make sure the person receiving the guestroom key is the guest registered for that room. Appropriate identification should always be requested. An effort should be made to retrieve keys from guests when they themselves have been lost. These areas could be used to store unauthorized or stolen items, and general housekeeping may become a problem. If this practice is permitted, no one should be allowed to place a lock on a door without hotel management or other building departments (such as engineering) having a key. In an emergency, keys must be available for access. A possible alternative is for contractors to store their equipment, including tools, in heavily reinforced large steel boxes, chests, and cabinets that can be secured using high-security padlocks that are protected from attack with cutting tools, or the equipment can be stored in card-access controlled areas.

---

*For additional information on the control of keys, see Chapter 5, “Key Control.”

***Hotels that provide Internet connectivity for guests may need to access guest rooms to deal with computer network issues.
check out. For the convenience of, and as a reminder to, the guest, consider having well-secured\(^*\) key return boxes located in the lobby, at exit points of the hotel or motel, and in courtesy vehicles....

Whenever there is any known or suspected compromise of any metal keys, a loss or theft, or an unauthorized entry by key, the affected lock(s) should be changed or rotated to another portion of the property. When master keys or emergency keys are involved, re-keying the entire area should be considered.\(^{55}\)

Keys and access cards issued to the hotel staff should never be permitted to leave the hotel. They should be passed from shift to shift, and a receipt should be recorded each time they change hands. All personnel understand the importance of not permitting keys and access cards to be compromised.

**Mobile Patrols**

Mobile patrols may be conducted in hotels for a variety of security and fire life safety purposes. “Guards [security officers] are typically highly visible thus offering something of a deterrent effect and at the same time imparting a sense of security to the [hotel's guests, patrons,] and visitors."\(^{56}\) Patrolling increases this visibility. Patrols can also be used to note and quickly address anything significant or unusual affecting security or fire life safety. After conducting a risk assessment (as described in Chapter 4), the purpose, frequency, and routing of patrols can be determined by hotel management and the security department (and, if special circumstances warrant, with the cooperation of local authorities) and then carried out and thoroughly documented.

**When and Where?**

Patrols by security staff in hotel buildings may occur as follows:

- Continuously throughout all common areas (including hotel lobbies, retail arcades,\(^{**}\) and other areas that hotel guests and visitors can freely access); restaurant, recreation facilities (including swimming pool and spa areas), meeting room, and function areas; building stairwells; maintenance areas (including shipping and receiving areas, rubbish/trash disposal areas, and other areas as deemed necessary by the hotel) and guest room floors to report obstructions (particularly those blocking emergency egress routes), fire hazards, broken glass, missing equipment (such as portable fire extinguishers), water or gas leaks, wet floors, holes, defects in floor coverings, tiles missing, unsecured areas, malfunctioning lighting equipment, doors

\(^*\)It is absolutely essential that not only can the key return box's interior not be accessed, or a key “fished out,” but also the box itself must be firmly anchored so that it cannot be easily removed. Such boxes should be located in areas continuously supervised by hotel staff.  
\(^{**}\)In some hotels, the patrolling officer carries a pager, a mobile telephone, or a hand-held panic alarm so that hotel staff and retailers can summon the officer for assistance.
left unlocked or not completely closed, signs of forced entry, unauthorized and suspicious persons (such as persons loitering and possible prostitutes) and inebriated persons, and others (including hotel staff) found in areas in which they would not normally belong, and so on. (On hotel floors, patrol management stations are often installed at each stairwell so that the patrolling officer must traverse the floor to complete the tour.)

- Depending on a hotel's facilities, patrols may also be conducted of exterior grounds, public parks, and other areas, with times varying according to their operating hours. (Motor vehicles, electric carts, bicycles, tricycles, and personal transporters may be used for patrolling large parking areas with long travel distances.)

- Continuously in parking garages and lots to deter theft of vehicles and property within them; note parking violations and possibly issue warnings or citations (hotels are often reluctant to issue citations for fear of losing customers); observe vehicle lights or engines left on, leaks from vehicles, or other unusual conditions of parked vehicles; report fire hazards, water or gas leaks, malfunctioning lighting equipment, broken vehicle windows and other signs of forced entry, unauthorized and suspicious persons, and others (including hotel staff) found in areas in which they would not normally belong; and provide for the general safety of guests, patrons, and visitors. (In parking garages, patrol management stations are often installed at each stairwell so that the patrolling officer must traverse the floor in order to complete the tour.)

- To perform a fire watch when a hotel has exceptional hazards or the fire protection system is impaired. A fire watch is “the assignment of a person or persons to an area for the express purpose of notifying the fire department and/or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety dangers.” It is vital that when such an activity is to be performed that the local fire department or other authority having jurisdiction is consulted.

**Patrolling Tips**

- Patrols can be conducted either on foot or using a motor vehicle, an electric cart, a bicycle, a tricycle, or a personal transporter.

- There should be reliable communication between the patrolling officer and the security department or the supervisor.

---

*Violations include vehicles improperly parked, parked in a NO PARKING zone or space, parked in a RESERVED zone or space, or parked in a DISABLED/PHYSICALLY IMPAIRED designated space. When placing such a notice on a vehicle, preferably locate it in the lower corner of the driver's window (immediately above the door handle) where it will be visible to the driver when entering the vehicle but will not obstruct his or her field of vision when driving. Also, the notice should be of a nonadhesive material that can be easily removed from the glass (comments by Chuck Hutchinson, National Director of Security and Life Safety, The Hanover Company, August 2008).**

**For example, in the United States, according to NFPA 601, Standard for Security Services in Fire Loss Prevention, Chapter 3, Security Functions and Duties, “a security officer shall make rounds at intervals determined by management. When operations in the property normally are suspended, officers shall make rounds hourly or as assigned by management. Where special conditions exist, such as the presence of exceptional hazards or when fire protection equipment is impaired, management shall institute additional rounds. The first round shall begin within 30 minutes after the end of activities of the preceding work shift. During this round, the security officer shall make a thorough inspection of all buildings or spaces” (Section 3-2.1-3.2.2).**

**NFPA. Glossary of Terms, National Fire Code. Quincy, MA: National Fire Protection Association; Copyright 2005.**
Whenever possible, routine patrols should be conducted in a random, unpredictable manner to avoid a fixed pattern or routine that someone planning to commit a crime can observe. Sometimes, an effective tactic is for an officer to “double back,” or retrace steps to a previous location; anyone observing the patrolling officer’s movements would usually not expect the officer to return quickly to an area just visited.

“Alertness, interest and thoroughness must be displayed. A suspicious mind must be cultivated and anything that appears other than normal must be looked into.”

Using a flashlight or a torch in areas where lighting is poor or nonexistent is extremely useful.

Simply applying pressure with the hand on a guest room door will reveal if it is securely closed.

“A simple but effective patrol plan should be established in each area. Its efficiency should be regularly checked by means of [patrol management devices], radio or telephone checks at regular intervals, etc. Failure to report, or deviation from described assignments, should immediately be investigated.”

Patrol management devices “provide the security manager with a consistent record of rounds and occurrences at a facility without the need for human supervision to ensure that rounds are completed as assigned.” If an electronic patrol management device is not used, a notebook is very useful for recording observations. (The patrolling officer can carry the notebook, or it can be positioned at designated patrol stations so the officer can record when visiting a particular area.)

As with the hiring of other members of the hotel staff, security personnel should be carefully screened, including being subject to a thorough background investigation. They should also be thoroughly trained in their duties and responsibilities (see Chapter 7 “Selection, Training, Testing, and Supervision of Security Staff” for additional information).

Emergency Planning

For a building owner or manager to effectively manage an incident that constitutes an emergency in a hotel building, it is critical to plan ahead. Before proceeding, it is appropriate to review several key concepts.

Key Concepts

An incident is an “event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization’s operations, services, or functions—which, if not managed, can escalate into an emergency, crisis, or disaster.”

---

59 See a description of “patrol management devices” in Chapter 5.
A disruption is “an event that interrupts normal business, functions, operations, or processes whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a [power] blackout, terror attack, technology failure, or earthquake).” 62

An emergency is “an event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response.” 63 During an emergency there may be chaotic conditions, particularly if there is a disruption in normal communications.

A crisis is “an unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.” 64

Emergency management (also sometimes known as crisis management) is defined as “the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness [and] response.” 65

A plan is defined as “a scheme or method of acting or proceeding developed in advance.” 66

Combining the terms emergency management and a plan can lead to a definition of an emergency management plan as “a scheme or method of acting or proceeding developed in advance for the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness and response.” 67

62 ibid, p. 46.
"The objective of an [emergency management plan] should be to allow those responsible for the [facility] during an emergency to focus on the solution of major problems, not to attempt immediately to bring order out of chaos. If all predictable and routine items are considered in the plan, those responsible for actions during an emergency will be able to deal with the unpredictable or unusual situations that will surely develop."\(^{67}\)

According to Groner,

\begin{quote}
The chaotic and dynamic nature of building emergencies requires an exceedingly rapid assessment of the situation. The timeframe is measured in seconds and minutes, not hours and days. The rapid onset of many events means that the process should be well underway before emergency responders arrive at the building.

\textit{Human factors professionals have been actively researching this problem under the generally accepted term of “situation awareness.”} Endsley (1988) has provided a well-accepted definition: “The perception of the elements within the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.”\(^{68}\)

As noted in the definition, it is insufficient to understand the momentary status of the situation; projecting its development is of great importance in choosing a strategy to safeguard building occupants.\(^\bullet\)
\end{quote}

The purpose of an emergency management plan is to help hotel emergency staff in their efforts to achieve situation awareness and make sound decisions to provide for the safety of hotel guests and patrons during building emergencies, such as fire.

The value of emergency planning is not only the emergency management plan itself but also in the development process leading to it and the education of hotel emergency staff that should occur in the process.

---


\(\bullet\) - Achieving situation awareness is the primary challenge to optimizing building movement strategies prepared for the NIST Workshop on Building Occupant Movement during Fire Emergencies June 9–10, 2004, by Norman E. Groner, John Jay College of Criminal Justice, City University of New York, Department of Public Management, 455 West 59th Street, New York, New York 10019, e-mail: ngroner@jjay.cuny.edu. Groner (p. 2) went on to state in his paper that

Progress in helping building management and emergency responders achieve situation awareness will require a fundamental change in how we approach the design of building protection systems. At present, our buildings are not well designed to achieve the needed level of situation awareness, despite the availability of many technological tools. Addressable detection devices can pinpoint the locations of detection of hazards, but the building interfaces used to display the information \[\text{(do)}\] not supply an immediately comprehensible understanding of the situation. Technological devices like CCTV cameras and smoke detectors are not deployed in ways that help building management and emergency responders understand the status of key egress systems like stairs and corridors. Research and development towards the support of situation awareness in buildings is a priority.
How to Develop a Building Emergency Management Plan

The building emergency management plan* in Appendix 9–2 (which is on the CD-ROM provided with this book) is a suggested format for developing an emergency management plan for an office building. It includes actions intended to reduce the threat to the life safety of building occupants from emergencies, both fire and non-fire-related, that are likely to occur in a specific building, or in close proximity to it, until the arrival of emergency responders. A hotel could adopt such an emergency plan as part of its effort to develop its own building emergency management plan. However, several critical differences—building emergency staff organization, occupant documentation and training, and evacuation drills—need to be taken into account.

Building Emergency Staff Organization

The building emergency staff organization that will carry out emergency response procedures for a hotel differs from that of an office building. The most obvious difference is that hotels do not have floor response personnel such as floor wardens, stairwell monitors, elevator monitors, search monitors, and disabled/physically impaired assistance monitors. The responsibility for overseeing the safe and orderly evacuation of occupants from a hotel floor resides with hotel staff, including hotel management, security, engineering, and possibly housekeeping staff (the personnel involved will vary according to the size of the hotel, its staffing capabilities, and the time of day or night).

A typical staff organization** for a high-rise hotel is outlined in Figure 10–1. This sample depicts the fire safety director as reporting to hotel management. However, it is noted that the authority that has jurisdiction in many cities empowers the fire safety director with full authority to evacuate a building without the need to obtain approval from hotel owners or managers.

Each unit of the building emergency staff organization has duties and responsibilities that have been developed and tailored to the specific needs of the hotel and to each type of emergency they may be required to handle. These duties and responsibilities should be defined clearly so that there will be a coordinated and effective response to each emergency situation. For example, the duties and responsibilities of hotel management, the building fire safety director,*** and the hotel engineering and security staff**** in handling a fire emergency include ensuring that the fire department has been immediately notified, all occupants (including guests and patrons) in the affected area have been advised of the situation, any necessary evacuation procedures of occupants

---

*The emergency management plan presented here addresses preparedness and emergency response but does not address business continuity.

**Terminology for the emergency staff organization units and members may vary, and some facilities may designate additional team members (such as a building evacuation supervisor, an emergency coordinator, emergency evacuation teams, a crowd manager, and first aid officers).

***Smaller hotels may not formally refer to a fire safety director. The responsibility for coordinating the hotel's fire life safety program, including emergency response procedures, will reside with the hotel manager on duty at the time of an incident.

****In addition, building parking staff may be called on to assist in the evacuation of occupants from parking areas. Housekeeping and cleaning staff may be required to clean up areas after the occurrence of water leaks, liquid spills, and water discharged from sprinklers.
has begun, a thorough search is made of all affected guest rooms,\* fire life safety systems are operating under emergency conditions, any investigation or initial suppression of the fire is carried out, and that the fire department and other responding personnel are met on arrival and briefed on the status of the situation. In contrast, during a bomb threat incident, these personnel may be involved in supervising the evacuation of occupants and checking areas, including common areas and guest rooms, where an explosive device may have been placed. In a medical incident, security staff, depending on the hotel’s policy and the type of situation, may be required to administer CPR, an AED (automated external defibrillator), or basic first aid before the emergency medical responders arrive.

**Occupant Documentation and Training**

“Since hotel guests are [primarily] transients, special consideration must be given to the potential threat to their life safety from fire. For example, occupants of the residential portion of a hotel sleep in unfamiliar surroundings and could possibly become disoriented when trying to evacuate under heavy smoke conditions. Likewise, persons in ballrooms, lounges, [casinos,] and restaurants could become disoriented due to low-level

\* Guests may be asleep at any time of the day. Also, they may be in a deep sleep due to the use of alcohol, sleeping pills, or other substances and may require help to evacuate. Others, such as disabled/physically impaired persons, may need assistance. “Emergency evacuation of people with disabilities is a primary concern for security personnel. This is a matter that must be reviewed with local fire authorities. In the event of a fire, the fire department may prefer that they be met by a [hotel] staff member with a full list of disabled persons on the property and their locations” (Ellis Jr RC, Stipanuk DM. Security and Loss Prevention Management. 2nd ed. Lansing, MI: Educational Institute of the American Hotel & Motel Association; 1999:245). On checking into the hotel, guests may communicate the nature of any such disability or physical impairment to the reception desk staff. This information can be noted in the guest’s folio or other document so it is readily available, particularly during an emergency. Also, the authority that has jurisdiction may have special requirements for accommodating disabled/physically impaired guests.
lighting, crowd size, and unfamiliarity with evacuation routes.” The training of hotel occupants in fire life safety procedures is very different for a hotel than that of office building occupants. Apart from verbal instructions that can be given by meeting organizers at the commencement of a gathering in a function, a meeting room, or a conference center, primarily hotel management relies on documentation and exit signage to communicate safety messages to its guests and visitors.

Security and safety information—including basic security and fire life safety tips—can be provided as follows:

- When a guest checks in to the hotel (for example, printed on the paper folder containing the room key or keycard; some hotels include a statement that “Upon arrival please notify the Front Desk if you require special evacuation assistance in the event of an emergency”).
- Contained in a guest information book or a brochure provided in the guest room.
- Posted on the back of the guest room main entrance door. This information includes a floor plan with the emergency telephone number; a description of what the hotel fire alarm sounds like (and looks like if strobe lights are available); the layout of the floor including room locations, corridors, elevators, and the nearest fire exits; a “YOU ARE HERE” indicator for the guest’s room location; a directional path depicting the direction of travel to each of the nearest fire exits; and the location of manual fire alarm stations and portable fire extinguishers on the floor—see a sample sign in Figure 10–2.
- Portrayed in a program routinely broadcast to guests on in-room television channels.
- Written on decals (for example, those adhered to sliding glass doors above the locking mechanism to remind guests to lock the door when sleeping or leaving the room; those warning guests not to place a clothing hanger on any sidewall sprinkler head and thus avoiding damaging it and causing an accidental discharge of water in the room; and “NO SMOKING SIGNS” sometimes posted in guest rooms, particularly on room balconies).
- Displayed on the guest room door equipped with a conventional door viewer with a printed sign warning the guest to view the caller before opening the door.
- Displayed on in-car elevator video screens. Such elevator bulletins may, for example, provide information that reminds occupants that in the event the elevator stops running, they should immediately use the elevator emergency communication device to request assistance; or they may be used to post other appropriate emergency notifications.


American Hotel and Lodging Association Traveler Safety Tips.

Such information, including hotel liability notices, should be securely attached to the door. If it is removed and not replaced, the hotel’s liability increases. (Marshall A. At your risk. Hotel & Motel Management, June 16, 1997, as stated in Ellis Jr RC, Stipanuk DM. Security and Loss Prevention Management. 2nd ed. Lansing, MI: Educational Institute of the American Hotel & Motel Association; 1999:183).

The need to secure windows and sliding doors on outside patios and terraces is more critical on ground floor guest rooms, particularly those facing open parking lots.
HOTEL LAWS

Statements* of appropriate local, city and state laws applicable to hotel owners and operators for the loss of guest's personal property. Such statements may include the following details:

- Monetary limits of liability (often called “innkeeper liability”**) for the loss through damage, destruction, theft or otherwise of guest belongings (such as suitcases, trunks, hand luggage, or traveling bags) and the contents within, including a clause that specifies that unless there is a written statement from the hotel owner or operator agreeing to assume greater liability this will apply to all other kinds of personal property in the guest's possession.

- Information that a guest in-room safe or a safe deposit box is available and that the hotel will not be liable for any personal items (such as money, credit cards, jewelry, documents, airline tickets, clothing, laptop computers or other items of considerable value), unless they are placed in the provided safe or safe deposit box. In addition, there may be an innkeeper liability statement as to the monetary limits of liability for the loss of the aforementioned items when secured in the safe or safe deposit box, including a clause that specifies that unless there is a written statement from the hotel owner or operator agreeing to assume greater liability, this will apply to all these items so stored.

There may also be a statement as to the rights of the hotel owner or operator to seize the guest's property, including baggage, and other items under the guest's control, if the guest fails to pay their room bill including guest services provided, and the conditions under which the hotel owner or operator may sell these items.

The room’s maximum occupancy may also be stated here.

SECURITY TIPS

- Close guest room door and engage the deadbolt lock and the security latch or the safety chain. Check that any doors to connecting rooms are locked.

- Use door viewer to identify anyone seeking entry. Never open door for someone unknown to you. If in doubt of a person’s identity, contact the hotel operator.

- Secure valuables using the guest in-room safe or the safe deposit box available at the main reception desk.

- When leaving room, make sure any exterior sliding glass doors and windows are closed and locked and your hotel room door is fully closed and locked.

- Keep room key or access card always with you.

FIRE LIFE SAFETY TIPS

- Upon arrival in your room, note where each nearest fire exit is located on your floor.

- If you discover fire or smoke, notify anyone in the immediate area of danger and telephone the hotel operator (or first call the fire department emergency number and then notify the operator) to report the situation.

- When leaving your room, before opening the door, feel it with the back of your hand to ensure it is not hot because of a fire behind it. If it is warm, do not open it. If the door is cool, open it slowly and close it immediately if smoke or heat is encountered. If safe to leave, take your room key or card with you, close the door, and proceed to the nearest safe stairwell. If you encounter smoke on entering a stairwell, proceed to an alternate safe stairwell. Always close the stairwell door after you enter it.***

- DO NOT USE ELEVATORS.

- If there is heavy smoke in the corridor outside your room and you cannot evacuate, seal the bottom of the guest room door with towels, sheets or blankets, and notify the hotel operator of your situation. If breathing becomes difficult, and smoke is not present outside, open any windows or sliding glass doors leading outside to a balcony.

FIGURE 10–2 Sample sign on the back of a hotel guest room door.
Some guests, as a fire life safety precaution, on first arriving at their hotel room immediately familiarize themselves by walking to the emergency exits on their floor, in particular noting the route leading to the nearest fire exit. Guests can also play an important part in any hotel life safety program by promptly reporting things such as suspicious persons or activities, safety hazards, or the smell of smoke to hotel management and security staff.

Exit signage (as described in Chapter 6) is also a critical part of the life safety program for hotel occupants. This includes floor evacuation plans that show the building core, perimeter, stairwells, elevators, every wall that faces every exit route, exit routes to the appropriate stairwells, symbols depicting the location of fire equipment and manual fire alarm devices, the floor number, fire department and hotel emergency telephone numbers, what stairwells have roof access, and what the fire alarm looks and sounds like.

FIGURE 10–2 Continued.

Some guests, as a fire life safety precaution, on first arriving at their hotel room immediately familiarize themselves by walking to the emergency exits on their floor, in particular noting the route leading to the nearest fire exit. Guests can also play an important part in any hotel life safety program by promptly reporting things such as suspicious persons or activities, safety hazards, or the smell of smoke to hotel management and security staff.

Exit signage (as described in Chapter 6) is also a critical part of the life safety program for hotel occupants. This includes floor evacuation plans that show the building core, perimeter, stairwells, elevators, every wall that faces every exit route, exit routes to the appropriate stairwells, symbols depicting the location of fire equipment and manual fire alarm devices, the floor number, fire department and hotel emergency telephone numbers, what stairwells have roof access, and what the fire alarm looks and sounds like.

MEDICAL EMERGENCY TIPS

- Call the hotel operator (or call the paramedic/emergency services emergency number and then notify the operator), stating the nature of the emergency and the room number or the location.
- If properly trained, assist the victim, but do not move the victim unless there is danger of additional, more serious injury.

Included here may be a simple floor plan indicating:

- Emergency telephone number
- What the hotel fire alarm sounds like (and looks like if strobe lights are available).
- The layout of the floor including room locations, corridors, elevators, and the nearest fire exits
- A “YOU ARE HERE” indicator for the guest’s room location
- A directional path depicting the direction of travel to each of the nearest fire exits
- Locations of manual fire alarm stations and portable fire extinguishers on the floor.

There may also be a written advisement to the guest that if they have any questions regarding security or fire life safety issues they should contact the hotel operator.

[Note: The text contains a table and a figure, but for the purpose of this transcription, they are not included here.]

1The State of California Civil Code Section 1859 and Section 1860 and West’s Annotated California Code 1861 were consulted in preparing these statements.

2“‘The matter of limiting innkeepers’ liability goes far back in law. A cap on what an innkeeper must pay if travelers lose their belongings came about to protect those who provided shelter to people on the road—a desirable situation in the view of public policy—from being put out of business by visitors who sued after being robbed on the premises. In the United States, every state and territory has a law limiting this liability, and each state requires that notices of this be posted in a particular way.... Many of these limits were set in the last century, and inflation has made them out of date. In the last five years, some legislatures have been pushed by consumers into raising the limits” (Practical Traveler; How Safe Is the Hotel Safe? New York Times Log, by Betsy Wade. March 14, 1999. <http://query.nytimes.com/gst/fullpage.html?sec=travel&res=9B0DEFDD103FF937A25750C0A96F958260>; October 17, 2008).

3See “Evacuation Guidelines” in Appendix 9–3 for other possible items to include in this section.
Evacuation Drills
Hotels can utilize evacuation drills—commonly called fire drills—to train, instruct, reinforce, and test the preparedness of the hotel emergency staff, but due to the nature of hotel operations, they do not use this training tool for hotel occupants. This adds further weight to the absolute necessity for hotel staff to be always ready to react to an emergency in a competent and professional manner according to predetermined guidelines specified in the hotel’s Building Emergency Procedures Manual.

Important Consideration
It is important that as many as possible of those who will be involved in the execution of the emergency management plan participate in the planning process. Those concerned should include the emergency staff of the hotel, the hotel safety committee, and possibly public officials (such as those from the local fire and law enforcement agencies) and building management staff from neighboring buildings (with the view to developing mutual aid agreements). Public officials may require a particular format for the plan itself.

It cannot be stressed enough that the sample format for developing a hotel’s Building Emergency Procedures Manual is provided as an example of how a hotel may prepare its plan. Every site and hotel building is different, and emergency plans vary according to local laws and the requirements of the authority that has jurisdiction. It is up to each hotel to develop the emergency management plan most appropriate to its needs.

---

*A drill is defined by the NFPA. *Glossary of Terms, National Fire Code*, as “an exercise involving a credible simulated emergency that requires personnel to perform emergency response operations for the purpose of evaluating the effectiveness of the training and education programs and the competence of personnel in performing required response duties and functions” (National Fire Protection Association, Quincy, MA. Copyright 2005). A fire drill is such an exercise for a simulated fire emergency. The local authority that has jurisdiction will specify at what intervals the fire drills shall be conducted.

**Some hotels, particularly major ones, have a safety committee that meets on a regular basis. According to the *Safety Committees for the Real World*,

The purpose of a safety committee is to bring workers and managers together to achieve and maintain a safe, healthful workplace.... An example of a written safety committee policy is:

This safety committee was established to assist the company in achieving a safe, healthful workplace. The committee, through its representatives, will set specific goals to accomplish the following activities:

- Getting employees involved achieving and maintaining a safe, healthful workplace
- Identifying hazards and unsafe practices
- Ensuring that management investigates accidents and near-miss incidents
- Keeping accurate records of committee activities and recommendations
- Periodically evaluating the committee's strengths and weaknesses

Management will consider the committee's recommendations and respond to committee requests within a reasonable time

(Oregon Department of Consumer & Business Services, Oregon OSHA Standards and Technical Resources Section. <www.osha.oregon.gov/pdf/pubs/2341.pdf>:\1, 14). Some members of such a committee may be involved in the emergency management planning process for the hotel.

***A mutual aid agreement is “a pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement” (ASIS *Business Continuity Guideline*. Alexandria, VA: ASIS International; January 2005:8).
Summary

- “Because hotels offer such diversity of facilities and activities, no one security program will fit all properties. The security program must be designed to fit the needs and characteristics of the individual hotel. While crime is not always preventable, certain policies and procedures, properly implemented, may deter or discourage criminal activity.”  
- “Every establishment has to find the right balance for its environment—weighing the benefits of security against the extent to which each measure will inconvenience guests.”

- “Lodging property security efforts may involve such areas of concern as guestroom security, key control, locks, access control, perimeter control, alarm systems, communication systems, lighting, closed-circuit television, safe deposit boxes, inventory control, credit and billing procedures, computer security, staffing, pre-employment screening, employee training, responsible service of alcoholic beverages, emergency procedures, safety procedures, record keeping, and more.”

- Fire is a constant concern in hotel buildings. “Since hotel guests are [primarily] transients, special consideration must be given to the potential threat to their life safety from fire. For example, occupants of the residential portion of a hotel sleep in unfamiliar surroundings and could possibly become disoriented when trying to evacuate under heavy smoke conditions. Likewise, persons in ballrooms, lounges, [casinos,] and restaurants could become disoriented due to low-level lighting, crowd size, and unfamiliarity with evacuation routes.”

- The purpose of establishing, implementing, and maintaining a building emergency management plan is to provide for the life safety of all occupants within a hotel.

- The training of hotel occupants in fire life safety procedures is very different for a hotel. Apart from verbal instructions that can be given by organizers at the commencement of a function in the hotel, primarily hotel management relies on documentation and exit signage to communicate safety messages to guests and visitors.

Key Terms

Assembly occupancy. “An occupancy (1) used for a gathering of 50 or more persons for deliberation, worship, entertainment, eating, drinking, amusement, awaiting transportation, or similar uses; or (2) used as a special amusement building, regardless of occupant load.”

Atrium (plural atria). A large open space within a structure that is two or more floors high. Some buildings, particularly “larger-scale hotel building configurations often have atria two or three stories high and sometimes up to sixty stories high, which are...
often the focal point of building design. Atrium areas themselves may include several
occupancies or mixed functions associated with hotel operations.”

Bellhop. “Also bellboy or bellman, is a hotel porter, who helps patrons with their lug-
gage while checking in or out. They often wear a uniform like certain other page boys
or doormen. The job’s name is derived from the fact that the hotel’s front desk would
ring a bell to summon an available employee, who would “hop” (jump) to attention at
the desk in order to receive instructions.... Duties that are often included in this job are
opening the front door, moving luggage, valeting cars, calling cabs, transporting guests,
giving directions, basic concierge work, and responding to any of the guest needs.”

Business occupancy. “An occupancy used for the transaction of business (other than
those covered under “mercantile”) for the keeping of accounts and records and for
similar purposes.”

Concierge. Provides information and services to building tenants, residents, guests, and
visitors and performs other duties as specified by the facility.

Concierge floor. A hotel floor specially catering to guests (particularly business travelers)
who are offered extra service such as a room with upgraded bedding and turndown
service, access to a private lounge (some staying open from 6:00 a.m. to 10:00 p.m.
each day), separate meeting rooms, and complimentary meals, drinks, newspapers,
concierge services, and other amenities. Many concierge floors are access controlled
and therefore provide an extra layer of security.

Doorman. “An individual hired to provide courtesy and security services at a residential
building or hotel. They are particularly common in urban luxury highrises [and major
hotels]. At a residential building, a doorman is responsible for opening doors and screen-
ing visitors and deliveries. He [or she] will often provide other courtesy services such as
signing for packages, carrying luggage between the elevator and the street, or hailing
taxis for residents and guests.” At hotels they provide a wide variety of guest services.

Guest. In hotel buildings, this person “lodges, boards, or receives refreshment for pay
(as at a hotel ... or restaurant) whether permanently or transiently.” A guest is
sometimes known as a patron.

Guest folio. “A printout of guest activity while in [a] hotel.”

Hotel. “The term ‘hotel’ is an all-inclusive designation for facilities that provide com-
fortable lodging and generally, but not always food, beverage, entertainment, a busi-
ness environment, and other ‘away from home’ services.”

Hotel-residences. “Hotel residences have kitchens and everything else an owner would expect
in a typical abode, they also include amenities such as maid and room service, plus restaur-
ants, spas and gyms.... Typically, [these] residences are on the top floors of hotels.”

---

76 ibid.
Copyright 2005.
82 ibid., p. ix.
83 Olmsted L. Hotel residences: all the perks, none of the work. USA Today, 8D; September 19, 2008.
Inn. A lodging facility (such as a hotel or a motel) that provides food and lodging to guests. In Britain, it formerly referred to a place of residence for students.84

Innkeeper. The landlord of an inn or a lodging facility. See also landlord.

Landlord. A person or an organization that owns a facility and leases or rents it, or a part of it, to a tenant(s). See also innkeeper.

Lodging facility. A facility such as a hotel or a motel. See also hotel and motel.

Mercantile occupancy. “An occupancy used for the display and sale of merchandise.”85

Motel. “A general designation for lodging establishments that specialize in attracting the motoring public by offering parking accommodations. The distinctions between hotels and motels are gradually disappearing.”86 See also hotel.

Mutual aid agreement. “A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.”87

Occupancy. “The purpose for which a building or other structure, or part thereof, is used or intended to be used.”88

Patron. “A person who is a customer, client, or paying guest, [especially] a regular one, of a store, hotel, or the like.”89 See also guest.

PBX operator. A person who greets people telephoning a hotel. They answer callers’ questions, provide guidance, and direct calls to various hotel departments. Also, they handle guest inquiries and setting up wakeup calls. As well as these communications services, they may also be responsible for monitoring the hotel’s fire life system.90 Sometimes known as a switchboard operator.

Penthouse. A structure on the roof of a building to cover a stairway, elevator shaft, or other equipment, or a dwelling on the top floor or roof of a building.91

Premises security. “That combination of security measures (such as locks, fences, lights, closed circuit television, and security officer patrolling) in use at a premises (such as a hotel, apartment complex, and office building).”92

Slander. “The speaking of base and defamatory words tending to prejudice another in his reputation, community standing, office, trade, business, or means of livelihood.”93

Standard of care. “In law of negligence, that degree of care which a reasonably prudent person should exercise in same or similar circumstances. If a person’s conduct falls below such standard, he may be liable in damages for injuries or damages resulting from his conduct.”94

---

94ibid., pp. 1404, 1405.
Visitor. In hotel buildings it is a nonguest who visits a hotel guest or uses its facilities (such as meeting rooms, conference facilities, recreational facilities, restaurants, bars, a casino, or a discotheque).

Additional Reading


5. Ellis RC Jr, Stipanuk DM. Security and Loss Prevention Management. 2nd ed. Lansing, MI: Educational Institute of the American Hotel & Motel Association; 1999. This book contains excellent information about hotel security and loss prevention, including numerous case studies and premises security court cases; security procedures covering guest concerns, including proper safe deposit box procedures and swimming pool, sauna, hot tub, and exercise room safety; departmental responsibilities in guest and asset protection; the protection of funds, including accounting control procedures, physical protection of the accounting function, cashiering procedures, establishing credit policies and procedures, and an internal audit program; and risk management and insurance.


Residential and Apartment Buildings

The terms *residential building* and *apartment building* are used interchangeably in this book.

A residential building is a building containing separate residences where a person may live or regularly stay. Each residence contains independent cooking and bathroom facilities and may also be known as an apartment or a condominium.

A residence is “a temporary or permanent dwelling place, abode, or habitation to which one intends to return as distinguished from a place of temporary sojourn or transient visit.”¹

An apartment is “an individual dwelling unit, usually on a single level and often contained in a multi-unit building or development.”²

A condominium is “a multiple-unit structure in which the units and pro rata shares of the common areas are owned individually; a unit in a condominium property. Also, the absolute ownership of an apartment or unit, generally in a multi-unit building, which is defined by a legal description of the air space the unit actually occupies plus an undivided interest in the common elements that are owned jointly with the other condominium unit owners.”³

An apartment building is a “building containing more than one dwelling unit.”⁴

“Apartments differ from multi-unit residential occupancies that are not considered homes, such as hotels and boarding homes, by the provision of individual cooking facilities, the number of sleeping rooms, and the less transient nature of the occupants.”⁵

A residential and apartment building may consist of individual owner-occupied apartments, apartments leased or rented by the owner (either the building landlord⁶ or

---

²*Glossary of Real Estate Management Terms.* Chicago, IL: Institute of Real Estate Management of the National Association of Realtors®; 2003:8.
³*ibid.*, p. 32.
⁴*ibid.*, p. 8.
⁶*A landlord is a person or an organization that owns a facility and leases or rents it, or a part of it, to a tenant(s). In the case of an apartment building, the leasing will be of apartments.
the individual apartment owner), and public housing facilities. Residential buildings may also be occupied by students (as is the case with school and college or university dormitories). This chapter does not specifically address public housing facilities and student dormitories; however, much of the information presented herewith could be applied to those types of facilities.

Residential and apartment buildings also will usually “include parking facilities which may be open, enclosed, above- or below-ground, and often directly beneath or adjacent to the [residential and apartment building] itself. These arrangements may require special types of fire protection, and the building codes may require fire separations.”

To systematically examine the security and fire life safety of residential and apartment buildings, this chapter addresses the following areas: occupancy characteristics; assets, threats, vulnerabilities, and countermeasures; security programs; and emergency management.

### Occupancy Characteristics

In addition to individual apartments and residences occupying an entire floor, a part thereof, or possibly several floors with interconnecting staircases, other amenities may be available to the residents. Such services and activities may include “newsstands, retail shops, restaurants, cocktail lounges, health clubs, concierges, and other quality services. Generally, parking facilities are available [many of which include self-park and valet service]. Some have recreational facilities, such as saunas and swimming pools, while others may offer tennis and racquetball courts, gyms, and exercise rooms.” There may also be business centers, which include computers with high-speed Internet connections, as well as function areas, conference rooms, and private screening facilities that residents can rent or lease.

At any one time of the day, the number of residents in a residential and apartment building may vary according to factors such as their work status and age group. For example, if a high proportion of the residents are young or middle-aged business professionals, there will probably be a low concentration of residents during normal business hours (Monday to Friday, during daytime hours) when many will be at work; if a large number of residents are elderly retired people, there will likely be a high concentration of residents present during normal business hours. After hours, particularly late at night, most of the residents will likely be in the building (apart from those traveling on business and on holidays and vacation).

Generally speaking, residential and apartment buildings are managed by one group; this will consist of a building or a property manager and administrative staff,

---

plus support staff such as in-house or contract engineers, maintenance staff, security personnel, janitors and cleaners, elevator technicians, landscaping staff, and other vendors associated with building operations.

During normal business hours (Monday to Friday, during daytime hours), the building or property management staff will tend to be on duty (depending on the size and occupancy of the building, there may also be a property manager who lives on site). After hours (Monday to Friday, early evening until the next business morning; weekends and holidays), most buildings will have fewer numbers of engineers and maintenance staff, elevator technicians, and other support staff on duty. The actual numbers of staff will vary according to the size of the building, the services that it offers, the complexity of its operations, and the security needs of the facility.

After hours, building or property management staff (living either on or off site) can be contacted using communication means that include telephones, pagers, e-mail, and text messaging. Some buildings designate an on-duty manager to handle after hours calls relating to building operations.

Assets, Threats, Vulnerabilities, and Countermeasures

A risk assessment (as detailed in Chapter 4) is an important tool for developing an appropriate security and fire life safety program for a residential and apartment building. A “risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple low cost mitigation measures [countermeasures], but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with identified vulnerability, allow prioritization of resources to implement mitigation measures.”

Key steps in the process involve examining the assets, the threats against the assets, the vulnerabilities of the assets, and the countermeasures or mitigation measures that can be used to address identified vulnerabilities of the assets (within the confines of risk management). These areas are now examined for residential and apartment buildings.

Assets

Tangible assets in residential and apartment buildings include the lives of residents, visitors, contractors, vendors, and the apartment building staff; personal property contained within the apartments; and the building itself, its fittings, and its equipment. Building equipment includes of the electrical, water, gas, mechanical, heating, ventilating, air-conditioning, lighting, elevator, escalator, communication, security, and fire life safety systems. In addition, there are other types of assets that may include kitchen appliances, furniture and furnishings, entertainment equipment, antiques and works of art, cash and negotiable instruments, telephones, computers, printers, and general-use items for daily living—and assets in

common area vending machines, laundry facilities, fitness centers, saunas, swimming pools, spas/hot tubs, dining areas, restaurants, retail shops, newsstands, entertainment and business centers, and vehicles parked in the building’s parking garage.

Intangible assets include the livelihood of residents, visitors, contractors, vendors, and the apartment building staff; intellectual property and information stored in paper files, reference books, microfilm, and within computer systems and peripherals; and the reputation and status of the apartment building.

Threats
The types of security and fire life safety threats to residential and apartment building assets are outlined in Chapter 3. Briefly they include the following:

- **Security threats to people:** assault, assault and battery, kidnapping, manslaughter, mayhem, murder, robbery, sex offenses (including rape, sexual harassment, and lewd behavior), and stalking.
- **Security threats to property and information:** aberrant behavior, arson, burglary, cyberattack, disorderly conduct, espionage, larceny, sabotage, theft, trespass, and vandalism. In addition, there may be the disruption of building utilities such as water; electrical power; natural gas, sewer; heating, ventilation, and air-conditioning (HVAC); telecommunications; security; and life safety systems. Some security threats may involve terrorism.
- **Security threats to people and property:** bombs, chemical and biological weapons, civil disturbance, fires, hazardous materials, natural disasters, and nuclear attack.
- **Life safety threats:** aircraft collisions; bombs and bomb threats; daredevils, protestors, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstrations, and civil disorder; medical emergencies; natural disasters (earthquakes, tsunamis, volcanoes, heat waves, storms, and floods and landslides); contractible diseases (pandemic influenza, severe acute respiratory syndrome, and tuberculosis); power failures; slip-and-falls; stalking and workplace violence; traffic accidents; and water leaks.

Sometimes problems arise when residents have parties inside their apartments that cause excessive noise; likewise, the excessive use of alcohol or drugs can be the trigger for incidents to occur. Problems of a similar nature may occur in recreation and function areas that residents are using for social events.

Fire Risk in Residential and Apartment Buildings
Fire is a constant risk in high-rise residential and apartment buildings. “The occupancy hazards of apartment buildings include all risk factors that may arise in particular segments of the population. Preschoolers and older adults, if present, have a higher risk of dying in fires because of the mental or physical limitations associated with their age. Older children and younger adults may be at risk if they are physically or mentally handicapped, or as a result of drug or alcohol abuse. Fatal fires are more common at night when people are asleep.”

---

In discussing fire risk, it is helpful to analyze fire incident data for the four property classes—office buildings, hotels and motels, apartment buildings, and hospitals (and other facilities that care for the sick)—that account for the majority of high-rise building fires. Even though this data pertains only to the United States, it is worth considering because it includes the types of commercial buildings that are addressed in this book (namely, office, hotel, residential and apartment, and mixed-use buildings).

A study by Dr. John Hall, Jr., of the National Fire Protection Association’s (NFPA) Fire Analysis and Research Division, using statistics from the U.S. Fire Administration’s National Fire Incident Reporting System (NFIRS), stated that from 1987 to 1991, office buildings, hotels and motels, apartment buildings, and facilities that care for the sick, averaged 13,800 high-rise building fires per year and associated annual losses of 74 civilian deaths, nearly 720 civilian injuries, and $79 million in direct property damage. However, “most of these high-rise building fires and associated losses occurred in apartment buildings.” Hall added that for this period: “Only a small share of high-rise building fires spread beyond the room of origin, let alone the floor of origin.”

The most recent published study by Hall shows that “in 2002, high-rise buildings in these four property classes combined had 7,300 reported structure fires and associated losses of 15 civilian deaths, 300 civilian injuries, and $26 million in direct property damage.” He concluded that “these statistics generally show a declining fire problem over the nearly two decades covered” and, similar to his previous findings, “most high-rise building fires and associated losses occur in apartment buildings.” He further comments pertaining to the latter, “this may seem surprising, but it shouldn’t. Homes dominate the U.S. fire problem so completely that it is always a good bet that any newly examined fire problem, unless it is one that cannot occur in homes, will have its largest share in homes.” However, Hall did caution that, due to a number of factors (one being lower participation in national fire incident reporting in recent years) “the patterns shown in data available so far should be given limited weight.”

---

**“Here, ‘risk’ refers solely to the risk of having a reported fire” (Hall Jr JR. *High-Rise Building Fires*. Quincy, MA: National Fire Protection Association; September 2001:17).**

**“Tracking of the fire experience in [U.S.] high-rise buildings, however, has been less than systematic because the nationally representative fire incident data bases did not originally include reporting of height of structure. Reasonably good reporting began with 1985 fires…. NFPA [National Fire Protection Association] and other analysts have long used lists of particularly memorable incidents to study the high-rise fire problem, but these and other available special data bases are heavily weighed towards larger and more severe incidents” (Hall Jr JR. *High-Rise Building Fires*. Quincy, MA: National Fire Protection Association; September 2001:1).**

**“The term ‘motel’ is a general designation for lodging establishments that specialize in attracting the motoring public by offering parking accommodations. The distinctions between hotels and motels are gradually disappearing, however” (Beaudry MH. *Contemporary Lodging Security*. Newton, MA: Butterworth-Heinemann; 1996:ix).**

12ibid, p. 53.
132002 is the most recent year for which data was available for this report.
15ibid.
16ibid., p. 4.
17ibid.
18ibid., p. 3.
19ibid., p. 4.
It is worth noting here that O’Hagan, in his book *High Rise/Fire and Life Safety*, stated that high-rise residential building fires to some extent are different in nature and not as severe as fires in high-rise office buildings (see the earlier discussion in Chapter 2). Two of his stated reasons for this position are (1) high-rise residential buildings are typically of masonry construction and lack the empty spaces between the interior of their exterior walls and the outer edges of their floors (that typify the curtain walls of steel-framed [core construction] buildings) and (2) for privacy and usage reasons, residential buildings are typically compartmentalized with walls and partitions that have adequate fire resistance to withstand the fire until the arrival of the fire department; as a result individual fires are considerably smaller in area.\(^{20}\)

**Vulnerabilities**

Weaknesses that can make an asset (such as a residential and apartment building, and its operations, including the apartments, and the people who use the building) susceptible to loss or damage\(^{21}\) will largely depend on the building itself and the nature of its operations. A vulnerability assessment is required to “evaluate the potential vulnerability of the critical assets against a broad range of identified threats/hazards.”\(^{22}\)

**Countermeasures**

Mitigation measures to counteract identified vulnerabilities of an asset to a threat may consist of security systems and equipment (see Chapter 5), fire life safety systems and equipment (see Chapter 6), security personnel (see Chapter 7), security policies and procedures (see the next section, “Security Programs”), and emergency management (see the later section, “Emergency Planning”). These countermeasures need to be looked at in terms of security design. “Security design involves the systematic integration of design, technology, and operation for.... The process of designing security into architecture is known as Crime Prevention Through Environmental Design (CPTED).”\(^{23}\) As mentioned previously, the key to selecting appropriate countermeasures for a particular facility is for a risk assessment to be conducted. (See Chapter 4.)

Because fire is a risk in high-rise buildings, the following is noted regarding their fire protection features: residential and apartment buildings that have properly designed, installed, operated, tested, and maintained automatic fire detection and suppression systems and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes and automatic smoke control systems to restrict the spread of smoke—do have the necessary early warning systems to quickly detect fires and warn occupants (including residents and visitors) of their presence; and they also have the necessary automated sprinkler systems to quickly extinguish a fire in its early stages. One of the key issues here is the presence or absence of sprinklers.


\(^{22}\)ibid., p. iii.

In the study mentioned in the previous section, “Threats,” Hall commented on fire protection in high-rise buildings by stating,

In several instances, the value of these fire protection features [i.e., automatic extinguishing systems (primarily sprinklers), fire detection equipment, and fire-resistant construction] may be seen clearly in a statistical analysis of 1994–1998 loss per fire averages, with and without the protection. For high-rise buildings, automatic extinguishing systems are associated with a reduction of at least 88% in the rate of deaths per 1,000 fires for each of the three property classes (excluding office buildings, which had no deaths recorded in NFIRS [National Fire Incident Reporting System] in high-rise buildings) and at least 44% in the average dollar loss per fire for each of the four property classes. Fire detection equipment is associated with a reduction of 55% in the rate of deaths per 1,000 fires in apartment buildings. Fire-resistant construction is associated with a reduction of 30% in average dollar loss per fire in apartment buildings. This probably is produced not directly by the construction but indirectly by the compartmentation features that tend to be used with fire-resistant construction, features that keep more fires smaller and so keep property losses lower. (Note, though, that compartmentation practices probably vary more by type of occupancy than by type of construction.) Because high-rise buildings often use all three systems, it is very difficult to try to separate their effects on loss rates, and many rates are very sensitive to deaths or large dollar loss in individual incidents.

Automatic extinguishing systems and fire detection equipment and the compartmentation features associated with fire-resistant construction all contribute to fire protection by helping to keep fires small, with extinguishing and construction doing so directly and detection doing so by providing early warning that can lead to earlier manual suppression....

Finally, the effectiveness of these fire protection systems and features and their widespread use in high-rise buildings mean that when people are killed in high-rise residential fires, they are much more likely to have been close to the fire, where it is more likely that fatal injury could occur before [the] fire could be stopped or blocked by these systems and features.24

Security Programs

Security programs for residential and apartment buildings, and for individual residents, involve policies, rules and regulations, and procedures designed “to prevent unauthorized persons from entering, to prevent the unauthorized removal of property, and to prevent crime, violence, and other disruptive behavior.”25 Security’s overall purpose is to protect life and property.

Building Access Control

There are many different people who may, at any one time, wish to enter a residential and apartment building. They include building owners and management staff, building contractors (such as elevator technicians and engineering, maintenance, security, janitorial, and parking personnel), residents, visitors, salespersons, tradespeople (including construction workers, electricians, plumbers, carpenters, gardeners, telecommunications repair persons, persons replenishing vending machines, and others who service equipment within the building), building inspectors, couriers, delivery persons, solicitors, sightseers, people who are lost, vagrants or homeless people, mentally disturbed individuals, vandals, suicidal persons, protestors, and daredevils. There may also be others who try to enter building parking areas, laundry facilities, fitness centers, saunas, spas/hot tubs, swimming pool areas, dining areas, restaurants, retail shops, newsstands, entertainment and business centers, or an individual residence or apartment, with the sole purpose of committing a crime.

It is primarily the building owner and manager—with the cooperation of the residents—who determines the access control measures for this wide spectrum of persons. These measures aim to screen out unwanted persons or intruders and at the same time provide a minimum of inconvenience to building residents and their guests. When a security program is designed, occupancy characteristics such as the type of building occupancy, its pattern of use, and the time and day need to be considered. Varying degrees of access control can be achieved using security staff—in some residential properties they are known as a security officer, a security guard, a doorman, a concierge, or by other titles that differ according to the respective duties and responsibilities—and various security measures.

Building access controls include vehicle access to parking lots, garages and loading dock/shipping and receiving areas; pedestrian access to building lobbies, elevator lobbies, and passenger and freight/service elevators; and access routes to retail spaces, restaurants, promenades, mezzanines, atria, and maintenance areas. Measures for controlling access to these areas vary from site to site, depending on building management’s policy, but generally incorporate some or all of those described in the following sections.

Vehicle Access to Parking Lots or Garages

Access to parking lots or garages may be manual or automatic using a variety of methods that include the following:

1. Entry at will. There are no controls on the entry of vehicles (apart from possible vehicle height, weight, and width restrictions at the point of entry).
2. A vehicle detector embedded in the roadway, which automatically opens an entry gate or raises a gate arm.
3. A parking attendant, a valet, or a security person, stationed either at the point of entry or at a remote location linked to the point of entry by an intercom or a closed-circuit television (CCTV) system and a key switch or a remote control.

*In this context, a solicitor is a person who approaches building occupants with the intent to sell something, to ask for business for a company, to request charitable contributions, or to obtain magazine subscriptions. This definition would include people who beg or panhandle for money or food.
device that opens an entry gate, raises a gate arm, or lowers a surface-mounted traffic barrier.

4. A ticket (imprinted with the date and time of entry) dispensed by a machine at the point of entry that when withdrawn from the control unit automatically opens an entry gate or raises a gate arm.

5. An electronic access card, an alphanumeric key pad, or a vehicle identification system such as a transponder that opens an entry gate, raises a gate arm, or lowers a surface-mounted traffic barrier.

When exiting a controlled-access parking lot or structure, the driver usually will be required to submit to a similar procedure to that encountered on entry and then make a monetary payment (sometimes using a pay-on-exit machine) or use a token. Many access control systems with entry and exit card readers incorporate an antipassback feature. This prevents an access card from being used again to authorize entry of a second vehicle before the card has been used to authorize exit of the first vehicle.

**Vehicle Access to Loading Dock/Shipping and Receiving Areas**

Vehicles entering loading dock/shipping and receiving areas either may do so at will and park at whatever loading bays or docks are available, or they may be permitted to enter and be directed to park in certain areas by a loading dock attendant who will then supervise subsequent loading or unloading. (Some buildings keep loading dock doors and gates closed between delivery and pickup. Also, docks that are normally unattended may have an intercom or buzzer system, possibly in conjunction with CCTV, to allow drivers to remotely summon building staff for assistance.)

For security purposes, the dock attendant normally will maintain a log or record of the vehicle license plate number, the driver’s name and company, the time in, and the time out. Depending on building policy, vehicle keys may remain in the vehicle, or be given to the dock attendant for safekeeping and to permit the attendant to move the vehicle if necessary.

The activity of drivers and delivery persons usually will be confined to the loading dock/shipping and receiving areas, unless they need to proceed to residences or apartments for deliveries or pickups. For this reason, rest areas, toilet facilities, and pay phones often are provided in these areas. If drivers and delivery persons enter the building, they are usually required to notify the dock attendant of the specific residence or apartment they will be visiting and the approximate duration of their stay. They may also be issued special identification badges and be required to leave some form of personal identification (such as a driver’s license) with the attendant.

**Pedestrian Access to Buildings**

Pedestrians entering residential and apartment buildings during normal business hours may simply enter at will and proceed to whatever area they desire, or they may be asked to submit to some form of credentialing procedure before they are permitted to enter the facility and proceed to interior locations. The procedure in place may vary according

---

*For luxury residential and apartment buildings containing high-priced automobiles, a surface-mounted barrier can be a good physical obstacle that prevents a car thief from exiting a parking garage in a stolen vehicle. Of course, the vehicle owner should not leave inside the vehicle an item such as an access card that can be presented at the point of exit to lower the barrier and thereby permit exit of the vehicle.*
to the time (either normal business hours or after hours) and the day (either standard working days or weekends and holidays) that the access is requested.

**Normal Business Hours**

During normal business hours, access control for some residential and apartment buildings is relaxed and may solely rely on a security officer, doorman, concierge, or receptionist trained to observe both incoming and outgoing pedestrian traffic. Persons who are not residents may be challenged with a simple “May I help you?” Specific questions can then determine the particulars—for example, whether the person is a resident, is visiting a tenant (if so, which one?), is delivering or picking up items (if so, to whom? from whom?), or is servicing or inspecting equipment in the building (if so, where? at whose request?). These questions not only help screen out intruders with no legitimate reason for entering but also assist persons who need directions.

For other buildings, access control is stricter, using a variety of methods (including electronic access cards which are presented to readers at building entrance doors, lobby kiosks, on elevator bank walls or inside elevator cars, or to optical turnstiles; and possibly a combination of technologies for identity management). The degree of access control imposed by building policy will determine the percentage of unwanted persons successfully screened out. “The security program should be designed just tight enough to screen out as many intruders as it takes to reduce problems to the level that can be accepted. This means that a useful security program will rarely screen out all intruders.” Since the population density of residential and apartment buildings is not as high as office buildings, screening out all intruders usually does not result in unacceptable delays or inconvenience to the residents and visitors.

In a very large, more densely populated residential building, the screening of visitors may be facilitated by establishing a separate visitor center or using visitor management software to expedite entry. The former allows visitors to be moved to a separate staging area for processing. The latter is a password-protected, web-based management system that permits authorized users of the system to preregister visitors online before they arrive at a building. All relevant information about the visitor (such as name, person the individual will be visiting, time of visit, and any special instructions for handling the visitor) can be stored in a database and, in some cases, used to print out a visitor badge when the person is cleared for entry. This process not only facilitates visitor handling but also records visitor traffic. It also could be used to track the attendance of vendors and contractors (also recording company information in the database). Some systems even allow visitor self-registration using a scanned identification document, such as a driver’s license.

Access control to building maintenance spaces—mechanical rooms and floors, air-conditioning rooms, telecommunications and utilities access points, elevator machine rooms, and janitorial closets—and areas under construction or renovation is usually tight. Depending on building policy, persons accessing these areas may be logged in and

---

*In some luxury residential and apartment buildings, single elevators are sometimes dedicated for the exclusive use of high-profile tenants, particularly those occupying penthouse apartments.


**The value of visitor badges decreases if the visitor is allowed access to areas where occupants are not required to wear identification badges. In such a case, the visitor can simply remove his or her visitor badge and blend in with the regular occupants.*
out, required to wear special identification badges, given keys (although issuing keys to vendors or visitors can be a security risk) or an electronic access card (if the card is not returned, it can be immediately deactivated) to a particular area, or provided an escort. Some contractors servicing certain types of equipment in specific building areas may be permitted to install their own locking devices at access points leading to this equipment (see further comments in the “Key Points to Consider” section later in this chapter). Main electrical switchgear and power transformer rooms are usually deemed such a life safety risk that building personnel are not issued keys to these areas.

After Normal Business Hours

After normal business hours, access control to most residential and apartment buildings and interior areas is usually strict. An obvious way to provide off-hours access to a residential and apartment building would be to furnish keys to all building occupants or to those who need to enter the facility after hours. This approach, however, can have disastrous consequences proportional to the size of the building and the number of occupants. A heavy workload and costly expense can be created by lost keys, keys not returned by departing residents, and the necessity of rekeying building entrances and reissuing keys to residents every time a key has gone astray. In addition, there may be the problem of unauthorized duplication of keys. To avoid all of this, most buildings never issue building access keys to tenants but rely on some way of verifying a person’s right to enter the building. This verification may involve the following procedures.

Visual Recognition

Building security staff, a concierge, or a receptionist may verify on sight a person’s right to enter. Several problems may result, however, from this form of verification. For example, although the chances are slender, someone who closely resembles a resident may be admitted in error. Also, particularly if the building is large with a high number of residents, it will be difficult for security staff, the concierge, or the receptionist to recognize all persons authorized to enter. If there is a change or substitution of the security staff or receptionist, the new person will not be familiar with the persons authorized to enter. This may result in the questioning of residents who normally are never challenged and subsequent complaints to building management. Finally, if the security staff is distracted by another duty, an unauthorized person may gain entry without being observed.

Authorization Documents

A document (a letter, a memorandum, or an e-mail) listing those authorized for after-hours access may be provided in advance to security staff at the building entrance. Persons requesting access will identify themselves to building security staff. Security will check the individual’s name (which should be confirmed by a driver’s license or other photo identification) with the names listed in the document. In some buildings, residents will provide management with a written request listing the names of the persons involved and the time after-hours access is permitted. Building security staff, the concierge, or the receptionist can set up a file sorted alphabetically by tenant name, or by the last name of the person to be granted access, to minimize time spent searching for the appropriate authorization. Building security staff must thoroughly check all documents authorizing access to ensure that the decision to grant access is valid.

Building Access Control Systems

Electronic access control systems can provide after-hours access by operating a building entry door.
Resident Systems
An electronic access control system can allow a resident to present an access card or a key fob to a card reader outside a building main entrance door. Depending on the type of system, an intercom, a telephone, or a CCTV camera may also be provided at this point of entry. If there is a problem using the card, the resident can use the intercom or telephone to communicate with onsite security staff or an offsite central monitoring station. If the person's right of entry is confirmed, the staff can grant access in person or remotely.

Once a resident is inside a building lobby, his or her progress can be controlled using a variety of methods. These include electronic access cards being presented to readers at lobby kiosks, on elevator bank walls, inside elevator cars, or to optical turnstiles, and possibly a combination of technologies for identity management.

For security reasons, most building access cards display only a sequential number and, if used with an insertion or swipe-type card reader, an arrow depicting the correct way to insert or swipe the card. Then, if a card is lost, there are no identifying marks to indicate where it may be used. An advantage of an electronic access card is that when a resident no longer resides at a building, a computer can be used to deactivate the card, eliminating the need to retrieve the card itself.

Visitor Systems
A building telephone entry system or a voice-over Internet protocol (VoIP) entry system can allow direct communication by a person seeking entry outside a building to an individual apartment using a telephone line or VoIP. The resident can then remotely operate the building entry door to allow the guest to enter the building.

Also, there are systems available that, for example, enable residents to be “given access to live camera views in the [building's video] surveillance system via two modes: either through their web browser Internet access set up in the Milestone [IP video management] software and viewed on their computers; or through a special cable TV channel provided by the telecom provider to the [building]. This gives all residents a camera view of the entrance to the building, so that they can check who is calling on the intercom.”

The resident can then refuse entry or remotely operate the building entry door to allow the visitor entry to the building.

After-Hours Access Register or Log
Whichever access control procedures are used, some residential and apartment buildings maintain an after-hours access register or log to record after-hours access activity. In this log, details such as the person’s name (printed for legibility) and signature, the name of

---

*Key fobs are increasingly used in apartment buildings and condominium buildings for access to common areas (i.e., lobby doors, storage areas, fitness room, pool). These usually contain a passive RFID [radio frequency identification] tag. The fob operates in much the same manner as a proximity card to communicate (via a reader pad) with a central server for the building, which can be programmed to allow access only to those areas in which the tenant or owner is permitted to access, or only within certain time frames” (Key fob. Wikipedia. November 8, 2008. <http://en.wikipedia.org/wiki/Key_fob>; November 13, 2008).

the resident he or she is visiting, the date, and time in and out are included. In case of an after-hours building emergency, the log can be used to help ascertain who is in the building. However, the register or log does not provide a record of all persons in the building after hours, because some persons will have accessed the building during normal business hours before the access control log was in use. To determine exactly which tenants are in the building after hours, it would be necessary either to telephone or to personally visit every tenant. Such a procedure, particularly in large office buildings, is not considered practical.

**Right to Pass Signs or Plates**

Signs or sidewalk plates, generally located outside the building, may state the following:

“RIGHT TO PASS BY PERMISSION, AND SUBJECT TO CONTROL, OF OWNERS” or “PERMISSION TO PASS REVOCABLE AT ANY TIME.”

If a person who does not have a legitimate reason for being in the building is discovered, then the owner, manager, or agent acting on behalf of the building may revoke the person’s right to remain. After being told to depart the premises, those who refuse to leave may be subject to arrest by law enforcement. Also, anyone reentering a building after having been warned that he or she is not authorized to enter may be treated as a trespasser.

**Apartment Access Controls**

Entry to residences and apartments is primarily the responsibility of the residents themselves. Whether they are leased or owner-occupied apartments, residents have control over their own premises. (However, if an emergency makes it necessary for property management or an outside agency, such as law enforcement, to enter an apartment, a minimum of two people should enter. If a second individual is not available and if the situation and time permit, at least a second person should be notified of the requirement to enter before it is accomplished.) Entries into residences and apartments should always be thoroughly documented.

**Unwanted Solicitors**

Residents can play an important role in building security by reporting solicitors. Solicitors may come to buildings with items for sale secreted in a bag or a briefcase. If they can obtain entry through the building lobby, once on a floor they will open up the container, take out their product, and proceed from floor to floor, resident to resident, selling their merchandise. Even though solicitors may be legitimate, their presence is disruptive to residents; furthermore, criminals can pose as solicitors. The resident should

*Depending on the circumstances, they should knock on the door before opening it and call out loudly to identify themselves and their intentions. Such actions can help avoid embarrassing and awkward situations and protect from unfair accusations. Intrusions into residences and apartments should always be thoroughly documented.
never buy anything the solicitor is selling. To do so provides an excuse for the solicitor to attempt to return to the building.

Residents should report solicitors to building security as soon as possible, with a detailed description of the person involved. Residents are not expected to put themselves in harm’s way by delaying the person until security can respond to escort the solicitor out of the building.

**Apartment Security Systems**

Some residents install their own access control systems to monitor entry to their apartments. Sometimes, CCTV systems, intercoms, and intrusion detection systems are used. When considering a system, the local fire authority that has jurisdiction should be consulted to determine whether local codes and standards permit such an installation—this is particularly important when the access control devices are to be installed on doors leading directly from elevator lobbies to the apartment. These doors involve paths of egress during emergency evacuation and therefore require special locking arrangements permitted by the authority.

**Doors Locked**

It is important that residents *never* open their doors for anyone they do not know personally. Some residents equip their main entrance door(s) with a conventional door viewer (sometimes called a view port) to provide a clear view of the other side of the door (using a hollow end or peephole to look through and a lens at the other end to give a wide viewing angle). This allows the resident to see the person requesting entry before granting or denying access. Also, digital door viewers are available. Such a device “includes an LCD monitor that mounts on the inside of the … room door with a digital camera on the outside to provide a clear and effortless view.”

**Resident Lock-Outs**

If a resident accidentally locks him or herself out of the apartment and needs entry, there must be a clear policy to handle such requests. Some buildings require the resident, after he or she has been positively identified, to complete and sign a “Permission to Reenter” or “Resident Access Authorization” form. Others require designated building management personnel to be notified before access is granted. These arrangements are often detailed in already-executed written agreements entered into by the tenant with the building owner or operator.

**Escorts of Building Users**

People in residential and apartment buildings may be escorted for a variety of reasons. It may be to protect individuals or the property that they are carrying. It may also be to show a person where to go or to ensure that the person does not remove property. In the high-rise setting, building users can be escorted to, from, and within the building, and within resident areas.

---

Chapter 11 • Residential and Apartment Buildings 565

Escorts to and from the Building
Escorts to and from a building usually occur after normal business hours. Security staff members generally conduct these escorts. Residents, particularly older residents or females, may request building security to escort them to areas of the property such as parking garages. Building policy should dictate how, when, and where the escorts are to be conducted.

Escorts within the Building
Building policy may require that persons needing access to certain maintenance spaces and areas under construction or renovation be provided with an escort to accompany them whenever they are in these areas. Building engineering or security staff may be required to provide such escorts.

Some buildings have a list of local and state agencies whose inspectors are authorized to enter, but it is absolutely critical to verify the identification of these individuals and to make building management aware (if possible) of their presence before they are granted entry. It is important to escort anyone claiming to be an inspector while he or she is in the facility. On occasion, professional burglars posing as local or state inspectors have been granted entry to buildings.

Also, if janitorial personnel are employed to clean apartments, they may require escorts when they are removing trash material from building floors and transporting it to trash compactors and dumpsters.

Property Control
Objectives of controlling property that moves in and out of residential and apartment buildings are as follows:

- To prevent stolen property or other unauthorized items from leaving. Stolen property may include resident’s kitchen appliances, furniture and furnishings, entertainment equipment, antiques and works of art, cash and negotiable instruments, computers, printers, general-use items for daily living, and sometimes items and equipment from common area laundry facilities, recreation areas, dining areas, restaurants, retail shops, newsstands, entertainment and business centers; it may also include property from vehicles parked in the building’s parking garage.
- To prevent dangerous items entering. Items such as explosives, illegal drugs, and hazardous material might easily be secreted on a person or in a vehicle and brought into a building.
- To prevent unnecessary or disruptive delivery traffic. By keeping out misdirected deliveries, unnecessary traffic is avoided. By routing deliveries through proper entrances, such as loading docks and freight/service elevators, disruptive traffic is avoided and, in some cases, the building and passenger elevators are protected against damage from hand trucks and bulky crates. By intercepting deliveries at these entrances to the building, it may be possible to detect intruders posing as delivery persons.

It is difficult, and often unnecessary, to implement strict property control measures in a residential and apartment building, because residents are primarily responsible for their

own apartments and belongings. The use of property removal passes and asset tracking systems to control property is not common. However, the removal of large items from a facility, particularly those from a residence or an apartment, should be scheduled ahead of time and any such unscheduled activity reported immediately to building management. Requiring building residents and visitors to pass through one particular supervised point to enter or leave the building increases the possibility of detecting unauthorized removals.

Security staff should also be alert for people who act in a suspicious manner, as well as for objects, items, materials, or parcels that look out of place or suspicious. It is most unusual for vehicles, even those entering under-building residential parking garages and loading dock areas, to be inspected. Restriction of parking in residential parking garages to only residents and authorized building staff is a sound security measure.

Good housekeeping should always be practiced for trash (rubbish) storage, trash compacting, and dumpster areas.

**Couriers and Delivery Persons**

Residential and apartment buildings have service deliveries of items such as mail, prepared food, groceries, newspapers, laundry, and various other items. Also, sometimes couriers come to a building to perform deliveries or pick up laundry, packages, and sundry other items. The entry of such delivery persons and couriers needs to be strictly controlled. Some buildings allow these persons to go to the appropriate residence after they have been screened for entry by building security in the main lobby reception area.

During mail delivery hours (usually 9:00 a.m. to 5:00 p.m., Monday through Friday), when many residents are not available to accept package deliveries, many buildings have centralized, wall-mounted mail receptacles where each resident has an individual mailbox for deliveries to be deposited. However, “with the growing Internet shopping trend and magazine subscriptions still growing strong, more parcels and larger pieces of mail are delivered daily. The typical mailbox—especially the smaller boxes commonly used in apartment buildings—is not large enough to accommodate these larger items.”

This may lead to larger mailboxes and parcel lockers being required in larger apartment buildings where an alternate delivery mechanism (such as a concierge or a security officer able to accept deliveries on behalf of the residents) does not exist.

For security and safety reasons, some residential and apartment buildings do not permit security staff or a concierge to accept any deliveries. The building does not want to accept the responsibility and potential liability of accepting items the resident may later refuse (such as certain legal documents); also, packages may contain dangerous or illicit items. Some buildings permit the acceptance of after-hours packages on certain occasions and under special circumstances. This usually requires a written request by the resident and an explicit understanding that the building and its agents are absolved from any liability resulting from acceptance of the package on behalf of the resident.

Like any well-run operation, such programs need to be meticulously documented to provide an audit trail to track deliveries and pickups and ensure that these tasks are

---

*For security measures to screen for people- and vehicle-delivered explosive devices (see Chapter 9).

**After which they may be issued special identification badges and required to leave some form of personal identification (such as a driver’s license).


***The resident is later notified and asked to pick up the item concerned, or a security officer or a concierge later delivers the item to the resident’s apartment.
being done in a timely manner. If there is a question about the time property was picked up or items delivered, or about the individual who signed for it, accurate records should be immediately available for review.

**Construction and Remodel Activities**

When the apartments are being constructed and remodeled, the security department needs to be a critical part of the operation. It is particularly important that access control measures are in place to prevent the unauthorized removal of property.

**Lost and Found Property**

Handling lost and found property is an often-neglected but critical part of an effective security program. Most people can recall the anguish they felt on discovering that a valuable personal possession or business item was missing. Likewise, one may remember the exhilaration at being contacted and informed that the missing property had been found and was available for pickup.

If property is lost in a building and is subsequently found and handed to building security staff, the item should be kept in a secure place and, if possible, expeditiously returned to its rightful owner. This can considerably enhance the trust and confidence that building residents and visitors will have in the building security operation. Just the opposite will be true if a tenant learns that the found item was handed to building security staff and was then lost or went missing.

**Lost and Found Property Log**

Building security staff should maintain a list of lost and found items in a lost and found property log. The log should contain details such as the following:

- A brief description of the property, including any serial or asset tag numbers
- The date, time, and place the property was lost or found
- The identity of, and means to contact, the person who lost or found the property
- If the property is claimed, the identity of, and means to contact, the claimant and the signature of the person who received the property
- The name(s) of the person(s) who took the report of the lost property, logged in the found item(s), or handled the return of the property to its rightful owner.

**Handing Over to Local Authorities**

If the lost property is particularly valuable or sensitive, it may be necessary for the local law enforcement agency to be contacted; if the property is subsequently handed over to authorities, this fact, including the identity of the receiving law enforcement officer, should be noted. A receipt for the property should be obtained. Local and state laws often determine the handling of lost property. *

Some jurisdictions allow found property, when its owner is unknown and its value is below a certain amount, to be distributed to local charitable organizations. Others,

*For example, in California, Section 2080 of the California Civil Code does not require a person to take charge of found property, but if the person does, he or she can be sued for the negligent handling of it. The law further provides that if the owner of lost property is known, the property must be returned to that owner. If the owner is not known and the property has a value above ten dollars, the property must be turned over to the local police within a reasonable period of time (American Protective Services. Administrative News. Oakland, CA; 1993:4).
after a certain waiting period, auction the property or allow the finder to assume ownership of it.

**Trash Removal Control**

The design and implementation of trash removal controls will largely depend on the specific cleaning operations in effect at a building. For apartments that are owned and occupied, or leased or rented from the owner, the residents themselves will usually be responsible for keeping their own apartments clean. They may do it themselves or hire a cleaner to periodically clean the apartment. Building trash chutes may be provided for the residents to dispose of trash, or the building may arrange for trash to be collected from each floor.

Building management will use cleaning staff to clean common areas, including facilities provided by the building for the residents. To facilitate scrutiny of any trash removed from these areas, the bags used by these staff should be made of transparent plastic. Also, CCTV cameras in the dock areas may be used to deter the removal of items from trash bags before they are placed in dumpsters, compactors, or holding areas, or for later retrieval from the receptacles themselves.

Cleaning staff may be required to enter and leave the building through an employee entrance and be subject to certain property screening procedures. The object of the screening procedure is to observe any prohibited items being brought into the building and to detect any stolen property being removed from the building. As part of preemployment or preassignment agreements, cleaners may be asked to submit to a visual inspection of any items they are carrying to and from work—lunch pails, bags, backpacks, packages, and so on. The frequency of the inspections can be established as part of the agreement: inspections may be conducted every time the employee enters or leaves the building, at random, or only with cause. Depending on the number of staff employed (it may be only one or two for many apartment buildings), a cleaning supervisor or a member of building security may conduct these inspections. They are visual only, and employees are requested to open appropriate items themselves. Under no circumstances does the inspecting person touch the items being inspected or attempt to inspect any part of the employee’s person or clothing. All persons have a legal right and expectation of privacy, so items such as purses will be subject to inspection only under special circumstances, the nature of which should be established in writing beforehand. Some operations require janitorial staff to wear special clothing or smocks in which it is difficult to conceal items.

**Key and Electronic Access Card Control**

In residential and apartment buildings, keys and electronic access cards to the facility are under the control of building management, engineering, and usually security personnel. Building management personnel obviously need to have keys to gain entry to all areas of the facility they manage. Building engineers, because of the nature of their work, also need access to virtually all areas, including residences and apartments. Depending on how the building is managed, security staff also will have access to most areas.

**Key Control**

The decision as to whether master keys are issued to building security staff will vary from building to building. If they are not issued master keys, they will often be issued a
ring of keys, permitting them to enter various parts of the building. Many facilities keep apartment keys out of the routine possession of security staff but provide a controlled, documented means for these keys to be obtained if necessary. During emergencies and other special circumstances, security staff can obtain these keys quickly. After the situation has been resolved, the keys are again placed under supervision, perhaps in a locked cabinet or a key cabinet secured with a key, a lock code, an access card, or a consecutively numbered seal.

Keys issued to the security staff should never be permitted to leave the facility. They should be passed from shift to shift and a receipt should be recorded each time they change hands. All security personnel understand the importance of not permitting keys to be compromised.

Key Points to Consider

Keys should be issued only to those persons who can be entrusted with them and who have an *absolute* need for them. The status a key holder may feel by possessing certain keys should not enter into the decision-making process. The following points are important to consider:

- Residents should be issued keys that pertain to their residence only.
- Residents should never be issued building entrance keys. (If issuing entrance keys is unavoidable, the locks should be changed periodically or when a key has been lost or taken, and new keys should be issued to the residents authorized to have them.)
- Residents should not be allowed to duplicate keys. (Keys should be marked “Do Not Duplicate” as a deterrent to duplication. Also, keys issued to residents may be distinctively marked to help identify unauthorized keys they may have had cut themselves.)
- When a resident moves out, all apartment door entry locks should be changed.
- Janitorial staff should be issued keys only for the time they require them and for the particular areas to which they require access. Depending on the size of the janitorial staff, designated supervisors within the janitorial operation may be issued master keys that, for instance, provide access to the residences on an individual floor. In this way, the general cleaning staff does not need to be issued keys. In some buildings, no janitorial staff members are issued keys, and security staff must unlock the appropriate doors and relock them after the work is completed. Procedures will vary from building to building depending on size, complexity, and the manner in which cleaning is conducted and trash is removed.
- Elevator, escalator, dumbwaiter, rubbish chute, laundry and linen chute, and moving walk technicians may be permitted to carry keys that provide access to their equipment, or the building may retain possession and issue the keys only as needed.

In some buildings, telecommunications technicians and gas, water, and power utility workers are permitted to attach their own locking devices to areas containing their equipment. This practice is convenient because building staffs are not required to open

*For additional information on the control of keys, see Chapter 5, “Key Control.”*
these areas, but it compromises security because the control of keys and the areas themselves has been lost. These areas could be used to store unauthorized or stolen items, and general housekeeping may become a problem. If this practice is permitted, no one should be allowed to place a lock on a door without building security or other building departments (such as engineering) having a key. In an emergency, keys must be available for access. A possible alternative is for contractors to store their equipment, including tools, in heavily reinforced large steel boxes, chests, and cabinets that can be secured using high-security padlocks that are protected from attack with cutting tools.

In the event of a lost key, the circumstances surrounding the loss should be fully investigated and thoroughly documented.

Mobile Patrols

Mobile patrols may be conducted in residential and apartment buildings for a variety of security and fire life safety purposes. “Guards [security officers] are typically highly visible thus offering something of a deterrent effect and at the same time imparting a sense of security to the building’s tenants and visitors.” Patrols can also be used to note and quickly address anything significant or unusual affecting security or fire life safety. After conducting a risk assessment (as described in Chapter 4), the purpose, frequency, and routing of patrols can be determined by management and the security department (and, if special circumstances warrant, with the cooperation of local authorities) and then carried out and thoroughly documented.

When and Where?

Patrols by security staff in residential and apartment buildings may occur as follows:

- Depending on a building’s usage, patrols may also be conducted in swimming pool and spa areas, public parks, gardens, retail arcades, and other areas, with times varying according to the operating hours.
- When the building is normally closed (some buildings require such patrols continuously) throughout all common and maintenance areas (including stairwells), to report obstructions (particularly those blocking emergency egress routes), fire hazards, broken glass, missing equipment (such as portable fire extinguishers), water or gas leaks, wet floors, holes, defects in floor coverings, tiles missing, unsecured areas, malfunctioning lighting equipment, signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong, and so on.
- Continuously in parking garages and lots to deter theft of vehicles and property within them; note parking violations and issue warnings or citations; observe


31In some buildings, the patrolling officer carries a pager, a mobile telephone, or a hand-held panic alarm so that tenants, particularly retailers, can summon the officer for assistance.

31Violations include vehicles improperly parked, parked in a NO PARKING zone or space, parked in a RESERVED zone or space, or parked in a DISABLED/PHYSICALLY IMPAIRED designated space. When placing such a notice on a vehicle, locating it in the lower corner of the driver’s window (immediately above the door handle) will make it visible to the driver when entering the vehicle but will not obstruct his or her field of vision when driving. Also, if the notice is made of nonadhesive material, it will be easily removed from the glass.
vehicle lights or engines left on, leaks from vehicles, or other unusual conditions of parked vehicles; report fire hazards, water or gas leaks, malfunctioning lighting equipment, broken vehicle windows and other signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong; and provide for the general safety of tenants and visitors. (Motor vehicles, electric carts, bicycles, tricycles, and personal transporters may be used for patrolling large parking areas with long travel distances.)

- On building floors and in parking garages, patrol stations are often installed at each stairwell so that the patrolling officer must traverse the floor in order to complete the tour.
- To perform a fire watch when a building has exceptional hazards or the fire protection system is impaired. • A fire watch is “the assignment of a person or persons to an area for the express purpose of notifying the fire department and/or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety dangers.”

**Patrolling Tips**

- Patrols can be conducted either on foot or using a motor vehicle, an electric cart, a bicycle, a tricycle, or a personal transporter.
- There should be reliable communication between the patrolling officer and the security department or the supervisor.
- Whenever possible, routine patrols should be conducted in a random, unpredictable manner to avoid a fixed pattern or routine that someone planning to commit a crime can observe. Sometimes, an effective tactic is for an officer to “double back,” or retrace steps to a previous location; anyone observing the patrolling officer’s movements would usually not expect the officer to return quickly to an area just visited.
- “Alertness, interest and thoroughness must be displayed. A suspicious mind must be cultivated and anything that appears other than normal must be looked into.”
- Using a flashlight or a torch in areas where lighting is poor or nonexistent is extremely useful.
- “A simple but effective patrol plan should be established in each area. Its efficiency should be regularly checked by means of [patrol management devices], radio or telephone checks at regular intervals, etc. Failure to report, or deviation from

---

For example, in the United States, according to NFPA 601, *Standard for Security Services in Fire Loss Prevention*, Chapter 3, Security Functions and Duties, “a security officer shall make rounds at intervals determined by management. When operations in the property normally are suspended, officers shall make rounds hourly or as assigned by management. Where special conditions exist, such as the presence of exceptional hazards or when fire protection equipment is impaired, management shall institute additional rounds. The first round shall begin within 30 minutes after the end of activities of the preceding work shift. During this round, the security officer shall make a thorough inspection of all buildings or spaces” (Section 3-2.1-3.3.2.2).


**See the section “Patrol Management Devices” in Chapter 5.**
described assignments, should immediately be investigated.” Patrol management devices “provide the security manager with a consistent record of rounds and occurrences at a facility without the need for human supervision to ensure that rounds are completed as assigned.” If an electronic patrol management device is not used, a notebook is very useful for recording observations. (The patrolling officer can carry the notebook, or it can be positioned at designated patrol stations so the officer can record when visiting a particular area.)

Resident Security Education

There are many ways to educate building residents about the building’s security program. All building residents and their visitors should be made aware of the program and how various policies and procedures affect them. If people are aware of the logic behind security regulations, they usually are more willing to comply with them. This communication can be achieved in the following ways:

- Explain the regulations on an informal, as-needed basis. For example, building security staff may explain to a visitor the purpose of calling a resident before he or she can be admitted.
- Use posted signs; written policies and procedures published in the Resident Manual and on the building’s website; pamphlets, leaflets, flyers, newsletters, e-mails, and video training materials supplied by building management to the resident. Sometimes, information is displayed on in-car elevator video screens. Such elevator bulletins may, for example, provide information that reminds occupants that in the event the elevator stops running, they should immediately use the elevator emergency communication device to request assistance; or the bulletin may be used to post other appropriate emergency notifications. Appendix 9–1 on the CD-ROM provided with this book is a Sample Resident Security and Safety Awareness Checklist that could be revised and sent to residents at appropriate times during the year.
- Conduct security and safety orientation lectures, classes, briefings, workshops, and seminars. These events can be an effective medium, not only for communicating to residents what is required of them in the building security program but also as an opportunity to educate employees about basic security and safety measures they can adopt at home. (Such measures could include being aware of their surroundings, elevator safety, securing vehicle doors and windows, not leaving valuable items in view in parked vehicles, securing their residences and personal property, and reporting any problems in common areas.) The length of such events

---


*A Resident Manual (or Resident Information Manual) is usually supplied by building management to each resident. The manual is “a compilation of management policies and procedures that relate to [residents] and the use of their leased [or owned] space” (Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:171).

**For example, residents should be made aware that when they are about to enter an elevator, if they observe a suspicious person inside the car they should not proceed but simply wait for the next elevator; or if, while inside an elevator car, they similarly notice such a person, they may consider exiting the elevator as soon as possible or, if others are present, follow them when they disembark. “Never doubt your instincts. If you
will vary, but 45 minutes to an hour is probably the maximum that residents will permit. As with all effective teaching, the use of audio-visual aids—films, videotapes, DVDs, and slides—can help gain the attention of participants and assist in effectively communicating the required message. The frequency of classes, meetings, conferences, seminars, and workshops will vary from building to building; they may be regularly scheduled or conducted when a specific need arises. More will be said about the training of occupants, floor wardens and building emergency staff in the next section, “Emergency Planning.”

The residents themselves are an important part of any building security program. They should be educated to know that they are the eyes and ears of the building. Although the residents are not expected to be trained security professionals, they are expected to be active participants in the building security program by being aware of their surroundings and promptly reporting potential security problems to building management and security staff.

Emergency Planning

For a building owner or manager to effectively manage an incident that constitutes an emergency in a residential and apartment building, it is critical to plan ahead. Before proceeding, it is appropriate to review several key concepts.

Key Concepts

An *incident* is an “event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization's operations, services, or functions—which, if not managed, can escalate into an emergency, crisis, or disaster.”

A *disruption* is “an event that interrupts normal business, functions, operations, or processes whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a [power] blackout, terror attack, technology failure, or earthquake).”

An *emergency* is “an event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response.” During an emergency there may be chaotic conditions, particularly if there is a disruption in normal communications.

have a creepy feeling about a person, that’s because there’s usually a reason. Our bodies have ways of sensing danger. If you’ve ever been accosted or attacked, you will certainly understand the advantage of being proactive when it comes to elevator travel” (Fourchalk F. The ups and downs of elevator security. *Peace Arch News*. November 22, 2008. [www.bclocalnews.com/surrey_area/peacearchnews/lifestyles/34907009.html]; December 20, 2008). Standing close to the elevator control panel also affords an individual the opportunity to quickly access the emergency call button, phone, or intercom to summon help. “This way if someone begins to harass or threaten you, you can push all of the control buttons, which will cause the elevator to make several stops. This will now allow you many attempts to exit as the elevator stops at each floor” (Fourchalk F. The ups and downs of elevator security. *Peace Arch News*. November 22, 2008. [www.bclocalnews.com/surrey_area/peacearchnews/lifestyles/34907009.html]; December 20, 2008).


A crisis is “an unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.”

Emergency management (also sometimes known as crisis management) is defined as “the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness [and] response.”

A plan is defined as “a scheme or method of acting or proceeding developed in advance.”

Combining the terms emergency management and a plan can lead to a definition of an emergency management plan as “a scheme or method of acting or proceeding developed in advance for the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness and response.”

“The objective of an [emergency management plan] should be to allow those responsible for the [facility] during an emergency to focus on the solution of major problems, not to attempt immediately to bring order out of chaos. If all predictable and routine items are considered in the plan, those responsible for actions during an emergency will be able to deal with the unpredictable or unusual situations that will surely develop.”

According to Groner,

The chaotic and dynamic nature of building emergencies requires an exceedingly rapid assessment of the situation. The timeframe is measured in seconds and minutes, not hours and days. The rapid onset of many events means that

---


*United Nations International Strategy for Disaster Reduction. Terminology: Basic terms of disaster risk reduction. <www.unisdr.org/eng/library/lib-terminology-eng%20home.htm> 31 March 2004; July 8, 2008. The combined definition stated here uses a slightly modified version of the United Nations terminology. The UN definition states that emergency management is “the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness, response and rehabilitation.” The word rehabilitation has been removed. The reason for this is that for the purposes of this book, an emergency management plan addresses preparedness and response to an emergency and shortly thereafter. It does not deal with the rehabilitation process. Because, in the opinion of the author, that process is part of business continuity planning, which is “an interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption” (Business Continuity Planning. Wikipedia. <http://en.wikipedia.org/wiki/Business_continuity_planning>; July 9, 2008).


*Sometimes an emergency management plan is referred to as a prepare plan or emergency action plan. The latter is used by the NFPA and is defined as “Designated actions that employers, employees, and other building occupants should take to ensure they are safe from fire and other emergencies” (NFPA. Glossary of Terms, National Fire Code. Quincy, MA: National Fire Protection Association; 2005).


Chapter 11 • Residential and Apartment Buildings

The process should be well underway before emergency responders arrive at the building.

*Human factors professionals have been actively researching this problem under the generally accepted term of “situation awareness.”* Endsley (1988) has provided a well-accepted definition: “The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.”

As noted in the definition, it is insufficient to understand the momentary status of the situation; projecting its development is of great importance in choosing a strategy to safeguard building occupants.

The purpose of an emergency management plan is to help residential building emergency staff in their efforts to achieve situation awareness and make sound decisions to provide for the safety of occupants during building emergencies, such as fire.

The value of emergency planning is not only the emergency management plan itself but also in the development process leading to it and the education of residential building emergency staff that should occur in the process.

**How to Develop a Building Emergency Management Plan**

The building emergency management plan in Appendix 9–2 (which is on the CD-ROM provided with this book) is a suggested format for developing an emergency management plan for an office building. It includes actions intended to reduce the threat to the life safety of building occupants from emergencies, both fire and non-fire-related, that are likely to occur in a specific building, or in close proximity to it, until the arrival at the building of emergency responders. A residential and apartment building could adopt such an emergency plan as part of its effort to develop its own building emergency

---


**Achieving situation awareness is the primary challenge to optimizing building movement strategies** prepared for the NIST Workshop on Building Occupant Movement during Fire Emergencies June 9–10, 2004, by Norman E. Groner, John Jay College of Criminal Justice, City University of New York, Department of Public Management, 455 West 59th Street, New York, New York 10019, e-mail: ngroner@jjay.cuny.edu. Groner (p. 2) goes on to state in his paper that

*Progress in helping building management and emergency responders achieve situation awareness will require a fundamental change in how we approach the design of building protection systems. At present, our buildings are not well designed to achieve the needed level of situation awareness, despite the availability of many technological tools. Addressable detection devices can pinpoint the locations of detection of hazards, but the building interfaces used to display the information do not supply an immediately comprehensible understanding of the situation. Technological devices like CCTV cameras and smoke detectors are not deployed in ways that help building management and emergency responders understand the status of key egress systems like stairs and corridors. Research and development towards the support of situation awareness in buildings is a priority.*

**The emergency management plan presented here addresses preparedness and emergency response but does not address business continuity.**
management plan. However, several critical differences—building emergency staff organization and occupant documentation and training—need to be taken into account.

**Building Emergency Staff Organization**

The building emergency staff organization that will carry out emergency response procedures for a residential and apartment building differs from that of an office building. The most obvious difference is that residential buildings do not have floor response personnel (apart from possibly a warden on each floor). The responsibility for overseeing the safe and orderly evacuation of occupants from a residential floor resides with the floor warden (if available), building management, security, and engineering staff (the personnel involved will vary according to the size of the building, its staffing capabilities, and the time of day or night). Usually after normal business hours these facilities do not have many building emergency staff members present to help residents evacuate.

A typical staff organization for a high-rise residential and apartment building is outlined in Figure 11–1. This sample depicts the fire safety director as reporting to building management. However, it is noted that the authority that has jurisdiction in many cities empowers the fire safety director with full authority to evacuate a building without the need to obtain approval from building owners or managers.

Each unit of the building emergency staff organization has duties and responsibilities that have been developed and tailored to the specific needs of the building and to each type of emergency they may be required to handle. These duties and responsibilities should be defined clearly so that there will be a coordinated and effective response to each emergency situation. For example, the duties and responsibilities of building management, the building fire safety director, and the building engineering and security staff in handling a fire emergency will include ensuring that the fire department has been immediately notified, all occupants in the affected areas have been advised of the situation, any necessary evacuation of residents and visitors has begun, fire life safety systems are operating under emergency conditions, any investigation or initial suppression of the fire is carried out, and that the fire department and other responding personnel are met on arrival and briefed on the status of the situation. In contrast, during a bomb threat incident, these personnel may be involved in supervising the evacuation of residents and assisting in searching areas where an explosive device may have been placed. In a medical incident, security staff, depending on the building’s policy and the type of situation, may be required to administer CPR, an AED (automated external defibrillator), or basic first aid before the emergency medical responders arrive.

---

*Some apartment buildings, in an attempt to recruit floor wardens, will send regular communications to residents, including placing a letter under or a door hanger on the resident’s door every six months, to ask for volunteers to be the designated floor warden on their floor.*

**Terminology for the emergency staff organization units and members may vary, and some facilities may designate additional team members (such as a building evacuation supervisor, an emergency coordinator, emergency evacuation teams, a crowd manager, and first aid officers).**

***Some buildings might refer to the fire safety director as the building emergency controller.*

****In addition, building parking staff may be called on to assist in the evacuation of occupants from parking areas. Building janitorial staff may be required to clean up areas after the occurrence of water leaks, liquid spills, and water discharged from sprinklers; or, in the case of a bomb threat, they may be required to search areas with which they are familiar.*
Floor wardens, if present, will have specific duties and responsibilities that vary according to the type of emergency encountered. Primarily, these individuals oversee the safe and orderly evacuation of residents from a building floor.

**Occupant Documentation and Training**

“Occupants of each living unit must be given emergency instructions on a yearly basis, indicating the location of alarms, exiting paths, and actions to be taken in response to a fire in the living unit and in response to the sounding of an alarm.”

**Occupant Documentation**

Information provided as booklets, brochures, pamphlets, leaflets, flyers, wall posters, or items posted on a building's website can be used to train occupants. These materials should document procedures for emergencies considered likely to happen in a building. Some buildings limit the emergencies to fires, fire alarms, bomb threats, medical emergencies, and natural disasters relevant to a building's location. Figure A9–19 (which is contained in Appendix 9–2 on the CD-ROM provided with this book) is a sample occupant safety brochure for Pacific Tower Plaza, the hypothetical high-rise that is located in an area where earthquakes may occur.

---

Occupant documentation usually includes floor evacuation plans that show the building core, perimeter, stairwells, elevators, and every wall that faces every exit route; exit routes to the stairwells; symbols depicting the location of fire equipment and manual fire alarm devices; the floor number; fire department and building emergency telephone numbers; what stairwells have roof access; and what the fire alarm looks and sounds like. (See Figure 6–28 for a sample floor evacuation plan.) If a written brochure is used, it may also include a Certificate of Occupant Training (Figure A9–20 contained in Appendix 9–2 on the CD-ROM provided with this book) to be filled out by the occupant receiving the training and returned to the building fire safety director for record keeping.

Figure A9–21 in Appendix 9–2 on the CD-ROM provided with this book is a sample of a building’s website on which emergency phone numbers, an emergency procedures brochure, a site plan depicting outside safe refuge areas, building floor plans, a fire life safety video, and other emergency preparedness resources (such as links to public websites) are published. If such web-based fire life safety training is provided, some learning management systems record the actual training that each occupant has participated in. For example, after viewing a fire life safety training video, the occupant is asked to answer online questions to gauge his or her comprehension of the viewed material. The occupant’s answers are permanently recorded by the system. These records can be invaluable in determining occupant participation in fire life safety training. Also, they can be used as evidence to demonstrate a building’s efforts to prepare occupants for emergencies.

Some buildings post fire life safety information on the back of the main entrance door to the resident’s apartment. This could include a floor plan with the emergency telephone number, a description of what the building fire alarm sounds like (and looks like if strobe lights are available), the layout of the floor including room locations, corridors, elevators, and the nearest fire exits, a “YOU ARE HERE” indicator for the resident’s room location, a directional path depicting the direction of travel to each of the nearest fire exits, and the location of manual fire alarm stations and portable fire extinguishers on the floor—see a sample sign for a hotel in Figure 10–2. Information could also be portrayed in a program routinely broadcast to residents on in-room television channels. As a bare minimum, residents should be familiar with emergency exits on their floor, in particular noting the route leading to the nearest fire exit.

Occupant Training Class
A class that is taught by a qualified person (preferably the building fire safety director) is an invaluable way to inform building occupants of what to do in the event of a fire or other emergency.

In such a class, it is important to explain the building’s emergency systems, equipment, and relevant emergency procedures. The instructor must be thoroughly familiar with the building and its emergency management plan. Audiovisual aids and handout materials are extremely helpful. The use of videos, customized to a particular building (describing the emergency systems and equipment and the expected responses of occupants to building emergencies), are extremely useful tools.

Exit Signage
Exit signs (as described in Chapter 6) are also a critical part of the life safety program for residential and apartment building occupants. These include floor evacuation plans that show the building core, perimeter, stairwells, elevators, every wall that faces every exit route, exit routes to the appropriate stairwells, symbols depicting the location of fire equipment and manual fire alarm devices, the floor number, fire department and
emergency services telephone numbers, what stairwells have roof access, and what the fire alarm looks and sounds like.

Evacuation Drills
Residential and apartment buildings can utilize evacuation drills—commonly called fire drills—to train, instruct, reinforce, and test the preparedness of the building emergency staff and residents.

Residents can play an important part in any residential and apartment building fire life safety program by promptly reporting things such as suspicious persons or activities, safety hazards, or smell of smoke to building management and security staff.

Important Consideration
It is important that as many as possible of those who will be involved in the execution of the emergency management plan participate in the planning process. Those concerned should include the building emergency staff, and possibly public officials (such as those from the local fire and law enforcement agencies) and building management staff from neighboring buildings (with the view to developing mutual aid agreements). Public officials may require a particular format for the plan itself.

It cannot be stressed enough that the sample format for developing a residential and apartment’s Building Emergency Procedures Manual is provided as an example of how a building may prepare its plan. Every site and building is different, and emergency plans vary according to local laws and the requirements of the authority that has jurisdiction. It is up to each residential and apartment building to develop the emergency management plan most appropriate to its needs.

Summary

- From the time a vehicle enters the parking structure and residents proceed to the building, travel in the tower elevators, and enter an individual residence or apartment, there is a need for access control measures that sift out unwanted persons and intruders and yet constitute a minimum of inconvenience to legitimate building users.
- The purpose of establishing, implementing, and maintaining a building emergency management plan is to provide for the life safety of all building occupants.
- “Occupants of each living unit must be given emergency instructions on a yearly basis, indicating the location of alarms, exiting paths, and actions to be taken in response to a fire in the living unit and in response to the sounding of an alarm.”

---

*A drill is defined by the NFPA Glossary of Terms, National Fire Code, as “an exercise involving a credible simulated emergency that requires personnel to perform emergency response operations for the purpose of evaluating the effectiveness of the training and education programs and the competence of personnel in performing required response duties and functions” (Quincy, MA: National Fire Protection Association; 2005). A fire drill is such an exercise for a simulated fire emergency. The local authority that has jurisdiction will specify at what intervals the fire drills shall be conducted.

**A mutual aid agreement is ”a pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement” (ASIS Business Continuity Guideline. Alexandria, VA: ASIS International; January 2005:8).

Key Terms

**Apartment.** “An individual dwelling unit, usually on a single level and often contained in a multi-unit building or development.” See also **condominium** and **residential building**.

**Apartment building.** “A building containing more than one dwelling unit.” “Apartment buildings are those structures containing three or more living units with independent cooking and bathroom facilities, whether designated as apartment houses, condominiums, or garden apartments.” See also **condominium** and **residential building**.

**Bathroom.** A room that contains a bathtub and/or shower and usually a washbasin or a washbowl (i.e., a lavatory) and a toilet. Also called a **restroom**.

**Concierge.** Provides information and services to building tenants, residents, guests, and visitors, and performs other duties as specified by the facility.

**Condominium.** “A multiple-unit structure in which the units and pro rata shares of the common areas are owned individually; a unit in a condominium property. Also, the absolute ownership of an apartment or unit, generally in a multi-unit building, which is defined by a legal description of the air space the unit actually occupies plus an undivided interest in the common elements that are owned jointly with the other condominium unit owners.” Residential condominiums are commonplace in today’s society. See also **apartment building** and **residential building**.

**Doorman.** “An individual hired to provide courtesy and security services at a residential building or hotel. They are particularly common in urban luxury highrises [and major hotels]. At a residential building, a doorman is responsible for opening doors and screening visitors and deliveries. He [or she] will often provide other courtesy services such as signing for packages, carrying luggage between the elevator and the street, or hailing taxis for residents and guests.” At hotels they provide a wide variety of guest services. Although doorkeepers today tend to be men, sometimes women work in this capacity. The use of the term doorman in this book is not intended to exclude women.

**Dormitory.** A residence hall or a hall of residence with separate rooms or suites for sleep and study and that accommodate single or multiple students who share common bathing and toilet facilities.

**Guest.** In residential and apartment buildings, a guest is a “nonresident who stays in a resident’s private dwelling (with that resident’s consent) for one or more nights.”

**Landlord.** A person or an organization that owns a facility and leases or rents it, or a part of it, to a tenant(s). In the case of an apartment building, the leasing will be of apartments.

**Lessee.** “The tenant in a lease.” See also **tenant**.

---

46 *Glossary of Real Estate Management Terms.* Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:8.


49 *Glossary of Real Estate Management Terms.* Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:32.


52 *Glossary of Real Estate Management Terms.* Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:74.

53 Ibid., p. 94.
Rent. “Payment for the use of space or personal property owned by another. In real estate, a fixed periodic payment by a tenant to an owner for the exclusive possession and use of leased property.” 54

Residence. “A temporary or permanent dwelling place, abode, or habitation to which one intends to return as distinguished from a place of temporary sojourn or transient visit.” 55

Resident. “One who lives (or resides) in a place. Referring to residential tenants as ‘residents’ is preferred by many real estate professionals.” 56 See also tenant.

Residential building. A building containing separate residences where a person may live or regularly stay. Each residence contains independent cooking and bathroom facilities, and it may be known as an apartment, a residence, a tenement, or a condominium. See also apartment building and condominium.

Tenant. A person, a group of persons, or a company or firm that rents or owns and occupies space within a building. “A legal term for one who pays rent to occupy or gain possession of real estate; the lessee in a lease. Real estate managers often limit the use of the term tenant to commercial tenants and refer to residential tenants as residents.” 57 See also lessee and resident.

Visitor. In residential and apartment buildings it is a “nonresident who spends time at the home of a resident (with that resident’s consent) but does not stay overnight.” 58

Additional Reading


54 Ibid., p. 146.
56 Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:149.
57 Ibid., p. 171.
58 Ibid., p. 182.
This page intentionally left blank
Mixed-Use Buildings

For the purposes of this chapter, a mixed-use building is a building that houses commercial offices, apartments, residences, and hotel rooms in separate sections of the same high-rise structure (in contrast to low-to-mid-rise buildings located on a large campus-style site).

Hotel-residences are another type of mixed-use occupancy. “The hotel residences trend is notably different from its predecessors such as fractional/time share hotel units, which are not wholly owned, or condo hotels, which are wholly owned hotel rooms without, for example, kitchens. Not only do hotel residences have kitchens and everything else an owner would expect in a typical abode, they also include amenities such as maid and room service, plus restaurants, spas and gyms… Typically, [these] residences are on the top floors of hotels, reachable by controlled-access elevators, but only make up a fraction of the building.”

Mixed-use buildings usually “include parking facilities which may be open, enclosed, above- or below-ground, and often directly beneath or adjacent to the [office building] itself. These arrangements may require special types of fire protection, and the building codes may require fire separations.”

To systematically examine the security and fire life safety of mixed-use buildings, this chapter addresses the following areas: occupancy characteristics; assets, threats, vulnerabilities, and countermeasures; security programs; and emergency management.

Occupancy Characteristics

Because a mixed-use building can contain commercial offices, apartments, residences, and hotel rooms in sections of the same building, the mixed-use building itself displays the characteristics of each of these occupancies (as explained in Chapter 9 [“Office Buildings”], Chapter 10 [“Hotel Buildings”], and Chapter 11 [“Residential and Apartment Buildings”]).

Assets, Threats, Vulnerabilities, and Countermeasures

A risk assessment (as detailed in Chapter 4) is an important tool for developing an appropriate security and fire life safety program for a mixed-use building. A “risk assessment

*Technically, any high-rise building with more than one occupancy can be considered a mixed-use facility. For example, an office building that has a cafeteria and an observation deck; a hotel building that has a shopping arcade, restaurants, and a movie theater; and a residential and apartment building that has retail shops and a health club open to the public. Each occupancy within each respective facility manages its own operations and is managed overall by the building owner and manager. For the purposes of this chapter, each of the three major occupancies—office, hotel, and residential—are housed separately from each other. They operate autonomously, and yet overall are still managed by the same building owner and manager.

1Olmsted L. Hotel residences: all the perks, none of the work. USA Today. McLean, VA, 8D; September 19, 2008.

analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each
critical asset against each applicable threat. Inherent in this is the likelihood or prob-
ability of the threat occurring and the consequences of the occurrence. Thus, a very high
likelihood of occurrence with very small consequences may require simple[,] low cost
mitigation measures [countermeasures], but a very low likelihood of occurrence with
very grave consequences may require more costly and complex mitigation measures. The
risk assessment should provide a relative risk profile. High-risk combinations of assets
against associated threats, with identified vulnerability, allow prioritization of resources
to implement mitigation measures.”

Key steps in the process involve examining the assets, the threats against the assets,
the vulnerabilities of the assets, and the countermeasures or mitigation measures that
can be used to address identified vulnerabilities of the assets (within the confines of risk
management). These areas are now examined for mixed-use buildings.

Assets
Tangible assets include the people using the facility; • business and personal property
contained within the office, hotel, and apartment occupancies; and the building itself, its
fittings, and its equipment. Building equipment includes electrical, water, gas, mechani-
cal, heating, ventilating, air-conditioning, lighting, elevator, escalator, communication,
security, and fire life safety systems. In addition, there are other assets within each of the
occupancies:

- **Office buildings.** Telephones, computers, printers, typewriters, fax machines,
  photocopiers, audio-visual equipment, and general-use items (coffee machines,
  vending machines, refrigerators, microwaves, ovens, and furniture), and sometimes
  antiques and works of art, cash, and negotiable instruments. In addition, there
  may be assets in cafeterias, restaurants, retail shops, newsstands, copy/print
  services, and other common area facilities for office workers and the public.

- **Hotel buildings.** Telephones, computers, printers, fax machines, photocopiers,
  audio-visual equipment (including televisions in guest rooms, foyers, restaurants,
  and bars; and equipment for use in meeting rooms), general-use items (coffee
  machines, refrigerators, microwaves, furniture, and common area vending
  machines), and sometimes antiques and works of art, cash, and negotiable
  instruments (particularly in the reception, restaurant, and retail areas). In addition,
  there may be assets in kitchens, laundries and dry cleaning facilities, fitness
  centers, saunas, swimming pools, spas/hot tubs, tennis and racquetball courts,
  dining areas, restaurants, retail shops, newsstands, business centers, and other
  facilities for guest services.

- **Residential and apartment buildings.** Kitchen appliances, furniture and
  furnishings, entertainment equipment, antiques and works of art, cash and
  negotiable instruments, telephones, computers, printers, and general-use items
  for daily living—and assets in common area vending machines, laundry facilities,

---


*Depending on the nature of the mixed-use building, these users may include office tenants, office
building staff, hotel guests, hotel staff, apartment residents, residential and apartment building staff, visitors,
contractors, and vendors.
fitness centers, saunas, swimming pools, spas/hot tubs, dining areas, restaurants, retail shops, newsstands, and entertainment and business centers.

Also, vehicles parked in the building’s parking garage are tangible assets. Intangible assets include the livelihood of building users; intellectual property and information stored in paper files, reference books, microfilm, and within computer systems and peripherals; and the reputation and status of the mixed-use building and its tenants.

Threats

The types of security and fire life safety threats to mixed-use building assets are outlined in Chapter 3. Briefly they include the following:

- Security threats to people: assault, assault and battery, kidnapping, manslaughter, mayhem, murder, robbery, sex offenses (including rape, sexual harassment, and lewd behavior), and stalking.
- Security threats to property and information: aberrant behavior, arson, burglary, cyberattack, disorderly conduct, espionage, larceny, sabotage, theft, trespass, and vandalism. In addition, there may be the disruption of building utilities such as water; electrical power; natural gas; sewer; heating, ventilation, and air-conditioning (HVAC); telecommunications; security; and life safety systems. Some security threats may involve terrorism.
- Security threats to people and property: bombs, chemical and biological weapons, civil disturbance, fires, hazardous materials, natural disasters, and nuclear attack.
- Life safety threats: aircraft collisions; bombs and bomb threats; daredevils, protestors, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstrations, and civil disorder; medical emergencies; natural disasters (earthquakes, tsunamis, volcanoes, heat waves, storms, and floods and landslides); contractible diseases (pandemic influenza, severe acute respiratory syndrome, and tuberculosis); power failures; slip-and-falls; stalking and workplace violence; traffic accidents; and water leaks.

Fire Risk in Mixed-Use Buildings

Fire is an ever-present risk in high-rise mixed-use buildings. In discussing fire risk,* it is helpful to analyze fire incident data** for the four property classes—office buildings, hotels and motels,*** apartment buildings, and hospitals (and other facilities that

---


**“Tracking of the fire experience in [U.S.] high-rise buildings, however, has been less than systematic because the nationally representative fire incident data bases did not originally include reporting of height of structure. Reasonably good reporting began with 1985 fires…. NFPA and other analysts have long used lists of particularly memorable incidents to study the high-rise fire problem, but these and other available special data bases are heavily weighed towards larger and more severe incidents” (Hall Jr JR. High-Rise Building Fires. Quincy, MA: National Fire Protection Association; September 2001:1).

***“The term ‘motel’ is a general designation for lodging establishments that specialize in attracting the motoring public by offering parking accommodations. The distinctions between hotels and motels are gradually disappearing, however” (Beaudry MH. Contemporary Lodging Security. Newton, MA: Butterworth-Heinemann; 1996:ix).
care for the sick)—that account for the majority of high-rise building fires.\textsuperscript{4} Even though this data pertains only to the United States, it is worth considering because it includes the types of commercial buildings that are addressed in this book (namely, office, hotel, residential and apartment, and mixed-use buildings).

A study by Dr. John Hall, Jr., of the National Fire Protection Association’s (NFPA) Fire Analysis and Research Division, using statistics from the U.S. Fire Administration’s National Fire Incident Reporting System (NFIRS), stated that from 1987 to 1991, office buildings, hotels and motels, apartment buildings, and facilities that care for the sick averaged 13,800 high-rise building fires per year and associated annual losses of 74 civilian deaths, nearly 720 civilian injuries, and $79 million in direct property damage. However, “most high-rise building fires and associated losses occur in apartment buildings.”\textsuperscript{5} Hall added that for this period,

- Only a small share of high-rise building fires spread beyond the room of origin, let alone the floor of origin.
- In high-rise buildings [office buildings and hotels and motels], electrical distribution system fires rank first in causes of fire-related property damage.\textsuperscript{6}

The most recent published study by Hall shows that “in 2002, high-rise buildings in these four property classes combined had 7,300 reported structure fires and associated losses of 15 civilian deaths, 300 civilian injuries, and $26 million in direct property damage.”\textsuperscript{7} He concluded that “these statistics generally show a declining fire problem over the nearly two decades covered”\textsuperscript{8} and, similar to his previous findings, “most high-rise building fires and associated losses occur in apartment buildings.”\textsuperscript{9} He further commented pertaining to the latter, “this may seem surprising, but it shouldn’t. Homes dominate the U.S. fire problem so completely that it is always a good bet that any newly examined fire problem, unless it is one that cannot occur in homes, will have its largest share in homes.”\textsuperscript{10} However, Hall did caution that, due to a number of factors (one being lower participation in national fire incident reporting in recent years\textsuperscript{11}), “the patterns shown in data available so far should be given limited weight.”\textsuperscript{12}

### Vulnerabilities

Weaknesses that can make an asset (in this case, a mixed-use building and its operations) susceptible to loss or damage\textsuperscript{13} will largely depend on the building itself and the nature of its operations. A vulnerability assessment is required to “evaluate the potential vulnerability of the critical assets against a broad range of identified threats/hazards.”\textsuperscript{14}

\textsuperscript{5}ibid., p. 50.
\textsuperscript{6}ibid., p. 53.
\textsuperscript{7}Hall Jr JR. *High-Rise Building Fires*. Quincy, MA: National Fire Protection Association; August 2005:3.
\textsuperscript{8}ibid., p. 3.
\textsuperscript{9}ibid., p. 4.
\textsuperscript{10}ibid., p. 4.
\textsuperscript{11}ibid., p. 3.
\textsuperscript{12}ibid., p. 4.
\textsuperscript{14}ibid., p. iii.
Countermeasures

Mitigation measures to counteract identified vulnerabilities of an asset to a threat may consist of security systems and equipment (see Chapter 5), fire life safety systems and equipment (see Chapter 6), security personnel (see Chapter 7), security policies and procedures (see the next section, “Security Programs”), and emergency management (see the later section, “Emergency Planning”). These countermeasures need to be looked at in terms of security design. “Security design involves the systematic integration of design, technology, and operation.... The process of designing security into architecture is known as Crime Prevention Through Environmental Design (CPTED).”\(^{15}\) As mentioned previously, the key to selecting appropriate countermeasures for a particular facility is for a risk assessment to be conducted. (See Chapter 4.)

Because fire is a risk in high-rise buildings, the following is noted regarding their fire protection features: mixed-use buildings that have properly designed, installed, operated, tested, and maintained automatic fire detection and suppression systems, and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes, and automatic smoke control systems to restrict the spread of smoke—do have the necessary early warning systems to quickly detect fires and warn occupants of their presence, as well as the necessary automated sprinkler systems to quickly extinguish a fire in its early stages. One of the key issues here is the presence or absence of sprinklers.

In the study mentioned in the previous section, “Threats,” Hall commented on fire protection features in high-rise buildings by stating that,

\[
\text{In several instances, the value of these fire protection features [i.e., automatic extinguishing systems (primarily sprinklers), fire detection equipment, and fire-resistant construction] may be seen clearly in a statistical analysis of 1994-1998 loss per fire averages, with and without the protection. For high-rise buildings, automatic extinguishing systems are associated with a reduction of at least 88\% in the rate of deaths per 1,000 fires for each of the three property classes (excluding office buildings, which had no deaths recorded in NFIRS [National Fire Incident Reporting System] in high-rise buildings) and at least 44\% in the average dollar loss per fire for each of the four property classes. Fire detection equipment is associated with a reduction of 55\% in the rate of deaths per 1,000 fires in apartment buildings. Fire-resistant construction is associated with a reduction of 30\% in average dollar loss per fire in apartment buildings. This probably is produced not directly by the construction but indirectly by the compartmentation features that tend to be used with fire-resistant construction, features that keep more fires smaller and so keep property losses lower. (Note, though, that compartmentation practices probably vary more by type of occupancy than by type of construction.) Because high-rise buildings often use all three systems, it is very difficult to try to separate their effects on loss rates, and many rates are very sensitive to deaths or large dollar loss in individual incidents.}\]

Automatic extinguishing systems and fire detection equipment and the compartmentation features associated with fire-resistant construction all contribute to fire protection by helping to keep fires small, with extinguishing and construction doing so directly and detection doing so by providing early warning that can lead to earlier manual suppression....

Finally, the effectiveness of these fire protection systems and features and their widespread use in high-rise buildings mean that when people are killed in high-rise residential fires, they are much more likely to have been close to the fire, where it is more likely that fatal injury could occur before [the] fire could be stopped or blocked by these systems and features.¹⁶

These comments are not directly made about mixed-use buildings, but because such buildings may house offices, apartments, residences, and hotel rooms in separate sections of the same building, they are appropriate.

**Security Programs**

Security programs for mixed-use buildings and for individual tenants involve policies, rules and regulations, and procedures designed “to prevent unauthorized persons from entering, to prevent the unauthorized removal of property, and to prevent crime, violence, and other disruptive behavior.”¹⁷ Security’s overall purpose is to protect life and property.

Each occupancy—office, hotel, and residential—will have its own security program, as addressed in the respective chapters—Chapter 9, “Office Buildings,” Chapter 10, “Hotel Buildings,” and Chapter 11, “Residential and Apartment Buildings.” However, the building owner and management will develop a master security plan for the building itself.

Some of the factors that need to be considered include the following:

- How will access control of people be handled? What role will building security play in screening pedestrians before allowing them to enter the building? For example, will each of the three occupancies have a separate lobby and reception area, and will there be separate elevator banks dedicated to each occupancy?
- How will movement of people between the different occupancies be handled? Will there be a separate reception area for each occupancy?
- Will there be a building-wide access control system for the building? Who will maintain the system? Will each occupancy issue its own access cards?
- How will vehicle access to the parking garage be handled? For example, will each of the three occupancies have separate parking entrances and areas for parking vehicles?
- How will property moving in and out of the building be controlled? For example, will each of the three occupancies have separate loading docks and messenger


*Elliott R. Towering technology in Dubai. Security Management. Alexandria, VA; April 2007. This article about the world’s tallest mixed-use building, Burj Dubai, was consulted for ideas.
centers for the handling of property, or will there be a central loading dock and messenger center? How will couriers and messengers be processed for entry to perform deliveries and pickups from the individual occupancies in the building? How will lost and found property be handled? How will trash and rubbish removal from the individual occupancies in the building be handled?

- Will building security staff conduct mobile patrols in each of the occupancies? During these patrols, if issues are encountered, to whom does building security report these matters?
- Will each occupancy handle security incidents that occur within its own occupancy, or will building emergency staff be required to respond? If the former, what type of incidents must be reported to building security staff? How soon after the incident must it be reported? What type of incidents will require an additional response by building security?
- Will escorts of occupants be handled by the individual occupancy’s security personnel or by building security staff?
- Will each occupancy have its own separate security and fire command centers? Will the building’s main command center be fully integrated with these centers and able to always monitor their security and fire life safety systems? If so, during an emergency, can the building’s main command center override these systems and operate them?

These and many other issues will need to be addressed for the specific building in question. In a mixed-use facility, it is critical that the security master plan includes a clear delineation of security and fire life safety responsibilities for each of the individual occupancies and is developed in cooperation with the management of each of them.

Emergency Planning

For a building owner or manager to effectively manage an incident that constitutes an emergency in such a mixed-use building, it is critical to plan ahead. Each occupancy—office, hotel, and residential—will have its own building emergency management plan, as addressed in the respective chapters—Chapter 9, “Office Buildings,” Chapter 10, “Hotel Buildings,” and Chapter 11, “Residential and Apartment Buildings.” However, the building owner and management will develop a master building emergency management plan for the building itself.

The building emergency staff organization that will carry out emergency response procedures for the building will need to be clearly defined. A typical staff organization for a mixed-use building is outlined in Figure 12.1. This sample depicts the mixed-use building fire safety director as reporting to mixed-use building management. However, it is noted that the authority that has jurisdiction in many cities will empower the overall building fire safety director with full authority to evacuate a building, without the need to obtain approval from building owners or managers.

Each unit of the building emergency staff organization will have duties and responsibilities that have been developed and tailored to the specific needs of the building and to each type of emergency it may be required to handle. These duties and responsibilities must be defined, including the responsibilities of each occupancy’s emergency team and how it will coordinate emergency actions with the building’s emergency team. Only then can there be a coordinated and effective response to each emergency situation.
FIGURE 12–1  Sample mixed-use building emergency staff organization.
One crucial issue to be addressed is how the evacuation of occupants will be handled, including whether occupants will be permitted to evacuate from one occupancy to the adjacent one below (a possible solution is to have a designated refuge floor between each occupancy where evacuating occupants can go). Also, who will have the authority to initiate such an evacuation? Other important items will include the handling of disabled/physically impaired occupants, and the training, instructing, and testing of the preparedness of emergency personnel.

It is important that as many as possible of those who will be involved in the execution of the emergency management plan participate in the planning process. Those concerned should include the emergency staff for each occupancy and possibly public officials (such as those from the local fire and law enforcement agencies) and building management staff from neighboring buildings. Public officials may require a particular format for the plan itself.

It cannot be stressed enough that every site and building is different, and emergency plans vary according to local laws and the requirements of the authority that has jurisdiction. It is up to the management of each mixed-use building to develop the emergency management plan most appropriate to its needs.

Summary

- In a mixed-use facility, it is critical for the security master and building emergency management plan to include a clear delineation of security and fire life safety responsibilities for each of the individual occupancies and for the plan to be developed in cooperation with the management of the individual occupancies.
- The purpose of establishing, implementing, and maintaining a building emergency management plan is to provide for the safety of all building occupants.

Key Terms

Apartment. “An individual dwelling unit, usually on a single level and often contained in a multi-unit building or development.”

Apartment building. “A building containing more than one dwelling unit.” “Apartment buildings are those structures containing three or more living units with independent cooking and bathroom facilities, whether designated as apartment houses, ... condominiums, or garden apartments.” See also condominium and residential building.

Bathroom. A room that contains a bathtub and/or shower and usually a washbasin or washbowl (i.e., a lavatory) and a toilet.

Campus. “A site on which the buildings of an organization or institution are located.”

---

19Ibid., p. 8.
Condominium. “A multiple - unit structure in which the units and pro rata shares of the common areas are owned individually; a unit in a condominium property. Also, the absolute ownership of an apartment or unit, generally in a multi-unit building, which is defined by a legal description of the air space the unit actually occupies plus an undivided interest in the common elements that are owned jointly with other condominium unit owners.” Residential condominiums are commonplace in today’s society.

Guest. In hotel buildings it is a person who “lodges, boards, or receives refreshment for pay (as at a hotel ... or restaurant) whether permanently or transiently.” In residential and apartment buildings, a guest is a “nonresident who stays in a resident’s private dwelling (with that resident’s consent) for one or more nights.” A guest is sometimes known as a patron.

Hotel. “The term ‘hotel’ is an all - inclusive designation for facilities that provide comfortable lodging and generally, but not always food, beverage, entertainment, a business environment, and other ‘away from home’ services.”

Hotel-residences. “Hotel residences have kitchens and everything else an owner would expect in a typical abode, they also include amenities such as maid and room service, plus restaurants, spas and gyms.... Typically, [these] residences are on the top floors of hotels.”

Mixed-use building. A building that may contain commercial offices, apartments, residences, and hotel rooms in separate sections of the same building. Hotel-residences are another type of mixed-use occupancy.

Office building. A “structure designed for the conduct of business, generally divided into individual offices and offering space for rent or lease.”

Patron. See guest.

Residence. “A temporary or permanent dwelling place, abode, or habitation to which one intends to return as distinguished from a place of temporary sojourn or transient visit.”

Residential building. A building containing separate residences where a person may live or regularly stay. Each residence contains independent cooking and bathroom facilities and may be known as an apartment, a residence, a tenement, or a condominium. See also apartment building.

Security master plan. The strategic plan for the protection of a facility’s assets (people, property, and information). “The ultimate goal of good strategic planning is to lay out specific long-range plan objectives and then devise short-term action plans to meet each major objective (or goal).” This plan may or may not be formally documented. Sometimes it is called the security plan or the security operations plan.

22Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:32.
26Olmsted L. Hotel residences: all the perks, none of the work. USA Today. McLean, VA, 8D; September 19, 2008.
27Glossary of Real Estate Management Terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003:120.
**Visitor.** In office buildings it is a nonoccupant who spends time at the building. In hotel buildings, it is a nonguest who visits a hotel guest or uses the hotel's facilities (such as meeting rooms, conference facilities, recreational facilities, restaurants, bars, a casino, or a discotheque). In residential and apartment buildings, it is a “nonresident who spends time at the home of a resident (with that resident’s consent) but does not stay overnight.” In a mixed-use building, it could be all the preceding depending on the nature of its occupancies. See also *guest*.

**Additional Reading**


---

This page intentionally left blank
Liaison with Law Enforcement and Fire Authorities

For a high-rise building to have a successful security and fire safety program, it is important for the building owner or manager, the director of security, or the fire safety director to establish a liaison with various agencies in the public sector, including law enforcement and fire authorities. Developing and maintaining strong lines of communication and cooperation with these authorities will lead to a successful working relationship.

Liaison with Law Enforcement

Law enforcement authorities are concerned primarily with crime prevention and control. This involves the protection of the lives, property, and general welfare of the public community. Police departments, funded by public monies, achieve this protection largely through the enforcement of laws.

Building management interacts with public law authorities such as police and sheriff's departments and state or federal agencies. The police department is the primary law enforcement agency in most cities. Although other agencies may have final jurisdiction over many classes of crime, initial authority almost always rests with the local police department.

Police and sheriff’s departments handle tasks such as taking reports and investigating crimes; maintaining arrest, missing persons, and identification records; keeping records of lost and stolen property; taking reports of vehicle accidents; issuing gun permits; and transporting and maintaining custody of prisoners. Local police may also provide traffic control support for special events. A local marshal or constable may serve criminal and bench warrants and service of process.

State law enforcement agencies have authority that varies but may include enforcing traffic laws, conducting investigations, gathering intelligence, and protecting of public figures.

Federal agencies have jurisdiction over areas as defined by their charters.

---

In addition, buildings should maintain good networking relationships with the property management and security staff of similar-occupancy neighboring buildings. Sharing of information, particularly as it relates to crimes that may have occurred, can be extremely useful in operating successful security programs.

In some countries, the sheriff’s department serves a similar function outside city limits or if no municipal police department exists. An international association of law enforcement executives is the International Association of Chiefs of Police (IACP). IACP is the “world’s oldest and largest nonprofit membership organization of police executives, with more than 20,000 members in more than 89 different countries. IACP’s leadership consists of the operating chief executives of international, federal, state, and local agencies of all sizes,” IACP website, <www.theiacp.org>, (November 9, 2008).
Liaison with Fire Authorities

Fire authorities are primarily concerned with the preservation of people’s lives and properties, including the enforcement of local and state fire codes. Municipal, county, and state fire personnel who enforce fire codes and conduct arson investigations may have police officer status to assist them in carrying out their duties.

Building fire life safety systems and fire prevention inspections, as well as fire investigations, commonly are conducted in conjunction with the local fire department inspector or the fire marshal that has jurisdiction over the building. Frequently, state or federal agencies conduct inspections and investigations related to occupant safety.

Fostering Relationships with Law Enforcement and Fire Authorities

The building security representative can foster relationships with law enforcement by formal and informal communication. There is a strong underlying reason for such a relationship that is of mutual benefit to both law enforcement and the private security representative: the common objective of crime prevention. During criminal investigations conducted within a building, for example, a successful working relationship with law enforcement can greatly improve the outcome. Such investigations commonly are conducted in conjunction with the local police or sheriff’s department or federal agency, and their support and assistance must be obtained to bring the effort to a satisfactory conclusion. It is important to remember that the authority of a private investigator is comparable only to that of a private citizen in areas such as detaining suspects and obtaining access to information. (See the “Private Sector and Public Law Enforcement Investigations” section in Chapter 8 for information on this subject.)

The building safety representative can also foster relationships with fire authorities. They are only too anxious to assist building management in establishing and maintaining sound fire life safety programs for building users. Fire departments in some large cities have even established specialized high-rise divisions and units to help in this endeavor.

The following sections describe ways to initiate positive interaction with local law enforcement and the fire authority that has jurisdiction; these mostly have to do with mutual respect and planned coordination of efforts.

Communication

It is important to establish a clear line of communication with law enforcement and the fire department and, wherever possible, involve them in implementing the building’s security and fire life safety program.

Many law enforcement agencies have a community liaison officer. It is important for the building representative to become familiar with that individual and learn of offered services and ways to support the agency in question. Regularly scheduled group meetings with police department and building security representatives can be excellent vehicles for exchanging information and networking. Similarly, with the fire department, establishing contact and learning ways for mutual cooperation is beneficial.

Building management should support any public service education programs appropriate to the building and offered by law enforcement and fire department agencies.
Reporting Crimes

Whenever possible, provide law enforcement with statistics of criminal acts, particularly crimes of larceny, that have occurred at the building. Encourage tenants, residents, and guests to report crimes to law enforcement. Public reports are based on data generated at the local level. When these crimes are reported to law enforcement, such data will more accurately indicate what types of crimes are being committed in the community. This will provide a clearer picture of crime and may assist law enforcement in justifying requests for additional law enforcement personnel and equipment.

Complying with Laws

Always willingly comply with the law, particularly as it pertains to maintaining a safe workplace for building occupants. Maintain up-to-date self-inspections and maintenance of building fire life safety systems and equipment. Keep fire protection test records and log sheets current (including generator tests, sprinkler system water and air pressure gauge readings, tests of fire detection and suppression systems, portable fire extinguisher checks, and equipment service invoices). Maintain documentation according to the guidelines of the authority that has jurisdiction.

When state or local fire officials conduct inspections, escort the inspector on the tour of the building. The inspector may offer acceptable ways to correct deficiencies and may give advice that will be invaluable in preparing for the next inspection. Prompt correction of violations within established time frames and to the satisfaction of the inspector will assist in developing a good relationship.

Enlisting Public Agency Support

Consult the appropriate authority when problems exist that the building cannot satisfactorily handle. For example, if a tenant or resident fails to respond to the building fire safety director’s repeated requests to correct improper storage of material that constitutes a fire hazard, solicit the support of the local fire authority. The local fire inspector may decide to carry out an “unannounced” fire prevention inspection with particular emphasis on that tenant or resident. The inspector thus takes building management out of what can be a sensitive and potentially confrontational situation.

Also, consult with law enforcement regarding any serious theft problem within a building. When appropriate, involve law enforcement in security investigations.

Hospitality

Invite law enforcement agencies for a tour of the building to view the security program and acquaint them with the security operation. This will give them a better understanding of the building and its security objectives.

Offer law enforcement the use of the building for periodic training operations, such as hostage simulations.

Invite members of the fire department to tour the building and view its fire life safety program. Also, encourage them to conduct familiarization drills of the building.

If fire and law enforcement officials invite building representatives to tour their operations, graciously accept such offers.

Taking local law enforcement and fire representatives to lunch, at least annually, is strongly encouraged.
Disaster Exercises

Conduct a full-scale building disaster exercise in conjunction with local emergency response groups: the local fire department’s fire suppression crews and emergency medical responders, local hospitals and health services, local law enforcement, and other emergency organizations within the community. If thoroughly prepared and properly executed, these exercises can be of great educational value to building staff, tenants, residents, and all outside agencies and groups who participate, and they can greatly assist in developing working relationships with local fire and law enforcement agencies.

Public Agency Presentations

Invite law enforcement and fire department representatives to give presentations to building occupants. For example, representatives of police bomb squads can often provide interesting and helpful information regarding bombs and bomb threats. Fire departments, particularly in larger cities where generally more staff are available, may do special presentations on fire life safety. Some will even provide live demonstrations and hands-on portable fire extinguisher training for building occupants. Always invite fire department representatives to attend building fire drills and evacuation exercises.

Presentations by law enforcement and fire departments not only can benefit the building concerned but can also assist these public agencies in their efforts to control crime and promote public safety.

Professional Security and Fire Life Safety Organizations

Support private organizations, both local and national, that serve security and fire life safety interests.

Community Service

It is a good practice to sponsor community service programs that are offered through local law enforcement or fire department agencies. Sponsoring youth sports teams and assisting in volunteer fund-raisers can help considerably in the building management’s efforts to work effectively with local law enforcement and fire authorities.

Summary

- In addressing security, the managers of high-rise buildings focus on loss prevention, while public law enforcement agencies are primarily concerned with crime control and public safety. Building management is also concerned with the life safety of all its building users.

---

*For example, organizations such as ASIS International and the National Fire Protection Association (NFPA). ASIS International has local chapters, and some law enforcement representatives attend monthly meetings. Also, its Law Enforcement Liaison Council provides guidelines and recommendations as to how private security can interact with law enforcement agencies. Annual events like Law Enforcement Appreciation Day, when local members of law enforcement are invited by members of ASIS to a special luncheon, is an opportunity to express gratitude to members of law enforcement. NFPA, among its myriad activities, sponsors public fire safety education and awareness events such as the annual National Fire Prevention Week, which highlights important fire life safety issues.
• Fire authorities are concerned with the preservation of people’s lives and properties and with the enforcement of local and state fire codes.
• Representatives of a high-rise building can find many opportunities to cooperate with public agencies. These efforts can enhance the building security and fire life safety program and contribute to a safer community at large.

References


Laws, Codes, Standards, and Guidelines

Various laws, codes, standards, and guidelines affect the security and fire life safety of high-rise buildings.

The law, “in its generic sense, is a body of rules or action or conduct prescribed by the controlling authority, and having binding legal force.”

A code is “a systematic collection; a private or official compilation of all permanent laws in force consolidated and classified according to subject matter.”

A standard is “a model, type, or gauge used to establish or verify what is commonly regarded as acceptable or correct.”

A guideline is a document that steers our understanding of a particular subject. It provides direction but does not require adherence to the course of action or the advice provided.

Laws, codes, standards, and guidelines applicable to high-rise buildings aim to enhance public safety for the facility users through strategies established for the manufacture and use of various materials and equipment, the methods of construction, and the provision of various services for building operation.

Developers, building inspectors, fire marshals and fire department personnel, testing laboratories, manufacturers, architects, engineers, builders, installers, software developers, consultants, owners, managers, risk managers, insurance agents, security directors, fire safety directors, maintenance departments, law enforcement personnel, contract security firms, investigators, legal counsel, professional societies, and trade associations all have codes and standards to follow in their areas of expertise or responsibility. These codes and standards provide a format for quality and standardization throughout the industry.

Types of Standards

Two main types of standards are relevant to the security and fire life safety operations of high-rise buildings.

1. Statutory or regulatory standards are enacted under the law. Some come from federal government sources, whereas others, such as the licenses and regulations
governing private security firms and certain building and fire codes, are adopted by state, county, city, and local authorities.

2. Consensus or private standards are advisory recommendations applied by consent or agreement rather than required by law. Some of these standards have been developed or sponsored by federal governments, whereas others were developed by private sources such as professional societies (for example, fire, security, and building associations), trade associations (for example, fire alarm and burglar alarm associations), insurance companies, and systems and equipment manufacturers.

It is not within the scope of this book to comprehensively list all laws, codes, standards, and guidelines applicable to high-rise buildings. Even if such a record were provided, it would need to be customized for each facility, as Schum pointed out:

_In your personal experience, you will be faced with codes and standards not listed therein, and you may never have to deal with many of those listed. Code use tends to be [country specific or] regional, and every state, county, and city must be dealt with individually for local approvals and restrictions. However, most codes are based on national code publications._

Due to the utmost importance of building and fire prevention codes to the security and fire life safety of high-rise buildings, some mention is made of them and their enforcement.

**Building Codes**

According to Cote and Grant,

_A code is a law or regulation that sets forth minimum requirements and, in particular, a building code is a law or regulation that sets forth minimum requirements for the design and construction of buildings and structures. These minimum requirements, established to protect the health, well-being, and safety of society, attempt to represent society's compromise between optimum safety and economic feasibility._

---

*For example, in the United States, an important private organization is the American National Standards Institute (ANSI). It does not develop or enforce standards, but it reviews and validates the voluntary standards already prepared by private groups, designating the best of them as American National Standards. These standards represent a general agreement among manufacturers, distributors, and consumers on the best practices over a wide area of the building industry. ANSI reviews standards every five years to ensure they are up to date with current technology and practice.*


Although builders and building owners often establish their own requirements, the minimum code requirements of a jurisdiction must be met. Features covered include, for example, structural design, fire protection, means of egress, light, sanitation, and interior finish.

In a stylistic sense, there are two broad, general approaches used to write codes for the built environment: specification or prescriptive codes and performance-based codes. Prescriptive or specification-based codes spell out in detail what materials can be used, the building geometry (heights and areas), and how the various building components should be assembled. The traditional codes that have evolved through history tend to be prescriptive or specification oriented.

Performance-oriented building and fire codes [i.e. performance-based] detail the goals and objectives to be met and establish criteria for determining if the objective has been reached. Performance-oriented building and fire codes are a relatively new and evolving concept, which is only in recent years enjoying widespread acceptance.

Model building codes are not laws in themselves. They must be adopted into law by the appropriate local authorities before they can be enforced. “Building code requirements usually apply to new construction or to major alterations to existing buildings. Retroactive application of code requirements is very rare. Building code applicability usually ends with the issuance of an occupancy permit or certificate of occupancy.”

Fire Prevention Codes

In addition to building codes there are fire prevention codes. A fire code or fire prevention code usually deals with fire hazards that exist in a building after occupancy has been granted.
Who Enforces Building and Fire Prevention Codes?

The building department having jurisdiction usually enforces building codes; a fire official such as the fire marshal usually enforces fire prevention codes. To determine the laws and codes that apply to a particular facility, one must determine exactly which ones the authority having jurisdiction (AHJ)* has adopted.

Laws, codes, and standards are interpreted and enforced by human beings and therefore one should keep in mind that,

If you feel that an error has been made, contact the agency in writing and seek a clarification of that interpretation. Never assume that an agency official is correct. If a summons or a violation is issued to you, accept it, but advise the official that you are accepting it under protest. If the summons requires your signature, sign it, but also note that you are signing it under protest.9

Applicability of Laws, Codes, and Standards

Laws, codes, and standards can apply to both security and fire life safety in high-rise buildings; however, fire life safety operations are more strictly regulated than security operations.**

Fire Life Safety Measures

For fire life safety, the application of safety provisions is somewhat clearer. Many of the requirements for high-rise buildings are governed by codes adopted by the authority having jurisdiction and the requirements (particularly by building insurers) to use equipment listed, recognized, or certified by recognized testing groups. For example, modern high-rise buildings are required to install and maintain adequate fire protection systems and to establish and maintain a prefire plan that includes training occupants as to what they should do in case of a fire or other emergency. Any building owner or manager who does not comply is at considerable risk of sanctions and fines and to significant liability*** exposure if injuries, deaths, or property loss result from inadequate safety measures. Also, other public laws hold building owners and managers responsible to ensure that adequate life safety precautions are taken to provide a safe and healthful working environment and to keep premises reasonably safe for business visitors.

---


**For example, building codes address security as well as fire life safety issues, but in the United States, “more than half of a modern building code usually refers in some way or another to fire protection” (Cote AE, Grant CC. Building and fire codes and standards. In: Fire Protection Handbook. 20th ed. Quincy, MA: National Fire Protection Association; 2008:1–57).

Security Measures

Security and the Law

Whereas public police and protection services derive their authority to act from a variety of statutes, ordinances, and orders enacted at various levels of government, private police function essentially as private citizens. Their authority to so function is no more than the exercise of the right of all citizens to protect their own property. Every citizen has common law and statutory powers that include arrest, search, and seizure. The security officer has these same rights, both as a citizen and as an extension of an employee’s right to protect their employer’s property. Similarly, this common-law recognition of the right of defense of self and property is the legal underpinning for the right of every citizen to employ the services of others to protect property against any kind of incursion by others.

The broad statement of such rights, however, in no way suggests the full legal complexities that surround the question....

It is of enormous value, therefore, for everyone engaged in security to pursue the study of both criminal and civil law. Such a study is aimed neither at acquiring a law degree nor certainly at developing the skills to practice law. It is directed toward developing a background in those principles and rules of law that will be useful in the performance of the complex job of security.

Without some knowledge of the law, security officers frequently cannot serve their clients’ interests. They may subject themselves or their employers to ruinous lawsuits through well-meaning but misguided conduct.

Security and Liability

In the past few years, the number of suits filed against security officers and companies has increased dramatically. Predictions for the next ten years indicate no further increase. One possible reason for the leveling off of suits is that security management has a better understanding of the problems associated with liability situations today. The earlier increase may be partly attributed to the growth of the security industry and to the public’s demand for accountability and professionalism in the security area. Most of the cases filed against private security officers and operations belong in the tort category.

---

*This section is extracted, with modifications and additions, from Chapter 6 in Introduction to Security by Fischer RJ, Green G, 6th ed. (used with permission of Butterworth-Heinemann, Woburn, MA, 1998: 117, 118). Wherever a high-rise building is located, the criminal and civil law of that specific country should be consulted.

**In the high-rise setting, such citizens may include building owners, managers, security directors, fire safety directors, building maintenance departments, security officers, and the individual building occupants themselves. A security officer is a person who has been commissioned or authorized to perform duties primarily concerned with protection of the lives and property of people working within the private sector.

***This section is extracted, with modifications and additions, from Chapter 6 in Introduction to Security by Fischer RJ, Green G, 6th ed. (used with permission of Butterworth-Heinemann, Woburn, MA, 1998: 134–138).

****A tort is a civil action based on the principle that one individual can expect certain behavior from another individual. When the actions of one of the parties do not meet reasonable expectations, a tort action may result. [For example,] in security applications, a guard [security officer] may take some action to interfere with the free movement of some person. There is a basis for a suit no matter whether the [security officer] knows the actions are wrong, or is unaware that the actions are wrong but acts in a negligent manner” (Fischer RJ, Halibozek E, Green G. Introduction to Security. 8th ed. Burlington, MA: Elsevier Butterworth-Heinemann; 2008:129).
In most cases of negligence, the jury considers awarding damages to compensate the plaintiff. The awards generally take into account the physical, mental, and emotional suffering of the plaintiff, and future medical payments may be allowed for.

Punitive damages are also possible but are more likely to be awarded in cases of intentional liability. Punitive damages are designed to punish the tortfeasor [the individual who commits a tort] and to deter future inappropriate behavior. Punitive damages are also possible in negligence cases where the actions of the tortfeasor were in total disregard for the safety of others.

Duty to Protect from Third-Party Crime

The area of civil liability is of great importance to the security industry because the courts have been more willing to hold the industry legally responsible for protection in this area than in others. This trend is particularly noticeable in the hotel and motel industry where owners are liable for failure to adequately protect guests from foreseeable criminal activity. In some circumstances, a landlord or hotel or motel owner might be held accountable for failure to provide adequate protection from criminal actions. In Klein v. 1500 Massachusetts Avenue Apartment Corporation, a tenant who was criminally assaulted sued the corporation. The decision centered on the issue that the landlord had prior notice of criminal activity (including burglary and assault) against his tenants and property. In addition, the landlord was aware of conditions that made it likely that criminal activities would continue. The court ruled that the landlord had failed in an obligation to provide adequate security and was thus liable. A similar case was made against Howard Johnson's by the actress Connie Frances. Frances alleged that the hotel had failed to provide adequate locks on the doors. The jury awarded Frances over $1 million.

[Other] decisions (Philip Aaron Banks, et al. v. Hyatt Corporation and Refco Poydras Hotel Joint Venture and Allen B. Morrison, et al. v. MGM Grand Hotel, et al.) have followed earlier landmark cases. In the Banks case, the court held the hotel liable for foreseeable events that led to the murder of Banks by a third party. Banks was shot only four feet from the hotel door.

---


**“A pecuniary compensation of indemnity, which may be recovered in the courts by any person who has suffered loss, detriment, or injury, whether to his person, property, or rights, through the unlawful act or omission or negligence of another…. Damages may be compensatory or punitive according to whether they are awarded as the measure of actual loss suffered or as punishment for outrageous conduct and to deter future transgressions” (Publisher’s Editorial Staff. *Black’s Law Dictionary*. 6th ed. [Nolan JR, Nolan-Haley JM, co-authors] St. Paul, MN: West Publishing; 1990:389, 390).

***“A person who brings an action; the party who complains or sues in a civil action and is so named on the record” (Publisher’s Editorial Staff. *Black’s Law Dictionary*. 6th ed. [Nolan JR, Nolan-Haley JM, co-authors] St. Paul, MN: West Publishing; 1990:1150).

10Klein v. 1500 Massachusetts Avenue Apartment Corporation, 439 F. 2d 477 DC Cir (1970).


The suit alleged that the hotel failed to provide adequate security and to warn Banks of the danger of criminal activity near the hotel entrance. The jury awarded the plaintiffs $975,000, even though evidence was introduced that showed that the hotel had made reasonable efforts to provide additional protection in the area. The court stated that “the owner or operator of a business owes a duty to invitees to exercise reasonable care to protect them from injury,” noting that “the duty of a business to protect invitees can extend to adjacent property, particularly entrances to the business premises, if the business is aware of a dangerous condition on the adjacent property and fails to warn its invitees or to take some other reasonable preventive action.”

In the Morrison case, a robber followed Morrison from the hotel desk into the elevator after Morrison had cashed in his chips and withdrew his jewelry and cash from the hotel’s safe. The robber took Morrison’s property at gun point and then knocked him unconscious. Morrison brought suit against the hotel for failing to provide adequate security, noting that a similar robbery had recently occurred. The appellate court supported Morrison’s contention saying, “a landowner must exercise ordinary care and prudence to render the premises reasonably safe for the visit of a person invited on his premises for business purposes.” In McCarty v. Pheasant Run, Inc., however, the court recognized that invitees who fail to take basic security precautions may not have cause for action against the hotel.

In determining foreseeability, another factor to take into account is the nature and condition of the premises at the time the incident occurred. The following case was reported in Premises Liability: Legal Considerations for the Industrial and Retail Manager.

In a case, Gomez v. Ticor, involving a murder in a parking garage of a commercial office building[,] the court commented that the very nature of a parking structure to be such that criminal activity was something that could be anticipated:

[W]e note the unique nature of a parking complex, which invites acts of theft and vandalism. In such structures, numerous tempting targets (car stereos, car contents, the cars themselves) are displayed for the thief; high walls, low ceilings and the absence of cars’ owners allow the thief or vandal to work in privacy and give him time to complete his task. Such circumstances increase the likelihood of criminal misconduct. In addition, the deserted, labyrinthine nature of these structures, especially at night, makes them likely places for robbers and rapists to lie in wait. Robbery, rape, and

---


** “The ability to know in advance; [for example] the reasonable anticipation that harm or injury is a likely result from certain acts or omissions” (Publisher’s Editorial Staff. Black’s Law Dictionary. 6th ed. [Nolan JR, Nolan-Haley JM, co-authors] St. Paul, MN: West Publishing; 1990:649).


14 Gomez v. Ticor, 145 Cal. App. 3d 622, 193 Cal. Rptr. 600, 1983 (as reported in “Premises Liability: Legal Considerations for the Industrial and Retail Manager,” p. 6, Mary Ann Alsnauer, Laura D. Wolpow, Howarth and Smith, Los Angeles, CA).
violent consequences to anyone who interrupts these crimes, may thus also be foreseeable.

In fact, the concept of foreseeability has been expanded beyond the narrow opinion that foreseeability is implied in failure to provide security for specific criminal behavior. This concept implies that, since certain attacks have occurred in or near the company, the company should reasonably be expected to foresee potential security problems and provide adequate security. In a recent Iowa Supreme Court decision, the court abolished the need for prior violent acts to establish foreseeability. In Galloway v. Bankers Trust Company and Trustee Midlands Mall, the court ruled foreseeability could be established by “all facts and circumstances,” not just prior violent acts. Therefore prior thefts may be sufficient to establish foreseeability since these offenses could lead to violence. In another case, Polly Suzanne Paterson v. Kent C. Deeb, Transamerica Insurance Co., W. Fenton Langston, and Hartford Accident & Indemnity Co., a Florida court held that the plaintiff may recover for a sexual assault without proof of prior similar incidents of the premises.

According to Thomas, Property and business owners should always remember that courts will review their duty of care in a given situation on a case-by-case basis. “If the place or character of the landowner’s business, or his past experience, is such that he should reasonably anticipate careless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it and to use such means of protection as are available to afford reasonable protection” Nola M. v. U.S.C., 16 Cal.App.4th 421 (1993).

Nondelegable Duty

Another legal trend is to prevent corporations from divesting themselves of liability by assigning protection services to an independent contractor. Under the principle of agency law, such an assignment transferred the liability for the service from the corporation to the independent contractor. The courts, however, have held that some obligations cannot be entirely transferred. This principle is called nondelegable duty. Based on this principle, contractual provisions that shift liability to the subcontractors have not been recognized by the courts. These contractual provisions are commonly called hold harmless clauses.

Imputed Negligence

Imputed negligence simply means that, “by reason of some relation existing between A and B, the negligence of A is to be charged against B, although B has played no part in it, has done nothing to aid or encourage it,

---

15 Galloway v. Bankers Trust Company and Trustee Midlands Mall, No. 63/86-1879 Iowa Supreme Court.  
or indeed has done all that he possibly can to prevent it. This is commonly called ‘imputed contributory negligence.’”

Vicarious Liability

One form of imputed negligence is vicarious liability. The concept of vicarious liability arises from agency law in which one party has the power to control the actions of another party involved in the contract or relationship. The principal is thus responsible for the actions of a servant or agent. In legal terms, this responsibility is called respondeat superior. In short, employers are liable for the actions of their employees while they are employed on the firms’ business. Employers are liable for the actions of their agents even if the employers do nothing to cause the actions directly. The master is held liable for any intentional tort committed by the servant where the servant’s purpose, however misguided, is wholly or partially to further the master’s business.

If security officers are acting within the scope of their employment and commit a wrongful act, the employer is liable for the actions. The matter then turns on the scope of the officer’s employment and the employer-employee relationship. One court described the scope of employment as depending on

1. The act as being of the kind the employee is employed to perform
2. The act occurring substantially within the authorized time and space limits of the employment
3. The offender being motivated, at least in part, by a purpose to serve the master.

Liability then is a function of the control exercised or permitted in the relationship between the security officer and the hiring company. If the hiring company maintains a totally hands-off posture with respect to personnel supplied by the agency, it may well avoid liability for wrongful acts performed by such personnel. On the other hand, there is some precedent for considering the hiring company as sharing some liability simply by virtue of its underlying rights of control over its own premises, no matter how it wishes to exercise that control. Many hiring companies are, however, motivated to contractually reject any control of security personnel on their premises in order to avoid liability. This, as was pointed out in The Private Police, works to discourage hiring companies from regulating the activity of security employees and “the company that exercises controls, e.g., carefully examines the credentials of the guard, carefully determines the procedures the guard will follow, and pays close attention to all his activities, may still be substantially increasing its risk of liability to any third persons who are in fact, injured by an act of the guard.”

It is further suggested in this excellent study that there may be an expansion of certain nondelegable duty rules in consideration of the responsibilities for the actions of security personnel. As was discussed previously, the concept of the nondelegable duty provides that there are certain duties and responsibilities that are imposed on an individual and for which that

individual remains responsible even though an independent contractor is hired to implement them. Such duties currently encompass keeping the workplace safe and the premises reasonably safe for business visitors. It is also possible that the courts may find negligence in cases where the hiring companies, in an effort to avoid liability, have neglected to exercise any control over the selection and training of personnel, and they may further find that such negligence on the part of the hiring company has led to injury to third-party victims.

Criminal Liability

Criminal liability is most frequently used against private security personnel in cases of assault, battery, manslaughter, and murder. Other common charges include burglary, trespass, criminal defamation, false arrest, unlawful use of weapons, disorderly conduct, extortion, eavesdropping, theft, perjury, and kidnapping. Security officers charged with criminal liability have several options in defending their actions. First, they might try to show that they were entitled to use force in self-defense or that they made a reasonable mistake, which would negate criminal intent. Other defenses include entrapment, intoxication, insanity, consent (the parties involved concurred with the actions), and compulsion (the officer was forced or compelled to commit the act). As has been already noted in previous discussions, a corporation or an association could be charged with criminal liability as well as an individual officer.

Security Guidelines and Standards

“...It is also generally recognized that the security field does not have what might be classified as ‘generally accepted security practices’ comparable to the ‘generally accepted accounting practices’ that guide the accounting profession.” However, since the late 1990s, particularly since September 11, 2001, this situation has changed. Today, in many countries throughout the world, there is an increasing movement toward developing societal guidelines and standards for security.

In particular, ASIS International (ASIS), through its Commission on Standards and Guidelines, is strongly supporting global efforts in the development and promulgation of security standards via the International Organization for Standardization (ISO). ASIS has been recognized by ISO as an international organization and granted liaison status.


*Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests... ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public” (ASIS International. May 29, 2007. <www.asisonline.org/guidelines/guidelines.htm#standards>; March 14, 2009). In addition to providing members and the security community with access to a full range of programs and services, ASIS administers certification programs that include the Certified Protection Professional (CPP), Board Certified in Security Management, the Physical Security Professional (PSP), and the Professional Certified Investigator (PCI) (“ASIS International security certifications.” 2008. <www.asisonline.org/certification/index.xml>; November 2, 2008).

**ISO (International Organization for Standardization) is “the world’s largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 157 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a
on several technical committees. “As a non-governmental organization, ISO has no legal authority to enforce standards implementation. Although ISO standards are voluntary, they may become recognized as an industry best practice and a market requirement. For this reason, the liaison status with ISO affords ASIS and its membership the unique opportunity to play a leading role in shaping the development of standards that affect security.”

What Is Adequate Security?

For security, “it is difficult to protect against legal actions regardless of what measures of protection are taken unless there is a basic agreement about what constitutes enough security…. There has not, however, been a national effort developed to undertake the process of developing standards for the security industry as a whole because of the complexity of the issue.”

Despite the move toward guidelines and standards, the issue still remains of whether developing these guidelines and standards will allow an objective determination of “adequate security.” In the high-rise environment, part of the problem lies in the fact that virtually every building is different and no two security professionals will always agree on what constitutes adequate security for a particular facility. So many security recommendations are subjective determinations by individuals with varying opinions about the value of particular measures. For example, one security professional may rely heavily on using video surveillance systems to observe security violations, whereas another may prefer the heavy deployment of security personnel; one may emphasize the use of access cards to control entry to a facility, whereas another may prefer security staff to screen tenants and visitors. Even if security professionals were able to agree on what an adequate security level is for a particular facility, inevitably budgetary considerations still must be taken into consideration. A fully occupied, financially sound building in a thriving business district will be more likely to invest money in its security program than will a partially occupied building that charges lower-than-market rents because the facility has deteriorated and is in an area many businesses have vacated. The dilemma for the building owner or manager is that the latter building may actually have a greater need for security than the former.

Summary

- Various laws, codes, standards, and guidelines affect the security and fire life safety of high-rise buildings.
- The applicability of various laws, codes, and standards for security and fire safety.
- Security and liability are important considerations.
Key Terms

**Arrest.** “To deprive a person of his liberty by legal authority.”

**Authority having jurisdiction (AHJ).** “A federal, state or local entity that has statutory authority.”

**Certificate of occupancy.** “Document issued by governmental authority certifying that all or a designated portion of a building complies with the provisions of applicable statutes and regulations, and permitting occupancy for its designated use.”

**Court.** A “systematic collection; a private or official compilation of all permanent laws in force consolidated and classified according to subject matter.”

**Damages.** “A pecuniary compensation of indemnity, which may be recovered in the courts by any person who has suffered loss, detriment, or injury, whether to his person, property, or rights, through the unlawful act or omission or negligence of another.... Damages may be compensatory or punitive according to whether they are awarded as the measure of actual loss suffered or as punishment for outrageous conduct and to deter future transgressions.”

**Defendant.** “The person defending or denying; the party against whom relief or recovery is sought in an action or suit or the accused in a criminal case.”

**Foreseeability.** “The ability to know in advance; [for example] the reasonable anticipation that harm or injury is a likely result from certain acts or omissions.”

**Guideline.** A document that steers our understanding of a particular subject. It provides direction but does not require adherence to the course of action or the advice provided.

**Law.** “In its generic sense, is a body of rules or action or conduct prescribed by the controlling authority, and having binding legal force.”

**Liability.** “An obligation according to law or equity.”

**Negligence.** “The failure to use such care as a reasonably prudent and careful person would use under similar circumstances.”

**Performance-based codes.** “Detail the goals and objectives to be met and establish criteria for determining if the objective has been reached.... Thus, the designer and builder gain

---


29 ibid., pp. 389, 390.

30 ibid., p. 419.

31 ibid., p. 649.

32 ibid., p. 884.


added freedoms to select construction methods and materials that may be viewed as nontraditional as long as it can be shown that the performance criteria can be met.”

Plaintiff. “A person who brings an action; the party who complains or sues in a civil action and is so named on the record.”

Prescriptive-based codes. “Spell out in detail what materials can be used, the building geometry (heights and areas), and how the various components should be assembled.” Also, known as specification-based codes.

Reasonable care. “That degree of care which a person of ordinary prudence would exercise in the same or similar circumstances.”

Standard. “A model, type, or gauge used to establish or verify what is commonly regarded as acceptable or correct.”

Standard of care. “In law of negligence, that degree of care which a reasonably prudent person should exercise in same or similar circumstances. If a person’s conduct falls below such standard, he may be liable in damages for injuries or damages resulting from his conduct.”

Tort. “A civil action based on the principle that one individual can expect certain behavior from another individual. When the actions of one of the parties do not meet reasonable expectations, a tort action may result. In security applications, a guard [security officer] may take some action to interfere with the free movement of some person. There is a basis for a suit no matter whether the [security officer] knows the actions are wrong, or is unaware that the actions are wrong but acts in a negligent manner.”

Additional Reading


---


This page intentionally left blank
Epilogue

As the world population grows—and as its cities grow—not only must accommodation be provided for work and housing but there will be more and more pressure on energy conservation and the preservation of land for food production. Increasingly, then, the high-rise alternative will need to be considered, not so much by choice as by necessity.

—Lynn S. Beedle, Founding Chairman of the Council on Tall Buildings and Urban Habitat

This page intentionally left blank
### The World’s Tallest Buildings

This list consists of only buildings that are completed and officially ranked on CTBUH listings.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Taipei 101</td>
<td>Taipei</td>
<td>2004</td>
<td>101</td>
<td>509</td>
<td>1670</td>
<td>Composite Office</td>
</tr>
<tr>
<td>2</td>
<td>Shanghai World Financial Center</td>
<td>Shanghai</td>
<td>2008</td>
<td>101</td>
<td>492</td>
<td>1614</td>
<td>Composite Office</td>
</tr>
<tr>
<td>3</td>
<td>Petronas Tower 1</td>
<td>Kuala Lumpur</td>
<td>1998</td>
<td>88</td>
<td>452</td>
<td>1483</td>
<td>Composite Office</td>
</tr>
<tr>
<td>4</td>
<td>Petronas Tower 2</td>
<td>Kuala Lumpur</td>
<td>1998</td>
<td>88</td>
<td>452</td>
<td>1483</td>
<td>Composite Office</td>
</tr>
<tr>
<td>5</td>
<td>Sears Tower</td>
<td>Chicago</td>
<td>1974</td>
<td>110</td>
<td>442</td>
<td>1451</td>
<td>Steel Office</td>
</tr>
<tr>
<td>6</td>
<td>Jin Mao Building</td>
<td>Shanghai</td>
<td>1999</td>
<td>88</td>
<td>421</td>
<td>1341</td>
<td>Composite Office</td>
</tr>
<tr>
<td>7</td>
<td>Two International Finance Centre</td>
<td>Hong Kong</td>
<td>2003</td>
<td>88</td>
<td>415</td>
<td>1362</td>
<td>Composite Office</td>
</tr>
<tr>
<td>8</td>
<td>CITIC Plaza</td>
<td>Guangzhou</td>
<td>1996</td>
<td>80</td>
<td>391</td>
<td>1283</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>9</td>
<td>Shun Hing Square</td>
<td>Shenzhen</td>
<td>1998</td>
<td>69</td>
<td>386</td>
<td>1283</td>
<td>Composite Office</td>
</tr>
<tr>
<td>10</td>
<td>Empire State Building</td>
<td>New York</td>
<td>1931</td>
<td>102</td>
<td>361</td>
<td>1250</td>
<td>Steel Office</td>
</tr>
<tr>
<td>11</td>
<td>Central Plaza</td>
<td>Hong Kong</td>
<td>1992</td>
<td>78</td>
<td>374</td>
<td>1227</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>12</td>
<td>Bank of China</td>
<td>Hong Kong</td>
<td>1989</td>
<td>70</td>
<td>367</td>
<td>1205</td>
<td>Composite Office</td>
</tr>
<tr>
<td>13</td>
<td>Almas Tower</td>
<td>Dubai</td>
<td>2008</td>
<td>68</td>
<td>363</td>
<td>1191</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>14</td>
<td>Emirates Tower One</td>
<td>Dubai</td>
<td>1999</td>
<td>54</td>
<td>355</td>
<td>1165</td>
<td>Composite Office</td>
</tr>
<tr>
<td>15</td>
<td>Tunxun Sky Tower</td>
<td>Kaohsiung</td>
<td>1997</td>
<td>85</td>
<td>348</td>
<td>1140</td>
<td>Composite Office</td>
</tr>
<tr>
<td>16</td>
<td>Am Centre</td>
<td>Chicago</td>
<td>1973</td>
<td>83</td>
<td>346</td>
<td>1136</td>
<td>Steel Office</td>
</tr>
<tr>
<td>17</td>
<td>The Center</td>
<td>Hong Kong</td>
<td>1998</td>
<td>73</td>
<td>346</td>
<td>1135</td>
<td>Steel Office</td>
</tr>
<tr>
<td>18</td>
<td>John Hancock Center</td>
<td>Chicago</td>
<td>1969</td>
<td>77</td>
<td>319</td>
<td>1046</td>
<td>Concrete Office/Hotel</td>
</tr>
<tr>
<td>19</td>
<td>Rose Rotana Tower</td>
<td>Dubai</td>
<td>2007</td>
<td>72</td>
<td>333</td>
<td>1093</td>
<td>Composite Hotel</td>
</tr>
<tr>
<td>20</td>
<td>Shimao International Plaza</td>
<td>Shanghai</td>
<td>2008</td>
<td>60</td>
<td>333</td>
<td>1093</td>
<td>Concrete Hotel</td>
</tr>
<tr>
<td>21</td>
<td>Minsheng Bank Building</td>
<td>Wuhan</td>
<td>2008</td>
<td>68</td>
<td>331</td>
<td>1087</td>
<td>Steel Office</td>
</tr>
<tr>
<td>22</td>
<td>Q1</td>
<td>Gold Coast</td>
<td>2005</td>
<td>78</td>
<td>323</td>
<td>1058</td>
<td>Concrete Residential</td>
</tr>
<tr>
<td>23</td>
<td>World Trade Center</td>
<td>Dubai</td>
<td>1999</td>
<td>60</td>
<td>321</td>
<td>1057</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>24</td>
<td>Nina Tower I</td>
<td>Hong Kong</td>
<td>2006</td>
<td>60</td>
<td>319</td>
<td>1046</td>
<td>Composite Office/Hotel</td>
</tr>
<tr>
<td>25</td>
<td>Chrysler Building</td>
<td>New York</td>
<td>1930</td>
<td>77</td>
<td>319</td>
<td>1046</td>
<td>Steel Office</td>
</tr>
<tr>
<td>27</td>
<td>Bank of America Plaza</td>
<td>Atlanta</td>
<td>1993</td>
<td>55</td>
<td>317</td>
<td>1039</td>
<td>Composite Office</td>
</tr>
<tr>
<td>28</td>
<td>U.S. Bank Tower</td>
<td>Los Angeles</td>
<td>1990</td>
<td>73</td>
<td>310</td>
<td>1018</td>
<td>Steel Office</td>
</tr>
<tr>
<td>29</td>
<td>Menara Telekom Headquarters</td>
<td>Kuala Lumpur</td>
<td>1999</td>
<td>55</td>
<td>310</td>
<td>1017</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>30</td>
<td>Emirates Tower Two</td>
<td>Dubai</td>
<td>2000</td>
<td>56</td>
<td>309</td>
<td>1014</td>
<td>Concrete Hotel</td>
</tr>
<tr>
<td>31</td>
<td>AT&amp;T Corporate Center</td>
<td>Chicago</td>
<td>1989</td>
<td>60</td>
<td>307</td>
<td>1007</td>
<td>Composite Office</td>
</tr>
<tr>
<td>32</td>
<td>The Address Downtown Burj Dubai</td>
<td>Dubai</td>
<td>2008</td>
<td>63</td>
<td>306</td>
<td>1004</td>
<td>Concrete Hotel</td>
</tr>
<tr>
<td>33</td>
<td>JP Morgan Chase Tower</td>
<td>Houston</td>
<td>1982</td>
<td>75</td>
<td>305</td>
<td>1002</td>
<td>Composite Office</td>
</tr>
<tr>
<td>34</td>
<td>Baiyoke Tower II</td>
<td>Bangkok</td>
<td>1997</td>
<td>85</td>
<td>304</td>
<td>997</td>
<td>Concrete Hotel</td>
</tr>
<tr>
<td>35</td>
<td>Two Prudential Plaza</td>
<td>Chicago</td>
<td>1990</td>
<td>64</td>
<td>303</td>
<td>995</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>36</td>
<td>Wells Fargo Plaza</td>
<td>Houston</td>
<td>1983</td>
<td>71</td>
<td>302</td>
<td>992</td>
<td>Steel Office</td>
</tr>
<tr>
<td>37</td>
<td>Kingdom Centre</td>
<td>Riyadh</td>
<td>2002</td>
<td>41</td>
<td>302</td>
<td>992</td>
<td>Steel Office</td>
</tr>
<tr>
<td>38</td>
<td>Aspire Tower</td>
<td>Dubai</td>
<td>2006</td>
<td>36</td>
<td>300</td>
<td>984</td>
<td>Composite Office</td>
</tr>
<tr>
<td>39</td>
<td>One Island East</td>
<td>Hong Kong</td>
<td>2008</td>
<td>69</td>
<td>298</td>
<td>979</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>40</td>
<td>First Bank Tower</td>
<td>Toronto</td>
<td>1975</td>
<td>72</td>
<td>298</td>
<td>978</td>
<td>Steel Office</td>
</tr>
<tr>
<td>41</td>
<td>Eureka Tower</td>
<td>Melbourne</td>
<td>2006</td>
<td>91</td>
<td>297</td>
<td>975</td>
<td>Concrete Residential</td>
</tr>
<tr>
<td>42</td>
<td>Comcast Center</td>
<td>Philadelphia</td>
<td>2008</td>
<td>57</td>
<td>297</td>
<td>974</td>
<td>Composite Office</td>
</tr>
<tr>
<td>43</td>
<td>Landmark Tower</td>
<td>Yokohama</td>
<td>1993</td>
<td>73</td>
<td>296</td>
<td>972</td>
<td>Steel Office/Hotel</td>
</tr>
<tr>
<td>44</td>
<td>Emirates Crown</td>
<td>Dubai</td>
<td>2008</td>
<td>63</td>
<td>296</td>
<td>971</td>
<td>Concrete Residential</td>
</tr>
<tr>
<td>45</td>
<td>111 South Wacker Drive</td>
<td>Chicago</td>
<td>1990</td>
<td>66</td>
<td>293</td>
<td>961</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>46</td>
<td>SEG Plaza</td>
<td>Shenzhen</td>
<td>2006</td>
<td>71</td>
<td>292</td>
<td>957</td>
<td>Concrete Office/Hotel</td>
</tr>
<tr>
<td>47</td>
<td>American International Building</td>
<td>New York</td>
<td>1932</td>
<td>67</td>
<td>290</td>
<td>952</td>
<td>Steel Office</td>
</tr>
<tr>
<td>48</td>
<td>Key Tower</td>
<td>Cleveland</td>
<td>1991</td>
<td>57</td>
<td>289</td>
<td>947</td>
<td>Composite Office</td>
</tr>
<tr>
<td>49</td>
<td>Plaza 56</td>
<td>Shanghai</td>
<td>2001</td>
<td>66</td>
<td>288</td>
<td>945</td>
<td>Concrete/Steel Office</td>
</tr>
<tr>
<td>50</td>
<td>One Liberty Place</td>
<td>Philadelphia</td>
<td>1987</td>
<td>61</td>
<td>288</td>
<td>945</td>
<td>Steel Office</td>
</tr>
<tr>
<td>51</td>
<td>Millennium Tower</td>
<td>Dubai</td>
<td>2008</td>
<td>59</td>
<td>285</td>
<td>935</td>
<td>Concrete Residential</td>
</tr>
<tr>
<td>52</td>
<td>Tomorrow Square</td>
<td>Shanghai</td>
<td>2003</td>
<td>55</td>
<td>285</td>
<td>934</td>
<td>Composite Office/Hotel</td>
</tr>
<tr>
<td>53</td>
<td>Columbia Center</td>
<td>Seattle</td>
<td>1984</td>
<td>76</td>
<td>284</td>
<td>933</td>
<td>Composite Office</td>
</tr>
<tr>
<td>54</td>
<td>Chongqing World Trade Center</td>
<td>Chongqing</td>
<td>2005</td>
<td>60</td>
<td>283</td>
<td>929</td>
<td>Concrete Office</td>
</tr>
<tr>
<td>Rank</td>
<td>Building Name</td>
<td>City</td>
<td>Year</td>
<td>Stories</td>
<td>m</td>
<td>f</td>
<td>Material Use</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------</td>
<td>-----------------</td>
<td>------</td>
<td>---------</td>
<td>-----</td>
<td>-----</td>
<td>--------------</td>
</tr>
<tr>
<td>55</td>
<td>Cheung Kong Centre</td>
<td>Hong Kong</td>
<td>1999</td>
<td>63</td>
<td>283</td>
<td>928</td>
<td>Steel</td>
</tr>
<tr>
<td>56</td>
<td>The Trump Building</td>
<td>New York</td>
<td>1930</td>
<td>71</td>
<td>283</td>
<td>927</td>
<td>Steel</td>
</tr>
<tr>
<td>57</td>
<td>Bank of America Plaza</td>
<td>Dallas</td>
<td>1985</td>
<td>72</td>
<td>281</td>
<td>921</td>
<td>Composite</td>
</tr>
<tr>
<td>58</td>
<td>United Overseas Bank Plaza</td>
<td>Singapore</td>
<td>1992</td>
<td>66</td>
<td>280</td>
<td>919</td>
<td>Steel</td>
</tr>
<tr>
<td>59</td>
<td>Republic Plaza</td>
<td>Singapore</td>
<td>1995</td>
<td>66</td>
<td>280</td>
<td>919</td>
<td>Composite</td>
</tr>
<tr>
<td>60</td>
<td>Overseas Union Bank Centre</td>
<td>Singapore</td>
<td>1986</td>
<td>83</td>
<td>280</td>
<td>919</td>
<td>Steel</td>
</tr>
<tr>
<td>61</td>
<td>Citigroup Center</td>
<td>New York</td>
<td>1977</td>
<td>59</td>
<td>279</td>
<td>915</td>
<td>Steel</td>
</tr>
<tr>
<td>62</td>
<td>Hong Kong New World Tower</td>
<td>Shanghai</td>
<td>2002</td>
<td>61</td>
<td>278</td>
<td>913</td>
<td>Composite</td>
</tr>
<tr>
<td>63</td>
<td>Dhwang International Commerce Center</td>
<td>Nanjing</td>
<td>2006</td>
<td>54</td>
<td>276</td>
<td>906</td>
<td>Concrete</td>
</tr>
<tr>
<td>64</td>
<td>Scotia Plaza</td>
<td>Toronto</td>
<td>1989</td>
<td>68</td>
<td>275</td>
<td>902</td>
<td>Composite</td>
</tr>
<tr>
<td>65</td>
<td>Williams Tower</td>
<td>Houston</td>
<td>1983</td>
<td>64</td>
<td>275</td>
<td>901</td>
<td>Steel</td>
</tr>
<tr>
<td>66</td>
<td>Wuhan World Trade Tower</td>
<td>Wuhan</td>
<td>1998</td>
<td>60</td>
<td>273</td>
<td>896</td>
<td>Office</td>
</tr>
<tr>
<td>67</td>
<td>The Cullinan I</td>
<td>Hong Kong</td>
<td>2008</td>
<td>68</td>
<td>270</td>
<td>886</td>
<td>Concrete</td>
</tr>
<tr>
<td>68</td>
<td>The Cullinan II</td>
<td>Hong Kong</td>
<td>2008</td>
<td>68</td>
<td>270</td>
<td>886</td>
<td>Concrete</td>
</tr>
<tr>
<td>69</td>
<td>Renaissance Tower</td>
<td>Dallas</td>
<td>1975</td>
<td>56</td>
<td>270</td>
<td>886</td>
<td>Steel</td>
</tr>
<tr>
<td>70</td>
<td>China International Center Tower B</td>
<td>Guangzhou</td>
<td>2007</td>
<td>82</td>
<td>269</td>
<td>884</td>
<td>Concrete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>Dapeng International Plaza</td>
<td>Guangzhou</td>
<td>2006</td>
<td>56</td>
<td>269</td>
<td>883</td>
<td>Composite</td>
</tr>
<tr>
<td>72</td>
<td>21st Century Tower</td>
<td>Dubai</td>
<td>2003</td>
<td>55</td>
<td>269</td>
<td>883</td>
<td>Concrete</td>
</tr>
<tr>
<td>73</td>
<td>One Lujiazui</td>
<td>Shanghai</td>
<td>2008</td>
<td>47</td>
<td>269</td>
<td>883</td>
<td>Concrete</td>
</tr>
<tr>
<td>74</td>
<td>Naberezhnaya Tower C</td>
<td>Moscow</td>
<td>2007</td>
<td>61</td>
<td>268</td>
<td>881</td>
<td>Composite</td>
</tr>
<tr>
<td>75</td>
<td>Al Faisaliah Center</td>
<td>Riyadh</td>
<td>2000</td>
<td>30</td>
<td>267</td>
<td>876</td>
<td>Concrete</td>
</tr>
<tr>
<td>76</td>
<td>600 North Michigan Avenue</td>
<td>Chicago</td>
<td>1989</td>
<td>66</td>
<td>265</td>
<td>871</td>
<td>Steel/Concrete</td>
</tr>
<tr>
<td>77</td>
<td>Bank of America Corporate Center</td>
<td>Charlotte</td>
<td>1992</td>
<td>60</td>
<td>265</td>
<td>871</td>
<td>Concrete</td>
</tr>
<tr>
<td>78</td>
<td>Al Kazim Tower 1</td>
<td>Dubai</td>
<td>2008</td>
<td>53</td>
<td>265</td>
<td>869</td>
<td>Concrete</td>
</tr>
<tr>
<td>79</td>
<td>Al Kazim Tower 2</td>
<td>Dubai</td>
<td>2008</td>
<td>53</td>
<td>265</td>
<td>869</td>
<td>Concrete</td>
</tr>
<tr>
<td>80</td>
<td>BOCOM Financial Towers</td>
<td>Shanghai</td>
<td>1999</td>
<td>52</td>
<td>265</td>
<td>869</td>
<td>Concrete</td>
</tr>
<tr>
<td>81</td>
<td>120 Collins St.</td>
<td>Melbourne</td>
<td>1991</td>
<td>52</td>
<td>265</td>
<td>869</td>
<td>Concrete</td>
</tr>
<tr>
<td>82</td>
<td>Suntrust Plaza</td>
<td>Atlanta</td>
<td>1992</td>
<td>60</td>
<td>264</td>
<td>867</td>
<td>Concrete</td>
</tr>
<tr>
<td>83</td>
<td>Triumph Palace</td>
<td>Moscow</td>
<td>2005</td>
<td>61</td>
<td>264</td>
<td>866</td>
<td>Concrete</td>
</tr>
<tr>
<td>84</td>
<td>Shenzhen Special Zone Daily Tower</td>
<td>Shenzhen</td>
<td>1998</td>
<td>42</td>
<td>264</td>
<td>866</td>
<td>Concrete</td>
</tr>
<tr>
<td>85</td>
<td>Tower Palace Three, Tower G</td>
<td>Seoul</td>
<td>2004</td>
<td>73</td>
<td>264</td>
<td>865</td>
<td>Concrete</td>
</tr>
<tr>
<td>86</td>
<td>Trump World Tower</td>
<td>New York</td>
<td>2001</td>
<td>72</td>
<td>262</td>
<td>861</td>
<td>Concrete</td>
</tr>
<tr>
<td>87</td>
<td>Water Tower Place</td>
<td>Chicago</td>
<td>1976</td>
<td>74</td>
<td>252</td>
<td>859</td>
<td>Concrete</td>
</tr>
<tr>
<td>88</td>
<td>Grand Gateway Plaza I</td>
<td>Shanghai</td>
<td>2005</td>
<td>54</td>
<td>262</td>
<td>859</td>
<td>Concrete</td>
</tr>
<tr>
<td>89</td>
<td>Grand Gateway Plaza II</td>
<td>Shanghai</td>
<td>2005</td>
<td>54</td>
<td>262</td>
<td>859</td>
<td>Concrete</td>
</tr>
<tr>
<td>90</td>
<td>Aon Center</td>
<td>Los Angeles</td>
<td>1974</td>
<td>62</td>
<td>262</td>
<td>858</td>
<td>Steel</td>
</tr>
<tr>
<td>91</td>
<td>Hotel Panorama</td>
<td>Hong Kong</td>
<td>2007</td>
<td>64</td>
<td>261</td>
<td>856</td>
<td>Concrete</td>
</tr>
<tr>
<td>92</td>
<td>BCE Place-Canada Trust Tower</td>
<td>Toronto</td>
<td>1990</td>
<td>53</td>
<td>261</td>
<td>856</td>
<td>Composite</td>
</tr>
<tr>
<td>93</td>
<td>Dual Towers 1</td>
<td>Manama</td>
<td>2007</td>
<td>57</td>
<td>260</td>
<td>853</td>
<td>Concrete</td>
</tr>
<tr>
<td>94</td>
<td>Dual Towers 2</td>
<td>Manama</td>
<td>2007</td>
<td>57</td>
<td>260</td>
<td>853</td>
<td>Concrete</td>
</tr>
<tr>
<td>95</td>
<td>101 Collins Street</td>
<td>Melbourne</td>
<td>1991</td>
<td>50</td>
<td>260</td>
<td>853</td>
<td>Composite</td>
</tr>
<tr>
<td>96</td>
<td>Transamericas Pyramid</td>
<td>San Francisco</td>
<td>1972</td>
<td>48</td>
<td>260</td>
<td>853</td>
<td>Composite</td>
</tr>
<tr>
<td>97</td>
<td>GE Building, Rockefeller Center</td>
<td>New York</td>
<td>1933</td>
<td>70</td>
<td>259</td>
<td>850</td>
<td>Steel</td>
</tr>
<tr>
<td>98</td>
<td>Chase Tower</td>
<td>Chicago</td>
<td>1969</td>
<td>60</td>
<td>259</td>
<td>850</td>
<td>Steel</td>
</tr>
<tr>
<td>99</td>
<td>Commerzbank Zentrale</td>
<td>Frankfurt</td>
<td>1997</td>
<td>56</td>
<td>259</td>
<td>850</td>
<td>Composite</td>
</tr>
<tr>
<td>100</td>
<td>Two Liberty Place</td>
<td>Philadelphia</td>
<td>1990</td>
<td>58</td>
<td>258</td>
<td>848</td>
<td>Steel</td>
</tr>
</tbody>
</table>

Footnotes:
1. Height is measured from sidewalk level of the main entrance to the architectural top of the building, including spires, but not including antennas, signage, or flag poles.
2. For a more complete overview of the CTBUH's height criteria, see http://www.ctbuh.org/criteria.htm

© Council on Tall Buildings and Urban Habitat
### 100 Tallest Buildings in the World (not including spires)

**Key:**
- Building is completed and officially ranked by the CTBUH
- Building is under construction and topped out architecturally

**Last updated: January, 2009**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Country</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material Used</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Burj Dubai</td>
<td>Dubai</td>
<td>U.A.E.</td>
<td>2009</td>
<td>162</td>
<td>745</td>
<td>2428</td>
<td>Concrete/Steel</td>
<td>Hotel/Residential/Office</td>
</tr>
<tr>
<td>2</td>
<td>Shanghai World Financial Center</td>
<td>Shanghai</td>
<td>China</td>
<td>2006</td>
<td>101</td>
<td>492</td>
<td>1614</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>3</td>
<td>Taipei 101</td>
<td>Taipei</td>
<td>Taiwan</td>
<td>2004</td>
<td>101</td>
<td>449</td>
<td>1473</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>4</td>
<td>Sears Tower</td>
<td>Chicago</td>
<td>United States</td>
<td>1974</td>
<td>108</td>
<td>442</td>
<td>1451</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>5</td>
<td>Wanchai Tower</td>
<td>Hong Kong</td>
<td>China</td>
<td>2003</td>
<td>88</td>
<td>401</td>
<td>1316</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>6</td>
<td>Two International Finance Centre</td>
<td>Hong Kong</td>
<td>China</td>
<td>1999</td>
<td>86</td>
<td>383</td>
<td>1255</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>7</td>
<td>Jin Mao Bldg.</td>
<td>Shanghai</td>
<td>China</td>
<td>1998</td>
<td>86</td>
<td>379</td>
<td>1242</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>8</td>
<td>Empire State Building</td>
<td>New York</td>
<td>United States</td>
<td>1993</td>
<td>102</td>
<td>381</td>
<td>1250</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>9</td>
<td>Petronas Tower I</td>
<td>Kuala Lumpur</td>
<td>Malaysia</td>
<td>1996</td>
<td>88</td>
<td>379</td>
<td>1242</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>10</td>
<td>Petronas Tower II</td>
<td>Kuala Lumpur</td>
<td>Malaysia</td>
<td>1999</td>
<td>88</td>
<td>379</td>
<td>1242</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Trump International Hotel &amp; Tower</td>
<td>Chicago</td>
<td>United States</td>
<td>2009</td>
<td>96</td>
<td>358</td>
<td>1174</td>
<td>Concrete</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>12</td>
<td>Tunels &amp; Chain-Tal Tower</td>
<td>Kaohsiung</td>
<td>Taiwan</td>
<td>1998</td>
<td>85</td>
<td>348</td>
<td>1140</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>13</td>
<td>Jin Mao Tower</td>
<td>Shanghai</td>
<td>China</td>
<td>2000</td>
<td>90</td>
<td>347</td>
<td>1136</td>
<td>Concrete/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>14</td>
<td>John Hancock Center</td>
<td>Chicago</td>
<td>United States</td>
<td>1969</td>
<td>100</td>
<td>344</td>
<td>1127</td>
<td>Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>15</td>
<td>Nanjing Greenland Financial Center</td>
<td>Nanjing</td>
<td>China</td>
<td>2009</td>
<td>69</td>
<td>331</td>
<td>1086</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>16</td>
<td>Ryugyong Hotel</td>
<td>Pyongyang</td>
<td>North Korea</td>
<td>1992</td>
<td>105</td>
<td>330</td>
<td>1083</td>
<td>Concrete</td>
<td>Hotel</td>
</tr>
<tr>
<td>17</td>
<td>China World Trade Center Tower III</td>
<td>Beijing</td>
<td>China</td>
<td>2009</td>
<td>73</td>
<td>330</td>
<td>1083</td>
<td>Concrete/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>18</td>
<td>The Index</td>
<td>Dubai</td>
<td>U.A.E.</td>
<td>2009</td>
<td>80</td>
<td>328</td>
<td>1076</td>
<td>Composite</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>19</td>
<td>Shun Hing Square</td>
<td>Shenzhen</td>
<td>China</td>
<td>1996</td>
<td>69</td>
<td>325</td>
<td>1066</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>20</td>
<td>CITIC Plaza</td>
<td>Guangzhou</td>
<td>China</td>
<td>1997</td>
<td>80</td>
<td>323</td>
<td>1060</td>
<td>Concrete</td>
<td>Office</td>
</tr>
<tr>
<td>21</td>
<td>Nina Tower I</td>
<td>Hong Kong</td>
<td>China</td>
<td>2007</td>
<td>80</td>
<td>319</td>
<td>1046</td>
<td>Concrete/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>22</td>
<td>Rose Rotana Tower</td>
<td>Dubai</td>
<td>United States</td>
<td>2006</td>
<td>72</td>
<td>315</td>
<td>1034</td>
<td>Composite/Steel</td>
<td>Hotel</td>
</tr>
<tr>
<td>23</td>
<td>Emirates Tower One</td>
<td>Dubai</td>
<td>United States</td>
<td>2000</td>
<td>53</td>
<td>311</td>
<td>1020</td>
<td>Composite/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>24</td>
<td>Marina Bay Tower</td>
<td>香港</td>
<td>United States</td>
<td>1993</td>
<td>73</td>
<td>316</td>
<td>1018</td>
<td>Concrete</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>25</td>
<td>Menara Telekom Headquarters</td>
<td>Kuala Lumpur</td>
<td>Malaysia</td>
<td>2009</td>
<td>59</td>
<td>310</td>
<td>1017</td>
<td>Concrete</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>26</td>
<td>Central Plaza</td>
<td>Hong Kong</td>
<td>China</td>
<td>1992</td>
<td>78</td>
<td>309</td>
<td>1014</td>
<td>Concrete/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>27</td>
<td>Almas Tower</td>
<td>Dubai</td>
<td>United States</td>
<td>2008</td>
<td>68</td>
<td>306</td>
<td>1005</td>
<td>Composite/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>28</td>
<td>Bank of China</td>
<td>Hong Kong</td>
<td>China</td>
<td>1989</td>
<td>70</td>
<td>305</td>
<td>1001</td>
<td>Composite/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>29</td>
<td>Babyboke Tower II</td>
<td>Bangkok</td>
<td>Thailand</td>
<td>1997</td>
<td>85</td>
<td>304</td>
<td>997</td>
<td>Concrete</td>
<td>Hotel</td>
</tr>
<tr>
<td>30</td>
<td>Wells Fargo Plaza</td>
<td>Houston</td>
<td>United States</td>
<td>1983</td>
<td>71</td>
<td>302</td>
<td>992</td>
<td>Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>31</td>
<td>Kingdom Centre</td>
<td>Riyadh</td>
<td>Saudi Arabia</td>
<td>2002</td>
<td>41</td>
<td>302</td>
<td>992</td>
<td>Concrete/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>32</td>
<td>The Center</td>
<td>Hong Kong</td>
<td>China</td>
<td>1998</td>
<td>73</td>
<td>362</td>
<td>991</td>
<td>Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>33</td>
<td>Aspire Tower</td>
<td>Doha</td>
<td>Qatar</td>
<td>2007</td>
<td>36</td>
<td>300</td>
<td>984</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>34</td>
<td>One Island East</td>
<td>Hong Kong</td>
<td>China</td>
<td>2008</td>
<td>69</td>
<td>298</td>
<td>979</td>
<td>Concrete</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>35</td>
<td>First Bank Tower</td>
<td>Toronto</td>
<td>Canada</td>
<td>1975</td>
<td>72</td>
<td>298</td>
<td>979</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>36</td>
<td>Eureka Tower</td>
<td>Melbourne</td>
<td>Australia</td>
<td>2005</td>
<td>91</td>
<td>297</td>
<td>975</td>
<td>Concrete</td>
<td>Residential</td>
</tr>
<tr>
<td>37</td>
<td>Comcast Center</td>
<td>Philadelphia</td>
<td>United States</td>
<td>2006</td>
<td>57</td>
<td>297</td>
<td>974</td>
<td>Composite</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>38</td>
<td>Landmark Tower</td>
<td>Yokohama</td>
<td>Japan</td>
<td>1993</td>
<td>73</td>
<td>296</td>
<td>972</td>
<td>Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>39</td>
<td>311 S. Wacker Drive</td>
<td>Chicago</td>
<td>United States</td>
<td>1990</td>
<td>66</td>
<td>283</td>
<td>961</td>
<td>Concrete</td>
<td>Office</td>
</tr>
<tr>
<td>40</td>
<td>SEI Plaza</td>
<td>Shenzhen</td>
<td>China</td>
<td>2000</td>
<td>71</td>
<td>292</td>
<td>957</td>
<td>Concrete</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>41</td>
<td>Minsheng Bank Bldg.</td>
<td>Wuhan</td>
<td>China</td>
<td>2008</td>
<td>68</td>
<td>290</td>
<td>951</td>
<td>Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>42</td>
<td>Plaza 66</td>
<td>Shanghai</td>
<td>China</td>
<td>2007</td>
<td>66</td>
<td>288</td>
<td>945</td>
<td>Concrete/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>43</td>
<td>Bank of America Tower</td>
<td>New York</td>
<td>United States</td>
<td>2009</td>
<td>52</td>
<td>288</td>
<td>945</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>44</td>
<td>Capital City Moscow Tower</td>
<td>Moscow</td>
<td>Russia</td>
<td>2009</td>
<td>73</td>
<td>286</td>
<td>938</td>
<td>Concrete</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>45</td>
<td>Tomorrow Square</td>
<td>Shanghai</td>
<td>China</td>
<td>2000</td>
<td>55</td>
<td>285</td>
<td>934</td>
<td>Concrete/Steel</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>46</td>
<td>Columbia Center</td>
<td>Seattle</td>
<td>United States</td>
<td>1985</td>
<td>76</td>
<td>284</td>
<td>933</td>
<td>Concrete/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>47</td>
<td>Bank of America Plaza</td>
<td>Atlanta</td>
<td>United States</td>
<td>1992</td>
<td>55</td>
<td>284</td>
<td>933</td>
<td>Concrete/Steel</td>
<td>Office</td>
</tr>
<tr>
<td>48</td>
<td>Cheung Kong Centre</td>
<td>Hong Kong</td>
<td>China</td>
<td>1999</td>
<td>63</td>
<td>283</td>
<td>928</td>
<td>Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>49</td>
<td>Chrysler Bldg.</td>
<td>New York</td>
<td>United States</td>
<td>1930</td>
<td>77</td>
<td>282</td>
<td>925</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Bank of America Plaza</td>
<td>Dallas</td>
<td>United States</td>
<td>1985</td>
<td>72</td>
<td>281</td>
<td>921</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>52</td>
<td>The Address Downtown Burj Dubai</td>
<td>Dubai</td>
<td>United States</td>
<td>2008</td>
<td>63</td>
<td>280</td>
<td>920</td>
<td>Concrete</td>
<td>Hotel</td>
</tr>
<tr>
<td>53</td>
<td>United Overseas Bank Plaza One</td>
<td>Singapore</td>
<td>Singapore</td>
<td>1992</td>
<td>66</td>
<td>280</td>
<td>919</td>
<td>Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>54</td>
<td>Republic Plaza</td>
<td>Singapore</td>
<td>Singapore</td>
<td>1995</td>
<td>66</td>
<td>280</td>
<td>919</td>
<td>Concrete/Steel</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>55</td>
<td>Overseas Union Bank Centre</td>
<td>Singapore</td>
<td>Singapore</td>
<td>1988</td>
<td>63</td>
<td>280</td>
<td>919</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>56</td>
<td>Emirates Crown</td>
<td>Dubai</td>
<td>United States</td>
<td>2008</td>
<td>63</td>
<td>286*</td>
<td>919*</td>
<td>Concrete</td>
<td>Residential</td>
</tr>
<tr>
<td>57</td>
<td>Citigroup Center</td>
<td>New York</td>
<td>United States</td>
<td>1977</td>
<td>59</td>
<td>279</td>
<td>915</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>Rank</td>
<td>Building Name</td>
<td>City</td>
<td>Country</td>
<td>Year</td>
<td>Stories</td>
<td>m</td>
<td>f</td>
<td>Material</td>
<td>Use</td>
</tr>
<tr>
<td>------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>------</td>
<td>---------</td>
<td>-----</td>
<td>-----</td>
<td>----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>58</td>
<td>Two Prudential Plaza</td>
<td>Chicago</td>
<td>United States</td>
<td>1990</td>
<td>64</td>
<td>278</td>
<td>912</td>
<td>Concrete</td>
<td>Office</td>
</tr>
<tr>
<td>59</td>
<td>Q1</td>
<td>Gold Coast</td>
<td>Australia</td>
<td>2005</td>
<td>78</td>
<td>275</td>
<td>902</td>
<td>Concrete</td>
<td>Residential</td>
</tr>
<tr>
<td>60</td>
<td>Scotia Plaza</td>
<td>Toronto</td>
<td>Canada</td>
<td>1989</td>
<td>68</td>
<td>275</td>
<td>902</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>61</td>
<td>Williams Tower</td>
<td>Houston</td>
<td>United States</td>
<td>1963</td>
<td>64</td>
<td>275</td>
<td>901</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>62</td>
<td>Key Tower</td>
<td>Cleveland</td>
<td>United States</td>
<td>1991</td>
<td>57</td>
<td>271</td>
<td>888</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>63</td>
<td>The Cullinan I</td>
<td>Hong Kong</td>
<td>China</td>
<td>2008</td>
<td>68</td>
<td>270</td>
<td>886</td>
<td>Concrete</td>
<td>Residential</td>
</tr>
<tr>
<td>64</td>
<td>The Cullinan II</td>
<td>Hong Kong</td>
<td>China</td>
<td>2008</td>
<td>68</td>
<td>270</td>
<td>886</td>
<td>Concrete</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>65</td>
<td>A&amp;T Corporate Center</td>
<td>Chicago</td>
<td>United States</td>
<td>1989</td>
<td>61</td>
<td>270</td>
<td>886</td>
<td>Composite</td>
<td>Office</td>
</tr>
<tr>
<td>66</td>
<td>China International Center Tower B</td>
<td>Guangzhou</td>
<td>China</td>
<td>2007</td>
<td>62</td>
<td>269</td>
<td>884</td>
<td>Concrete</td>
<td>Office</td>
</tr>
<tr>
<td>67</td>
<td>One Liberty Place</td>
<td>Philadelphia</td>
<td>United States</td>
<td>1987</td>
<td>61</td>
<td>269</td>
<td>883</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>68</td>
<td>Naberezhnyaya Tower C</td>
<td>Moscow</td>
<td>Russia</td>
<td>2007</td>
<td>61</td>
<td>268</td>
<td>881</td>
<td>Composite</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>69</td>
<td>900 N. Michigan Ave.</td>
<td>Chicago</td>
<td>United States</td>
<td>1989</td>
<td>66</td>
<td>265</td>
<td>871</td>
<td>Steel/Concrete</td>
<td>Retail/Hotel/Office/Residential</td>
</tr>
<tr>
<td>70</td>
<td>Sun Trust Plaza</td>
<td>Atlanta</td>
<td>United States</td>
<td>1992</td>
<td>60</td>
<td>264</td>
<td>867</td>
<td>Concrete</td>
<td>Office</td>
</tr>
<tr>
<td>71</td>
<td>Tower Palace Three, Tower G</td>
<td>Seoul</td>
<td>South Korea</td>
<td>2004</td>
<td>73</td>
<td>264</td>
<td>865</td>
<td>Composite</td>
<td>Residential</td>
</tr>
<tr>
<td>72</td>
<td>Trump World Tower</td>
<td>New York</td>
<td>United States</td>
<td>2001</td>
<td>72</td>
<td>262</td>
<td>861</td>
<td>Concrete</td>
<td>Residential</td>
</tr>
<tr>
<td>73</td>
<td>Chongqing World Trade Center</td>
<td>Chongping</td>
<td>China</td>
<td>2005</td>
<td>60</td>
<td>262</td>
<td>860</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>74</td>
<td>Water Tower Plaza</td>
<td>Chicago</td>
<td>United States</td>
<td>1976</td>
<td>74</td>
<td>262</td>
<td>859</td>
<td>Concrete</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>75</td>
<td>Grand Gateway Plaza I</td>
<td>Shanghai</td>
<td>China</td>
<td>2005</td>
<td>54</td>
<td>262</td>
<td>859</td>
<td>Concrete</td>
<td>Office</td>
</tr>
<tr>
<td>76</td>
<td>Grand Gateway Plaza II</td>
<td>Shanghai</td>
<td>China</td>
<td>2005</td>
<td>54</td>
<td>252</td>
<td>859</td>
<td>Concrete</td>
<td>Office</td>
</tr>
<tr>
<td>77</td>
<td>Aon Center</td>
<td>Los Angeles</td>
<td>United States</td>
<td>1974</td>
<td>62</td>
<td>262</td>
<td>858</td>
<td>Steel</td>
<td>Office</td>
</tr>
<tr>
<td>78</td>
<td>Hotel Panorama</td>
<td>Hong Kong</td>
<td>China</td>
<td>2007</td>
<td>64</td>
<td>261</td>
<td>856</td>
<td>Concrete</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>79</td>
<td>Emirates Towers Two</td>
<td>Dubai</td>
<td>U.A.E.</td>
<td>2000</td>
<td>56</td>
<td>261</td>
<td>856</td>
<td>Concrete</td>
<td>Hotel</td>
</tr>
</tbody>
</table>

For a more complete overview of the CTBUH's height criteria, see [http://www.ctbuh.org/criteria.htm](http://www.ctbuh.org/criteria.htm)
## tallest single-function office buildings in the world

This list includes buildings that are under construction. Only buildings that are completed are officially ranked on CTBUH listings.

**Key:**
- Building is completed and officially ranked by the CTBUH
- Building is under construction and topped out architecturally, but not topped out architecturally
- Building is under construction, but currently on hold

### last updated: December, 2008

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>World Trade Center One</td>
<td>New York</td>
<td>2013</td>
<td>105</td>
<td>541</td>
<td>1776</td>
<td>Composite</td>
</tr>
<tr>
<td>2</td>
<td>Taipei 101</td>
<td>Taipei</td>
<td>2004</td>
<td>101</td>
<td>509</td>
<td>1670</td>
<td>Composite</td>
</tr>
<tr>
<td>3</td>
<td>Federation Towers - Vostok Tower</td>
<td>Moscow</td>
<td>2010</td>
<td>95</td>
<td>509#</td>
<td>1670#</td>
<td>Concrete/Steel</td>
</tr>
<tr>
<td>4</td>
<td>Petronas Tower 1</td>
<td>Kuala Lumpur</td>
<td>1998</td>
<td>88</td>
<td>452</td>
<td>1483</td>
<td>Composite</td>
</tr>
<tr>
<td>5</td>
<td>Petronas Tower 2</td>
<td>Kuala Lumpur</td>
<td>1998</td>
<td>88</td>
<td>452</td>
<td>1483</td>
<td>Composite</td>
</tr>
<tr>
<td>6</td>
<td>Sears Tower</td>
<td>Chicago</td>
<td>1974</td>
<td>110</td>
<td>442</td>
<td>1451</td>
<td>Steel</td>
</tr>
<tr>
<td>7</td>
<td>Two International Finance Centre</td>
<td>Hong Kong</td>
<td>2003</td>
<td>88</td>
<td>415</td>
<td>1362</td>
<td>Composite</td>
</tr>
<tr>
<td>8</td>
<td>Al Hamra Tower</td>
<td>Dubai</td>
<td>2010</td>
<td>77</td>
<td>412</td>
<td>1352</td>
<td>Composite</td>
</tr>
<tr>
<td>9</td>
<td>Citic Plaza</td>
<td>Guangzhou</td>
<td>1996</td>
<td>80</td>
<td>391</td>
<td>1283</td>
<td>Concrete</td>
</tr>
<tr>
<td>10</td>
<td>World Trade Center One</td>
<td>New York</td>
<td>2013</td>
<td>105</td>
<td>541</td>
<td>1776</td>
<td>Composite</td>
</tr>
<tr>
<td>11</td>
<td>Empire State Building</td>
<td>New York</td>
<td>1931</td>
<td>102</td>
<td>381</td>
<td>1250</td>
<td>Steel</td>
</tr>
<tr>
<td>12</td>
<td>Central Plaza</td>
<td>Hong Kong</td>
<td>1992</td>
<td>78</td>
<td>374</td>
<td>1227</td>
<td>Concrete</td>
</tr>
<tr>
<td>13</td>
<td>Bank of China</td>
<td>Hong Kong</td>
<td>1989</td>
<td>70</td>
<td>367</td>
<td>1205</td>
<td>Mixed</td>
</tr>
<tr>
<td>14</td>
<td>Bank of America Tower</td>
<td>New York</td>
<td>2009</td>
<td>54</td>
<td>366</td>
<td>1200</td>
<td>Steel</td>
</tr>
<tr>
<td>15</td>
<td>Almas Tower</td>
<td>Dubai</td>
<td>2008</td>
<td>68</td>
<td>363</td>
<td>1191</td>
<td>Concrete/Steel</td>
</tr>
<tr>
<td>16</td>
<td>Emirates Tower One</td>
<td>Dubai</td>
<td>1999</td>
<td>54</td>
<td>355</td>
<td>1165</td>
<td>Composite</td>
</tr>
<tr>
<td>17</td>
<td>Sino-Steel International Tower</td>
<td>Tianjin</td>
<td>2011</td>
<td>80</td>
<td>358</td>
<td>1175</td>
<td>Concrete</td>
</tr>
<tr>
<td>18</td>
<td>Ghazibua International Plaza</td>
<td>Wuhan</td>
<td>1993</td>
<td>55</td>
<td>317</td>
<td>1039</td>
<td>Composite</td>
</tr>
<tr>
<td>19</td>
<td>The Center</td>
<td>Chicago</td>
<td>1973</td>
<td>83</td>
<td>346</td>
<td>1136</td>
<td>Steel</td>
</tr>
<tr>
<td>20</td>
<td>Tianjin World Financial Center</td>
<td>Tianjin</td>
<td>2010</td>
<td>76</td>
<td>337</td>
<td>1106</td>
<td>Steel</td>
</tr>
<tr>
<td>21</td>
<td>Parcl Tower A</td>
<td>Seoul</td>
<td>2011</td>
<td>72</td>
<td>334</td>
<td>1095</td>
<td>Concrete/Steel</td>
</tr>
<tr>
<td>22</td>
<td>Minsheng Bank Building</td>
<td>Wuhan</td>
<td>2008</td>
<td>68</td>
<td>331</td>
<td>1087</td>
<td>Steel</td>
</tr>
<tr>
<td>23</td>
<td>Lam Tata Tower 2</td>
<td>Dubai</td>
<td>2010</td>
<td>60</td>
<td>320</td>
<td>1050</td>
<td>Concrete</td>
</tr>
<tr>
<td>24</td>
<td>White Magnolia Plaza 1</td>
<td>Shanghai</td>
<td>2012</td>
<td>66</td>
<td>320</td>
<td>1048</td>
<td>Steel</td>
</tr>
<tr>
<td>25</td>
<td>Chrysler Building</td>
<td>New York</td>
<td>1930</td>
<td>77</td>
<td>319</td>
<td>1046</td>
<td>Steel</td>
</tr>
<tr>
<td>27</td>
<td>Bank of America Plaza</td>
<td>Atlanta</td>
<td>1993</td>
<td>55</td>
<td>317</td>
<td>1039</td>
<td>Composite</td>
</tr>
<tr>
<td>28</td>
<td>U.S. Bank Tower</td>
<td>Los Angeles</td>
<td>1990</td>
<td>73</td>
<td>310</td>
<td>1018</td>
<td>Steel</td>
</tr>
<tr>
<td>29</td>
<td>Menara Telekom Headquarters</td>
<td>Kuala Lumpur</td>
<td>1999</td>
<td>55</td>
<td>310</td>
<td>1017</td>
<td>Concrete</td>
</tr>
<tr>
<td>30</td>
<td>City Hall and City Duma</td>
<td>Guangzhou</td>
<td>2010</td>
<td>71</td>
<td>310</td>
<td>1016</td>
<td>Concrete</td>
</tr>
<tr>
<td>31</td>
<td>AT&amp;T Corporate Center</td>
<td>Chicago</td>
<td>1989</td>
<td>60</td>
<td>307</td>
<td>1007</td>
<td>Composite</td>
</tr>
<tr>
<td>32</td>
<td>JP Morgan Chase Tower</td>
<td>Houston</td>
<td>1982</td>
<td>75</td>
<td>305</td>
<td>1002</td>
<td>Composite</td>
</tr>
<tr>
<td>33</td>
<td>Two Prudential Plaza</td>
<td>Chicago</td>
<td>1990</td>
<td>64</td>
<td>303</td>
<td>995</td>
<td>Concrete</td>
</tr>
<tr>
<td>34</td>
<td>Leatop Plaza</td>
<td>Guangzhou</td>
<td>2000</td>
<td>64</td>
<td>303</td>
<td>993</td>
<td>Concrete</td>
</tr>
<tr>
<td>35</td>
<td>Wells Fargo Plaza</td>
<td>Houston</td>
<td>1983</td>
<td>71</td>
<td>302</td>
<td>992</td>
<td>Steel</td>
</tr>
<tr>
<td>36</td>
<td>Wells Fargo Plaza</td>
<td>Chicago</td>
<td>1990</td>
<td>64</td>
<td>303</td>
<td>995</td>
<td>Concrete</td>
</tr>
<tr>
<td>37</td>
<td>Wells Fargo Plaza</td>
<td>Houston</td>
<td>1983</td>
<td>71</td>
<td>302</td>
<td>992</td>
<td>Steel</td>
</tr>
<tr>
<td>38</td>
<td>Tameer Commercial Tower</td>
<td>Abu Dhabi</td>
<td>2011</td>
<td>74</td>
<td>300</td>
<td>985</td>
<td>Concrete</td>
</tr>
<tr>
<td>39</td>
<td>Gran Torre Costanera</td>
<td>Santiago</td>
<td>2009</td>
<td>60</td>
<td>300</td>
<td>984</td>
<td>Concrete</td>
</tr>
<tr>
<td>40</td>
<td>Arraya 2</td>
<td>Kuwait City</td>
<td>2009</td>
<td>56</td>
<td>300</td>
<td>984</td>
<td>Concrete</td>
</tr>
<tr>
<td>41</td>
<td>One Island East</td>
<td>Hong Kong</td>
<td>2008</td>
<td>69</td>
<td>298</td>
<td>979</td>
<td>Concrete</td>
</tr>
<tr>
<td>42</td>
<td>First Bank Tower</td>
<td>Toronto</td>
<td>1975</td>
<td>72</td>
<td>298</td>
<td>978</td>
<td>Steel</td>
</tr>
<tr>
<td>43</td>
<td>Shanghai Wheelock Square</td>
<td>Shanghai</td>
<td>2009</td>
<td>59</td>
<td>298</td>
<td>978</td>
<td>Concrete</td>
</tr>
<tr>
<td>44</td>
<td>Four World Trade Center</td>
<td>New York</td>
<td>2012</td>
<td>64</td>
<td>297</td>
<td>975</td>
<td>Composite</td>
</tr>
<tr>
<td>45</td>
<td>Comcast Center</td>
<td>Philadelphia</td>
<td>2008</td>
<td>57</td>
<td>297</td>
<td>974</td>
<td>Composite</td>
</tr>
<tr>
<td>46</td>
<td>Central Park Office Tower</td>
<td>Dubai</td>
<td>1993</td>
<td>49</td>
<td>294</td>
<td>964</td>
<td>Concrete</td>
</tr>
<tr>
<td>47</td>
<td>311 South Wacker Drive</td>
<td>Chicago</td>
<td>1990</td>
<td>66</td>
<td>293</td>
<td>961</td>
<td>Concrete</td>
</tr>
</tbody>
</table>
Footnotes:
1. Height is measured from sidewalk level of the main entrance to the architectural top of the building, including spires, but not including antennae, signage, or flag poles.
2. A completed building can be considered such if it fulfills all three of the following criteria: a) topped out structurally and architecturally, b) fully-clad, and c) open for business, or at least partially occupied.
3. A tall building is “topped out” when all its structural members are in place.
4. A tall building is considered to be “under construction” when site clearing and excavation have been completed and foundation / piling work has begun.
5. A tall building is considered to be “on hold” when it is widely reported within the public domain that construction has halted.

# Note: Federation Towers consists of a complex of two towers plus a separate, spire-topped lift core connected to both towers. Vostok Tower is 365 meters/1198 feet high, Zapad Tower is 242 meters/795 feet high, and the external lift core spire is 509 meters/1670 feet high.

Material: A steel tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from steel.
A concrete tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from concrete.
A composite tall building utilizes a combination of both steel and concrete in the main structural elements throughout the building.
A concrete/steel tall building indicates a steel structural system located above a concrete structural system, with the opposite true of a steel/concrete building.

Use: A single-function tall building is defined as one where 85% or more of its total floor area is dedicated to a single usage. A mixed-use tall building contains two or more functions, where each of the functions occupy at least 15% of the tower’s total floor area. Ancillary / support areas such as car parks and mechanical plant space do not constitute mixed-use functions. Functions are denoted on CTBUH “Tallest” lists in ascending order.

For a more complete overview of the CTBUH’s height criteria, see http://www.ctbuh.org/criteria.htm

© Council on Tall Buildings and Urban Habitat
Tallest Single-Function Hotel Buildings in the World

This list includes buildings that are under construction. Only buildings that are completed are officially ranked on CTBUH listings.

Key:
- Building is completed and officially ranked by the CTBUH
- Building is under construction and topped out architecturally
- Building is under construction, but not topped out architecturally
- Building is under construction, but currently on hold

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mekkah Royal Clock Tower Hotel</td>
<td>Mekkah</td>
<td>2010</td>
<td>76</td>
<td>577</td>
<td>1893</td>
<td>Concrete</td>
</tr>
<tr>
<td>2</td>
<td>Rose Rotana Tower</td>
<td>Dubai</td>
<td>2007</td>
<td>72</td>
<td>333</td>
<td>1093</td>
<td>Composite</td>
</tr>
<tr>
<td>3</td>
<td>Shimao International Plaza</td>
<td>Shanghai</td>
<td>2006</td>
<td>60</td>
<td>333</td>
<td>1093</td>
<td>Concrete</td>
</tr>
<tr>
<td>4</td>
<td>Burj al Arab Hotel</td>
<td>Dubai</td>
<td>1999</td>
<td>60</td>
<td>321</td>
<td>1053</td>
<td>Composite</td>
</tr>
<tr>
<td>5</td>
<td>Emirates Tower Two</td>
<td>Dubai</td>
<td>2000</td>
<td>56</td>
<td>309</td>
<td>1014</td>
<td>Concrete</td>
</tr>
<tr>
<td>6</td>
<td>The Address Downtown Burj Dubai</td>
<td>Dubai</td>
<td>2008</td>
<td>63</td>
<td>306</td>
<td>1004</td>
<td>Concrete</td>
</tr>
<tr>
<td>7</td>
<td>Raffles City Downtown Hotel</td>
<td>Bangkok</td>
<td>1997</td>
<td>85</td>
<td>304</td>
<td>997</td>
<td>Concrete</td>
</tr>
<tr>
<td>8</td>
<td>Grand Lisboa</td>
<td>Macau</td>
<td>2008</td>
<td>52</td>
<td>258</td>
<td>847</td>
<td>Concrete</td>
</tr>
<tr>
<td>9</td>
<td>Central Market Hotel Tower</td>
<td>Abu Dhabi</td>
<td>2010</td>
<td>58</td>
<td>254</td>
<td>833</td>
<td>Concrete</td>
</tr>
<tr>
<td>10</td>
<td>Hotel JAL Tower</td>
<td>Tokyo</td>
<td>2009</td>
<td>60</td>
<td>270</td>
<td>886</td>
<td>Concrete</td>
</tr>
<tr>
<td>11</td>
<td>Grand Hyatt Hotel</td>
<td>Seoul</td>
<td>2008</td>
<td>57</td>
<td>235</td>
<td>711</td>
<td>Concrete</td>
</tr>
<tr>
<td>12</td>
<td>Grand Lisboa</td>
<td>Macau</td>
<td>2008</td>
<td>52</td>
<td>258</td>
<td>847</td>
<td>Concrete</td>
</tr>
<tr>
<td>13</td>
<td>Central Market Hotel Tower</td>
<td>Abu Dhabi</td>
<td>2010</td>
<td>58</td>
<td>254</td>
<td>833</td>
<td>Concrete</td>
</tr>
<tr>
<td>14</td>
<td>New Century Grand Hotel</td>
<td>Hangzhou</td>
<td>2005</td>
<td>45</td>
<td>218</td>
<td>715</td>
<td>Concrete</td>
</tr>
<tr>
<td>15</td>
<td>Grand Hyatt Hotel</td>
<td>Islamabad</td>
<td>2010</td>
<td>45</td>
<td>217</td>
<td>712</td>
<td>Concrete</td>
</tr>
<tr>
<td>16</td>
<td>Grand Hyatt Hotel</td>
<td>Islamabad</td>
<td>2010</td>
<td>45</td>
<td>217</td>
<td>712</td>
<td>Concrete</td>
</tr>
<tr>
<td>17</td>
<td>Grand Hyatt Hotel</td>
<td>Islamabad</td>
<td>2010</td>
<td>45</td>
<td>217</td>
<td>712</td>
<td>Concrete</td>
</tr>
<tr>
<td>18</td>
<td>Grand Hyatt Hotel</td>
<td>Islamabad</td>
<td>2010</td>
<td>45</td>
<td>217</td>
<td>712</td>
<td>Concrete</td>
</tr>
<tr>
<td>19</td>
<td>Four Seasons Hotel</td>
<td>New York</td>
<td>1993</td>
<td>52</td>
<td>208</td>
<td>682</td>
<td>Concrete</td>
</tr>
<tr>
<td>20</td>
<td>Tamani Hotel Marina</td>
<td>Dubai</td>
<td>2006</td>
<td>54</td>
<td>207</td>
<td>679</td>
<td>Concrete</td>
</tr>
<tr>
<td>21</td>
<td>Sofitel Jia Jang Oriental Pudong Hotel</td>
<td>Shanghai</td>
<td>2002</td>
<td>46</td>
<td>207</td>
<td>679</td>
<td>Concrete</td>
</tr>
<tr>
<td>22</td>
<td>Four Seasons Place, Central Station</td>
<td>Hong Kong</td>
<td>2005</td>
<td>55</td>
<td>205</td>
<td>673</td>
<td>Concrete</td>
</tr>
<tr>
<td>23</td>
<td>Marriott Bianjing Tianjin</td>
<td>Tianjin</td>
<td>2002</td>
<td>48</td>
<td>203</td>
<td>666</td>
<td>Concrete</td>
</tr>
<tr>
<td>24</td>
<td>Berjaya Times Square Tower A</td>
<td>Kuala Lumpur</td>
<td>2003</td>
<td>48</td>
<td>203</td>
<td>666</td>
<td>Concrete</td>
</tr>
<tr>
<td>25</td>
<td>Yuanyang Bldg.</td>
<td>Dalian</td>
<td>2000</td>
<td>51</td>
<td>201</td>
<td>659</td>
<td>Concrete</td>
</tr>
<tr>
<td>26</td>
<td>Radisson Hotel Shanghai New World</td>
<td>Shanghai</td>
<td>2003</td>
<td>46</td>
<td>200</td>
<td>656</td>
<td>Concrete</td>
</tr>
<tr>
<td>27</td>
<td>Dolton Hotel</td>
<td>Changsha</td>
<td>1998</td>
<td>51</td>
<td>200</td>
<td>655</td>
<td>Concrete</td>
</tr>
<tr>
<td>28</td>
<td>The Ocean Resort</td>
<td>Yeosu</td>
<td>2011</td>
<td>43</td>
<td>199</td>
<td>653</td>
<td>Concrete</td>
</tr>
<tr>
<td>29</td>
<td>Ukraine Hotel</td>
<td>Moscow</td>
<td>1955</td>
<td>34</td>
<td>196</td>
<td>650</td>
<td>Steel</td>
</tr>
<tr>
<td>30</td>
<td>Century Emperor Hotel</td>
<td>Changqing</td>
<td>1999</td>
<td>34</td>
<td>196</td>
<td>644</td>
<td>Concrete</td>
</tr>
<tr>
<td>31</td>
<td>The Palazzo</td>
<td>Las Vegas</td>
<td>2007</td>
<td>53</td>
<td>196</td>
<td>642</td>
<td>Composite</td>
</tr>
<tr>
<td>32</td>
<td>Encore</td>
<td>Las Vegas</td>
<td>2008</td>
<td>52</td>
<td>192</td>
<td>631</td>
<td>Concrete</td>
</tr>
<tr>
<td>33</td>
<td>Dubai Mall Hotel</td>
<td>Dubai</td>
<td>2009</td>
<td>37</td>
<td>192</td>
<td>629</td>
<td>Concrete</td>
</tr>
<tr>
<td>34</td>
<td>Hotel Sofitel Silver Plaza</td>
<td>Jinan</td>
<td>1999</td>
<td>56</td>
<td>186</td>
<td>610</td>
<td>Concrete</td>
</tr>
<tr>
<td>35</td>
<td>Gran Hotel Bali</td>
<td>Benidorm</td>
<td>2002</td>
<td>52</td>
<td>186</td>
<td>610</td>
<td>Concrete</td>
</tr>
</tbody>
</table>
Footnotes:
1. Height is measured from sidewalk level of the main entrance to the architectural top of the building, including spires, but not including antennae, signage, or flag poles.
2. A completed building can be considered such if it fulfills all three of the following criteria: a) topped out structurally and architecturally, b) fully-clad, and c) open for business, or at least partially occupied.
3. A tall building is “topped out” when all its structural members are in place.
4. A tall building is considered to be “under construction” when site clearing and excavation have been completed and foundation / piling work has begun.
5. A tall building is considered to be “on hold” when it is widely reported within the public domain that construction has halted.

* Construction halted on the Ryugyong Hotel in 1992 and the project remained on hold until 2008, when construction on the tower resumed.

Material: A steel tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from steel.
A concrete tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from concrete.
A composite tall building utilizes a combination of both steel and concrete in the main structural elements throughout the building.
A concrete/steel tall building indicates a steel structural system located above a concrete structural system, with the opposite true of a steel/concrete building.

Use: A single-function tall building is defined as one where 85% or more of its total floor area is dedicated to a single usage. A mixed-use tall building contains two or more functions, where each of the functions occupy at least 15% of the tower’s total floor area. Ancillary / support areas such as car parks and mechanical plant space do not constitute mixed-use functions. Functions are denoted on CTBUH “Tallest” lists in ascending order.

For a more complete overview of the CTBUH’s height criteria, see [http://www.ctbuh.org/criteria.htm](http://www.ctbuh.org/criteria.htm)

© Council on Tall Buildings and Urban Habitat
# Tallest Single-Function Residential Buildings in the World

This list includes buildings that are under construction. Only buildings that are completed are officially ranked on CTBUH listings.

**Key:**  
- Building is completed and officially ranked by the CTBUH  
- Building is under construction and topped out architecturally  
- Building is under construction, but not topped out architecturally  
- Building is under construction, but currently on hold

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pentominium</td>
<td>Dubai</td>
<td>2012</td>
<td>122</td>
<td>618</td>
<td>2028</td>
<td>Concrete/Steel</td>
</tr>
<tr>
<td></td>
<td>Chicago Spire</td>
<td>Chicago</td>
<td>2013</td>
<td>150</td>
<td>610</td>
<td>2000</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Princess Tower</td>
<td>Dubai</td>
<td>2009</td>
<td>101</td>
<td>414</td>
<td>1358</td>
<td>Concrete</td>
</tr>
<tr>
<td>3</td>
<td>23 Marina</td>
<td>Dubai</td>
<td>2009</td>
<td>90</td>
<td>389</td>
<td>1276</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>The Domian</td>
<td>Abu Dhabi</td>
<td>2010</td>
<td>88</td>
<td>382</td>
<td>1253</td>
<td>Concrete</td>
</tr>
<tr>
<td>4</td>
<td>Elite Residence</td>
<td>Dubai</td>
<td>2010</td>
<td>87</td>
<td>380</td>
<td>1247</td>
<td>Concrete</td>
</tr>
<tr>
<td>5</td>
<td>Lam Tara Tower 1</td>
<td>Dubai</td>
<td>2010</td>
<td>70</td>
<td>360</td>
<td>1181</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>G1 Tower</td>
<td>Dubai</td>
<td>2010</td>
<td>60</td>
<td>300</td>
<td>1148</td>
<td>Concrete</td>
</tr>
<tr>
<td>6</td>
<td>The Torch</td>
<td>Dubai</td>
<td>2009</td>
<td>80</td>
<td>345</td>
<td>1132</td>
<td>Concrete</td>
</tr>
<tr>
<td>7</td>
<td>Torre Planetarium I</td>
<td>Panama City</td>
<td>2011</td>
<td>92</td>
<td>343</td>
<td>1126</td>
<td>Concrete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Q1 Gold Coast</td>
<td>Dubai</td>
<td>2009</td>
<td>76</td>
<td>342</td>
<td>1122</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>The Landmark</td>
<td>Abu Dhabi</td>
<td>2009</td>
<td>72</td>
<td>324</td>
<td>1063</td>
<td>Concrete</td>
</tr>
<tr>
<td>2</td>
<td>HHIHR Tower</td>
<td>Dubai</td>
<td>2009</td>
<td>62</td>
<td>317</td>
<td>1040</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Ocean Heights</td>
<td>Dubai</td>
<td>2009</td>
<td>82</td>
<td>310</td>
<td>1017</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Lamar Tower 1</td>
<td>Jeddah</td>
<td>2010</td>
<td>65</td>
<td>310</td>
<td>1017</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Infinity Tower</td>
<td>Dubai</td>
<td>2011</td>
<td>73</td>
<td>307</td>
<td>1007</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>East Pacific Center Tower A</td>
<td>Shenzhen</td>
<td>UC</td>
<td>85</td>
<td>306</td>
<td>1004</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Torre Planetarium II</td>
<td>Panama City</td>
<td>2011</td>
<td>82</td>
<td>305</td>
<td>1001</td>
<td>Concrete</td>
</tr>
<tr>
<td>3</td>
<td>Gramercy Residences</td>
<td>Makati</td>
<td>2012</td>
<td>68</td>
<td>302</td>
<td>992</td>
<td>Concrete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 Eureka Tower</td>
<td>Melbourne</td>
<td>2006</td>
<td>91</td>
<td>297</td>
<td>975</td>
<td>Concrete</td>
</tr>
<tr>
<td>3</td>
<td>Emirates Crown</td>
<td>Dubai</td>
<td>2008</td>
<td>63</td>
<td>296</td>
<td>971</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Century Star Plaza R1</td>
<td>Chongqing</td>
<td>2009</td>
<td>68</td>
<td>286</td>
<td>938</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Sulafa Tower</td>
<td>Dubai</td>
<td>2010</td>
<td>75</td>
<td>285</td>
<td>935</td>
<td>Concrete</td>
</tr>
<tr>
<td>4</td>
<td>Millennium Tower</td>
<td>Dubai</td>
<td>2006</td>
<td>59</td>
<td>285</td>
<td>935</td>
<td>Concrete</td>
</tr>
<tr>
<td>5</td>
<td>G-Tower</td>
<td>Dubai</td>
<td>2010</td>
<td>54</td>
<td>284</td>
<td>932</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Torre Vitri</td>
<td>Panama City</td>
<td>2010</td>
<td>75</td>
<td>281</td>
<td>921</td>
<td>Concrete</td>
</tr>
<tr>
<td>6</td>
<td>MAG 218 Tower</td>
<td>Dubai</td>
<td>2009</td>
<td>66</td>
<td>275</td>
<td>902</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>The Point</td>
<td>Panama City</td>
<td>2009</td>
<td>65</td>
<td>275</td>
<td>902</td>
<td>Concrete</td>
</tr>
<tr>
<td>7</td>
<td>Faros de Panama Torre 2</td>
<td>Panama City</td>
<td>2009</td>
<td>73</td>
<td>270</td>
<td>886</td>
<td>Concrete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1 Eureka Tower</td>
<td>Melbourne</td>
<td>2006</td>
<td>91</td>
<td>297</td>
<td>975</td>
<td>Concrete</td>
</tr>
<tr>
<td>5</td>
<td>The Cullinan I</td>
<td>Hong Kong</td>
<td>2008</td>
<td>68</td>
<td>270</td>
<td>886</td>
<td>Concrete</td>
</tr>
<tr>
<td>6</td>
<td>21st Century Tower</td>
<td>Dubai</td>
<td>2003</td>
<td>55</td>
<td>269</td>
<td>883</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>The Belkman</td>
<td>New York</td>
<td>2010</td>
<td>76</td>
<td>267</td>
<td>876</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>The River Tower A</td>
<td>Bangkok</td>
<td>2010</td>
<td>73</td>
<td>266</td>
<td>872</td>
<td>Concrete</td>
</tr>
<tr>
<td>7</td>
<td>Al Kazim Tower 1</td>
<td>Dubai</td>
<td>2008</td>
<td>53</td>
<td>265</td>
<td>869</td>
<td>Concrete</td>
</tr>
<tr>
<td>8</td>
<td>Al Kazim Tower 2</td>
<td>Dubai</td>
<td>2008</td>
<td>53</td>
<td>265</td>
<td>869</td>
<td>Concrete</td>
</tr>
<tr>
<td>9</td>
<td>Arts Tower</td>
<td>Panama City</td>
<td>2010</td>
<td>80</td>
<td>264</td>
<td>866</td>
<td>Concrete</td>
</tr>
<tr>
<td>10</td>
<td>Triumph Palace</td>
<td>Moscow</td>
<td>2005</td>
<td>61</td>
<td>264</td>
<td>866</td>
<td>Concrete</td>
</tr>
<tr>
<td>11</td>
<td>Tower Palace Three, Tower G</td>
<td>Seoul</td>
<td>2004</td>
<td>73</td>
<td>264</td>
<td>865</td>
<td>Concrete</td>
</tr>
<tr>
<td>12</td>
<td>Trump World Tower</td>
<td>New York</td>
<td>2001</td>
<td>72</td>
<td>262</td>
<td>861</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Central Park Residential Tower</td>
<td>Dubai</td>
<td>UC</td>
<td>51</td>
<td>261</td>
<td>857</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>East Pacific Center Tower B</td>
<td>Shenzhen</td>
<td>UC</td>
<td>72</td>
<td>261</td>
<td>856</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Sapphire Tower</td>
<td>Istanbul</td>
<td>2008</td>
<td>54</td>
<td>261</td>
<td>856</td>
<td>Concrete</td>
</tr>
<tr>
<td></td>
<td>Marina Pinnacle</td>
<td>Dubai</td>
<td>2009</td>
<td>67</td>
<td>260</td>
<td>853</td>
<td>Concrete</td>
</tr>
<tr>
<td>12</td>
<td>Four Seasons Centre Condo Tower</td>
<td>Kuala Lumpur</td>
<td>UC</td>
<td>67</td>
<td>260</td>
<td>853</td>
<td>Concrete</td>
</tr>
<tr>
<td>13</td>
<td>Sorrento 1</td>
<td>Hong Kong</td>
<td>2003</td>
<td>75</td>
<td>256</td>
<td>841</td>
<td>Concrete</td>
</tr>
<tr>
<td>14</td>
<td>Mokdong Hyperion Tower A</td>
<td>Seoul</td>
<td>2003</td>
<td>69</td>
<td>256</td>
<td>840</td>
<td>Concrete</td>
</tr>
</tbody>
</table>

---

*The World's Tallest Buildings* 625

---

safetymessage.com
Footnotes:
1. Height is measured from sidewalk level of the main entrance to the architectural top of the building, including spires, but not including antennae, signage, or flag poles.
2. A completed building can be considered such if it fulfills all three of the following criteria: a) topped out structurally and architecturally, b) fully clad, and c) open for business, or at least partially occupied.
3. A tall building is "topped out" when all its structural members are in place.
4. A tall building is considered to be "under construction" when site clearing and excavation have been completed and foundation / piling work has begun.
5. A tall building is considered to be "on hold" when it is widely reported within the public domain that construction has halted.

Material: A steel tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from steel.
A concrete tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from concrete.
A composite tall building utilizes a combination of both steel and concrete in the main structural elements throughout the building.
A concrete/steel tall building indicates a steel structural system located above a concrete structural system, with the opposite true of a steel/concrete building.

Use: A single-function tall building is defined as one where 85% or more of its total floor area is dedicated to a single usage. A mixed-use tall building contains two or more functions, where each of the functions occupy at least 15% of the tower’s total floor area. Ancillary / support areas such as car parks and mechanical plant space do not constitute mixed-use functions. Functions are denoted on CTBUH “Tallest” lists in ascending order.

For a more complete overview of the CTBUH's height criteria, see http://www.ctbuh.org/criteria.htm

© Council on Tall Buildings and Urban Habitat
### Tallest Mixed-Use Buildings in the World

This list includes buildings that are under construction. Only buildings that are completed are officially ranked on CTBUH listings.

**Key:**
- Building is completed and officially ranked by the CTBUH
- Building is under construction and topped out architecturally
- Building is under construction, but currently on hold

**Last updated:** January, 2009

<table>
<thead>
<tr>
<th>Rank</th>
<th>Building Name</th>
<th>City</th>
<th>Year</th>
<th>Stories</th>
<th>m</th>
<th>f</th>
<th>Material</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shanghai World Financial Center</td>
<td>Shanghai</td>
<td>2008</td>
<td>101</td>
<td>492</td>
<td>1614</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>2</td>
<td>International Commerce Centre</td>
<td>Hong Kong</td>
<td>2010</td>
<td>106</td>
<td>484</td>
<td>1588</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>3</td>
<td>Nanjing Greenland Financial Center</td>
<td>Nanjing</td>
<td>2009</td>
<td>69</td>
<td>450</td>
<td>1476</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>4</td>
<td>Kingkey Finance Tower</td>
<td>Shenzhen</td>
<td>2011</td>
<td>97</td>
<td>439</td>
<td>1440</td>
<td>Office/Hotel</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>West Tower</td>
<td>Guangzhou</td>
<td>2009</td>
<td>103</td>
<td>438</td>
<td>1435</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>6</td>
<td>Dubai Towers Ooha</td>
<td>Ooha</td>
<td>2010</td>
<td>84</td>
<td>437</td>
<td>1434</td>
<td>Concrete/Steel</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>7</td>
<td>Jin Mao Building</td>
<td>Shanghai</td>
<td>1999</td>
<td>88</td>
<td>421</td>
<td>1381</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>8</td>
<td>Trump International Hotel &amp; Tower</td>
<td>Chicago</td>
<td>2009</td>
<td>96</td>
<td>415</td>
<td>1362</td>
<td>Concrete</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>9</td>
<td>Marina 101</td>
<td>Dubai</td>
<td>2010</td>
<td>101</td>
<td>412</td>
<td>1352</td>
<td>Concrete/Steel</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>10</td>
<td>Emirates Park Towers Hotel &amp; Spa 1</td>
<td>Dubai</td>
<td>2010</td>
<td>77</td>
<td>395</td>
<td>1296</td>
<td>Concrete/Steel</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>11</td>
<td>Emirates Park Towers Hotel &amp; Spa 2</td>
<td>Dubai</td>
<td>2010</td>
<td>77</td>
<td>395</td>
<td>1296</td>
<td>Concrete/Steel</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>12</td>
<td>Etion Place Dalian Tower 1</td>
<td>Dalian</td>
<td>2012</td>
<td>81</td>
<td>388</td>
<td>1274</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>13</td>
<td>Mercury City Tower</td>
<td>Moscow</td>
<td>2011</td>
<td>70</td>
<td>380</td>
<td>1247</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>14</td>
<td>Sky Tower</td>
<td>Abu Dhabi</td>
<td>2009</td>
<td>83</td>
<td>379</td>
<td>1243</td>
<td>Concrete/Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>15</td>
<td>The Square Capital Tower</td>
<td>Kuwait City</td>
<td>2010</td>
<td>63</td>
<td>351</td>
<td>1150</td>
<td>Concrete/Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>16</td>
<td>Tunxue Sky Tower</td>
<td>Kaohsiung</td>
<td>1997</td>
<td>85</td>
<td>348</td>
<td>1140</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>17</td>
<td>Faros de Panama Torre Central</td>
<td>Panama City</td>
<td>2010</td>
<td>85</td>
<td>346</td>
<td>1135</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>18</td>
<td>John Hancock Center</td>
<td>Chicago</td>
<td>1969</td>
<td>100</td>
<td>344</td>
<td>1127</td>
<td>Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>19</td>
<td>The Wharf Times Square</td>
<td>Wuxi</td>
<td>2011</td>
<td>83</td>
<td>339</td>
<td>1112</td>
<td>Concrete/Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>20</td>
<td>Hanoi Gyuongnam Landmark Tower</td>
<td>Hanoi</td>
<td>2011</td>
<td>70</td>
<td>336</td>
<td>1103</td>
<td>Composite</td>
<td>Office/Residential/Hotel</td>
</tr>
<tr>
<td>21</td>
<td>Wenzhou Trade Center</td>
<td>Wenzhou</td>
<td>2009</td>
<td>72</td>
<td>333</td>
<td>1094</td>
<td>Concrete/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>22</td>
<td>Century Star Plaza R6</td>
<td>Chongqing</td>
<td>2009</td>
<td>79</td>
<td>331</td>
<td>1085</td>
<td>Concrete/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>23</td>
<td>China World Trade Center Tower III</td>
<td>Beijing</td>
<td>2009</td>
<td>74</td>
<td>330</td>
<td>1083</td>
<td>Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>24</td>
<td>Hang Lung Plaza Tower 1</td>
<td>Shenyang</td>
<td>2013</td>
<td>70</td>
<td>330</td>
<td>1083</td>
<td>Concrete/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>25</td>
<td>The Index</td>
<td>Dubai</td>
<td>2009</td>
<td>80</td>
<td>328</td>
<td>1076</td>
<td>Concrete/Steel</td>
<td>Office/Residential</td>
</tr>
<tr>
<td>26</td>
<td>Al Yaqoub Tower</td>
<td>Dubai</td>
<td>2009</td>
<td>69</td>
<td>328</td>
<td>1076</td>
<td>Concrete/Steel</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>27</td>
<td>Yantai Shimao No.1 The Harbour</td>
<td>Yantai</td>
<td>2010</td>
<td>57</td>
<td>323</td>
<td>1060</td>
<td>Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>28</td>
<td>Hang Lung Plaza Tower 2</td>
<td>Shenyang</td>
<td>2013</td>
<td>70</td>
<td>320</td>
<td>1050</td>
<td>Concrete/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>29</td>
<td>Nina Tower I</td>
<td>Hong Kong</td>
<td>2006</td>
<td>80</td>
<td>319</td>
<td>1046</td>
<td>Concrete/Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>30</td>
<td>NE Asia Trade Tower</td>
<td>Incheon</td>
<td>2010</td>
<td>70</td>
<td>305</td>
<td>1021</td>
<td>Concrete/Steel</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>31</td>
<td>Eurasia</td>
<td>Moscow</td>
<td>2010</td>
<td>67</td>
<td>304</td>
<td>998</td>
<td>Composite</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>32</td>
<td>Kingdom Centre</td>
<td>Riyadh</td>
<td>2002</td>
<td>41</td>
<td>302</td>
<td>992</td>
<td>Concrete/Steel</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>33</td>
<td>Gate of the Orient</td>
<td>Suzhou</td>
<td>2009</td>
<td>68</td>
<td>302</td>
<td>990</td>
<td>Concrete/Steel</td>
<td>Office/Hotel/Residential</td>
</tr>
<tr>
<td>34</td>
<td>India Tower</td>
<td>Mumbai</td>
<td>2010</td>
<td>70</td>
<td>301</td>
<td>988</td>
<td>Steel</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>35</td>
<td>Tianjin International Trade Tower</td>
<td>Tianjin</td>
<td>2009</td>
<td>80</td>
<td>300</td>
<td>984</td>
<td>Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>36</td>
<td>Aspire Tower</td>
<td>Doha</td>
<td>2006</td>
<td>36</td>
<td>300</td>
<td>984</td>
<td>Composite</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>37</td>
<td>Landmark Tower</td>
<td>Yokohama</td>
<td>1993</td>
<td>73</td>
<td>296</td>
<td>972</td>
<td>Steel</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>38</td>
<td>Khalid Al Attar Tower 2</td>
<td>Dubai</td>
<td>2009</td>
<td>66</td>
<td>295</td>
<td>966</td>
<td>Concrete/Steel</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>39</td>
<td>Trump Ocean Club</td>
<td>Panama City</td>
<td>2009</td>
<td>68</td>
<td>293</td>
<td>961</td>
<td>Concrete/Steel</td>
<td>Hotel/Residential</td>
</tr>
<tr>
<td>40</td>
<td>SEG Plaza</td>
<td>Shenzhen</td>
<td>2000</td>
<td>71</td>
<td>292</td>
<td>957</td>
<td>Concrete</td>
<td>Office/Hotel</td>
</tr>
<tr>
<td>41</td>
<td>Chongqing Poly Tower</td>
<td>Chongqing</td>
<td>2010</td>
<td>70</td>
<td>290</td>
<td>951</td>
<td>Multiple</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Dongguan TBA Building</td>
<td>Dongguan</td>
<td>2010</td>
<td>68</td>
<td>289</td>
<td>948</td>
<td>Office/Hotel</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Park Hyatt Guangzhou</td>
<td>Guangzhou</td>
<td>2010</td>
<td>66</td>
<td>289</td>
<td>947</td>
<td>Office/Hotel/Residential</td>
<td></td>
</tr>
</tbody>
</table>
Footnotes:
1. Height is measured from sidewalk level of the main entrance to the architectural top of the building, including spires, but not including antennas, signage, or flag poles.
2. A completed building can be considered such if it fulfills all three of the following criteria: a) topped out structurally and architecturally, b) fully clad, and c) open for business, or at least partially occupied.
3. A tall building is “topped out” when all its structural members are in place.
4. A tall building is considered to be “under construction” when site clearing and excavation have been completed and foundation / piling work has begun.
5. A tall building is considered to be “on hold” when it is widely reported within the public domain that construction has halted.

Material: A steel tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from steel.
A concrete tall building is defined as one where the main vertical and lateral structural elements and floor systems are constructed from concrete.
A composite tall building utilizes a combination of both steel and concrete in the main structural elements throughout the building.
A concrete/steel tall building indicates a steel structural system located above a concrete structural system, with the opposite true of a steel/concrete building.

Use: A single-function tall building is defined as one where 85% or more of its total floor area is dedicated to a single usage. A mixed-use tall building contains two or more functions, where each of the functions occupy at least 15% of the tower’s total floor area. Ancillary / support areas such as car parks and mechanical plant space do not constitute mixed-use functions. Functions are denoted on CTBUH “Tallest” lists in ascending order.

For a more complete overview of the CTBUH’s height criteria, see http://www.ctbuh.org/criteria.htm

© Council on Tall Buildings and Urban Habitat
Acronyms

ABCB  Australian Building Codes Board
ACFE  Association of Certified Fraud Examiners
ACI  American Concrete Institute
ADA  Americans with Disabilities Act
AED  Automated external defibrillator
AIA  American Institute of Architects
AISC  American Institute of Steel Construction
AESRM  Alliance for Enterprise Security Risk Management
ANSI  American National Standards Institute
ASCE  American Society of Civil Engineers
ASHRAE  American Society of Heating, Refrigerating and Air-Conditioning Engineers
ASIS  ASIS International
ASME  American Society of Mechanical Engineers
ASTM  American Society for Testing and Materials
ATF  Bureau of Alcohol, Tobacco, Firearms, and Explosives
BOMA  Building Owners and Managers Association International
BPS  Building Performance Study
BS  British Standards
BSC  Building Security Council
BSCP  Building Security Certified Professional
CBCP  Certified Business Continuity Planner
CBD  Central Business District
CBR  Chemical, Biological, and Radiological
CCD  Charged-Couple Device
CCTV  Closed Circuit Television
CDRP  Certified Disaster Recovery Planner
CFE  Certified Fraud Examiner
CLSD  Certified Lodging Security Director
CPO  Certified Protection Officer
CPP  Certified Protection Professional
CPR  Cardiopulmonary resuscitation
CSA  Canadian Standards Association
CSI  Construction Specifications Institute
CSO  Chief Security Officer
CSS  Certified Security Supervisor
CTBUH  Council on Tall Buildings and Urban Habitat
DVR  Digital Video Recorder
ERM  Enterprise Risk Management
ESRM  Enterprise Security Risk Management
FBI  Federal Bureau of Investigation
FDNY  Fire Department of the City of New York
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Association</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation, and Air-Conditioning</td>
</tr>
<tr>
<td>IAPSC</td>
<td>International Association of Professional Security Consultants</td>
</tr>
<tr>
<td>IBC</td>
<td>International Building Code</td>
</tr>
<tr>
<td>ICC</td>
<td>International Code Council</td>
</tr>
<tr>
<td>IFMA</td>
<td>International Facility Management Association</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IREM</td>
<td>Institute of Real Estate Management</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>LCD</td>
<td>Liquid Crystal Display</td>
</tr>
<tr>
<td>LED</td>
<td>Light-Emitting Diode</td>
</tr>
<tr>
<td>NBCC</td>
<td>National Building Code of Canada</td>
</tr>
<tr>
<td>NFPA</td>
<td>National Fire Protection Association</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NRCC</td>
<td>National Research Council of Canada</td>
</tr>
<tr>
<td>OSHA</td>
<td>Occupational Safety and Health Administration</td>
</tr>
<tr>
<td>PA</td>
<td>Public Address</td>
</tr>
<tr>
<td>PAPD</td>
<td>Port Authority Police Department</td>
</tr>
<tr>
<td>PCI</td>
<td>Professional Certified Investigator</td>
</tr>
<tr>
<td>PE</td>
<td>Professional Engineer</td>
</tr>
<tr>
<td>PIR</td>
<td>Passive infrared</td>
</tr>
<tr>
<td>PSP</td>
<td>Physical Security Professional</td>
</tr>
<tr>
<td>PTZ</td>
<td>Pan, Tilt, and Zoom</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>SARS</td>
<td>Severe Acute Respiratory Syndrome</td>
</tr>
<tr>
<td>SFPE</td>
<td>Society of Fire Protection Engineers</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>VCR</td>
<td>Videocassette Recorder</td>
</tr>
<tr>
<td>VIP</td>
<td>Very Important Person</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice-over Internet Protocol</td>
</tr>
<tr>
<td>WTC</td>
<td>World Trade Center</td>
</tr>
<tr>
<td>WTC 1</td>
<td>World Trade Center 1 (North Tower)</td>
</tr>
<tr>
<td>WTC 2</td>
<td>World Trade Center 2 (South Tower)</td>
</tr>
<tr>
<td>WTC 7</td>
<td>World Trade Center 7</td>
</tr>
</tbody>
</table>
Abbreviations and Conversions

ft  feet
in.  inch
lb  pound  1 lb = 0.453 kg
m  meter  1 m = 3.28 ft
min  minute
psi  pounds per square inch

Metric conversion from pounds to kilograms
www.metric-conversions.org/weight/pounds-to-kilograms.htm

Metric conversions from inches to meters (metres)
www.metric-conversions.org/length/inches-to-meters.htm

Metric conversions from inches to centimeters (centimetres)
www.metric-conversions.org/length/inches-to-centimeters.htm

Metric conversions from yards to meters (metres)
www.metric-conversions.org/length/yards-to-meters.htm

Metric conversions from miles to kilometers (kilometres)
www.metric-conversions.org/cgi-bin/util/convert.cgi

Metric conversions from square feet to square meters (metres)
www.metric-conversions.org/area/square-feet-to-square-meters.htm
This page intentionally left blank
A
Aberrant behavior, 61, 176
Access card, 291, 344, 524
Access control, see Apartment building; Hotel;
Mixed-use building; Office Building;
Residential building
Accounts payable, 442
Acquired immunodeficiency syndrome (AIDS), 169
Active vehicle barrier, 344
Acoustic detector, intrusion detection system, 312
Addressable device, 364, 412
Adequate security, 611
AED, see Automated external defibrillator
Aftershock, 152
AHJ, see Authority having jurisdiction
AIDS, see Acquired immunodeficiency syndrome
Air-conditioning, see Heating, ventilation, and air-conditioning
Aircraft collisions
Bank of America Building, Tampa, 67
Empire State Building, 67–68
Pirelli Tower, 68–69
World Trade Center towers, see World Trade Center
Alexander Hamilton Hotel, fire, 515
Algorithm, 298, 344
Al-Khobar bombing, 109
ALL CALL, public address system, 355
All hazards, 231
All risk policy, 194
American National Standards Institute (ANSI), 602
American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE), 386–387
Annealed glass, 253
Annunciator
fire detection and alarm system, 356–358
intrusion detection system, 313
ANSI, see American National Standards Institute
Anthrax mailings, 147
Anti-passback, 298, 344
Anti-tailgating, doors, 247
Apartment, 22, 580, 591
Apartment building, see also Residential building
definition, 551, 580, 591
evacuation drills, 579
exit signs, 578–579
occupant documentation, 577–578
occupant training, 578
plan development, 575–579
occupancy characteristics, 552–553
overview, 21–23
risk assessment
assets, 553–554
countermeasures, 556–557
fire risk, 554–556
overview, 553
threats, 554–556
vulnerabilities, 556
security programs
access control
locks, 564
overview, 558
parking, 558–559
pedestrians, 559–563
solicitors, 563–564
visitor systems, 562–563
escorts, 564–565
property control
construction and remodeling, 567
couriers, 566–567
key control, 568–570
lost and found property, 567–568

633
safetymessage.com
Apartment building (Continued)
objectives, 565–566
patrols, 570–572
trash removal control, 568
resident security education, 572–573
security staff levels, 425
Area of refuge, 497
Area of rescue assistance, 497
Arrest, 612
Arson, 62, 176
As-built drawings, 231
Asch Building, fire, 126–128
ASHRAE, see American Society of Heating, Refrigerating, and Air Conditioning Engineers
ASIS International, 598, 610
Assault, 61–62, 177
Assault and battery, 62, 177
Assemblies, 18, 23
Assembly occupancy, 547
Asset
definition, 177, 185, 231
identification in security survey, 196
risk assessment
hotels, 508
mixed-use buildings, 584–585
office buildings, 463
residential and apartment buildings, 553–554
Asset criticality, 231
Asset management, 308
Asset tracking, 308–309
Asset value
assessment in terrorist attack mitigation, 207–210
definition, 231
Asymmetric threat, 177
Atrium, 257, 344, 547–548
Audit, investigations, 450
Authority having jurisdiction (AHJ), 229, 231, 604, 612
Automated external defibrillator (AED)
overview, 410–411
placement, 411–412
residential and apartment buildings, 576
Automatic sprinkler
definition, 366, 412
fire department connections, 368–370
fire pump, 368–369
historical perspective, 366
mechanisms, 364–375
pipes, 370
sprinkler types
extended coverage sidewall sprinkler, 373–374
quick-response sprinkler, 371–372
residential sprinkler, 372
sidewall sprinkler, 372–373
standard spray sprinkler, 370–371
supervision and manual operation, 376–377
system types
dry-pipe system, 375
preaction system, 375–376
wet-pipe system, 375
water supply
gravity tank, 367
pressure tank, 368
suction tank, 368
B
Balcony, 257
Bali nightclub, bombing, 106–107
Bank of America Building, aircraft collision in Tampa, 67
Barium ferrite card, 293
Barrier, 237, 344
BASE jumping, 117
Bathroom, 551, 580, 591
Beam, 16, 23
Bellhop, 521, 548
Benchmarking, 231
Berm, 237, 344
Berman, Bennet H., 429
Bessemer process, steel production, 5
bin Laden, Osama, 69, 106, 108
Biological weapons, 146–147
Biometric identification system-operated locks, 299–300
Bishopsgate financial area, bombing, 102, 465
Blackout, 169
Blair, Tony, 108
Blast curtain, 256, 344
Bollard, 240–241, 345
Bolt, locks, 270–271
Bomb, see also Explosives; Incendiary devices
stand-off distance, 239
suicide bombers, 96–97
table of incidents, 98
types, 96
vehicle-borne improvised explosive devices, 97–115
Bomb threat, 115–116
Booster pump, 368, 415
BPAT, see Building performance assessment team
Brannigan, Francis L., 44, 51
Break wire, intrusion detection system, 311
Broadway Central Hotel, 8
Brownout, 169
BSC, see Building Security Council
BSCP, see Building Security Certified Professional
Budget, 442
Building, 1, 23
Building codes, 602–603
Building core, risk assessment in terrorist attack mitigation functions, 208
infrastructure, 208–209
Building envelope
atrium, 257
balconies, 257
definition, 244, 345
doors, 246–249, 258–262
fire escapes, 245–246
floors and ceilings, 257–258
openings, 252
vehicle openings, 249–251
walls and roof, 245
windows, 252–257
Building hardening, 231
Building offset, 56, 231
Building performance assessment team (BPAT), 76
Building Security Certified Professional (BSCP), 227–228
Building Security Council (BSC), see Promoting Logical Unified Security
Building telephone entry system, 300–301
Bullet-resistant glass, 255
Bullhorn, 320
Burglar-resistant glass, 255
Burglary, 62, 177
Burj Dubai, 12, 14–15, 314
Business continuity planning, 494, 497, 541, 574
Business occupancy, 506, 548
C
Cameras, see Closed-circuit television
Campus, 231, 591
Cantilevered beam, 20, 23
CAP Index, see Crimes Against Persons and Property Index
Capacitance detector, intrusion detection system, 311
Carbon dioxide extinguishing systems applications, 381
overview, 380
Carbon dioxide fire extinguishers, 401–402
Card readers applications, 298
types, 293–298
CBD, see Central business district
CCD, see Charge-coupled device
CCTV, see Closed-circuit television
Ceiling, suspended, 257–258
Central business district (CBD), 28, 56
Central station, 345
Certificate of occupancy, 32, 56, 612
Chain of command, 442
Charge-coupled device (CCD), 323–324, 345
Chemical weapons, 146–147
Chicane, 177
Chrysler Building, 12
Citigroup Center, hostage situation, 150, 465
Civil disorder, 151, 177
Closed-circuit television (CCTV) applications
buildings, 336–337
overview, 321–322, 335
parking lots and garages, 337–339
asset tracking, 308
cameras
analog versus digital cameras, 323–324
dummy cameras, 327
lens types, 322–323
mounting and housing, 324–325
pan, tilt, and zoom, 325–327
definition, 345
illumination, 322
monitors, see Video monitor
network transmission, 327–328
office buildings, 477, 482
prospects, 335
signal transmission, 321, 327
speaker and microphone incorporation, 320
switchers, see Video switcher
video analytics, 331–332
safetymessage.com
Closed-circuit television (CCTV) (Continued)
video recording and storage, 334–335
workplace violence prevention, 174
World Trade Center bombing response, 102
CMOS camera, see Complementary metal
oxide semiconductor camera
Coaxial cable, 321, 345
Code
building codes, 602–603
definition, 601, 612
enforcement, 604
fire prevention codes, 603
Code of ethics, security, 428
Column, 16, 23
Combination locks
features, 288–290
limitations, 290
Command center, see also Fire command
center; Security command center
definition, 349
equipment, 235–236, 292, 313, 317–320
fire command center, 144, 333, 355, 357,
375, 380, 385, 387, 584
organization, 342
World Trade Center, 36–37, 53, 67, 102
Command center operator, 425, 443
Communication systems, 317–321
Compartmentation, 18, 23, 385
Complementary metal oxide semiconductor
(CMOS) camera, 324
Composite floor, 23
Concealed space, see Interstitial space
Concierge, 443, 548, 580
Concierge floor, 522, 548
Concrete barrier, 240
Condominium, 23, 580, 592
Conduction, 121–122
Confidence trick, 510
Console operator, 425, 443
Consultants, see Risk assessment
Contract security service
costs, 423–424
definition, 443
successful program prerequisites, 422
through selection process importance, 424
vital issues, 422–423
Control unit, intrusion detection system,
312–313
Convection, 121–122
Cook County Administration Building, fire,
139–141
Copenhagen Hotel, fire, 515
Council on Tall Buildings and Urban Habitat
(CTBUH), 12
Countermeasure, 185, 231
Courier, 483–484, 497, 531, 566–567
Courtesy notice, 430
CPTED, see Crime prevention through
environmental design
Credential, 291, 345, 470, 497
Credential-operated locks, 291–299
Crime, 29, 56, 177
Crime analysis, 56
CRIMECAST, 192
Crime pattern analysis, 29, 56
Crime prevention through environmental
design (CPTED)
derinition, 178, 232
hotels, 518
mixed-use buildings, 587
office buildings, 466
principles, 196–197
residential and apartment buildings, 556
workplace violence prevention, 175
Crimes Against Persons and Property (CAP)
Index, 192
Criminal liability, 610
Crisis, 494, 497, 539, 574
Crisis management, see Emergency
management
Critical asset, 204, 208
Cross-over floor, 413, see also Sky-lobby
CTBUH, see Council on Tall Buildings and
Urban Habitat
Curb lane, layer of defense, 191
Curtain wall, 18, 23, 40
Cyberattack, 62–63, 178
Cyberterrorism, 63–64, 178
Cyclone, 165–166, 178

D
Damages, 606, 612
Daredevils, 116–117
Deadbolt, 271–272, 526
Defend-in-place, 497
Defendant, 612
Delayed evacuation, 498
Demonstration, 150–151, 178
Department of Defense (DoD), terrorism risk
mitigation, 216
Destination dispatch, 413
Digital video recorder (DVR), 333–335
Index 637

Dip tray, 345
Director of loss prevention, 443
Director of security, 425, 443
Dirty bomb, 148–149, 178
Disability, 498
Disabled assistance monitor, 498
Disaster
definition, 66, 178
exercises, 598
Discipline
definition, 443
principles, 438–440
Disease
influenza pandemic, 167–168
severe acute respiratory syndrome, 168
transmission, 166–167
tuberculosis, 168–169
Disorderly conduct, 62, 178–179
Disruption, 494, 498, 539, 573
Dockmaster, 426, 443
DoD, see Department of Defense
Dome camera, 324, 326
Door viewer, 345
Doorman, 426, 443, 548, 580
Doors, see also Locks
attack methods, 249–250, 271
interior doors
maintenance spaces, 261
restroom doors, 261
stairwell doors, 260
viewers, 259
won doors, 260–261
lobby doors, 246–248
stairwell exterior fire doors, 248–249
Dormitory, 552, 580
Double-deck elevator, 264
Drill, 56–57, 498
Dry chemical fire extinguishers, 402–403
Dry chemical system, 382–383, 413
Dry-pipe system, 375
Dumbwaiter, 262, 345
Dummcamera, 327
Dumpster, 482, 498
Dupont Plaza Hotel and Casino, fire, 132–134, 515
Duress alarm, 313, 345
Duress code, 345
DVR, see Digital video recorder

E
EAP, see Emergency action plan
Earthquake
aftershock, 152
definition, 151–152, 179
high-rise impact, 157
magnitude, 152
major incidents, 153–155
monitoring, 156
Northridge earthquake, 157–160
Edison, Thomas, 187
Egress, 42
Electrical switch, intrusion detection system, 310–311
Electric locks, 287–288
Electromagnetic hold-open devices, 290–291
Electromagnetic locks, 280–281
Electronic guard tour system, 340–341
Electronic surveillance, 450
Electro-optical amplitude modulator, 259
Elevator
configurations, 264–266
controls
car controls, 389–390
computerized controls, 394
firefighter controls, 392–393
lobby controls, 390–392
definition, 23
emergency power, 395
emergency use guidelines, 393–394
historical perspective, 4
incidents, 118–120
operator, 426
safety feature evolution, 388
standby power, 395
status panel, 387–388
types, 262–264
Elevator monitor, 498
Emergency action plan (EAP), 495, 498
Emergency call and assistance station, 408–409
Emergency specific emergencies
definition, 66, 179, 494, 498, 539, 573
security staff overwhelming, 100–101
Emergency key, hotel, 535
Emergency management, 494, 499, 539, 574
Emergency management plan
definition, 495, 499, 539, 574
development
hotels, 541–546

safetymessage.com
Emergency management plan (Continued)
office buildings, 496
residential and apartment buildings, 575–579
objectives, 540
Emergency operations center (EOC), 499
Emergency planning
hotels, 541–546
office buildings, 494–496
overview, 52–53
residential and apartment buildings, 573–579
Emergency power
elevators, 395
systems, 395–397
Emergency procedures manual, see Building
Emergency Procedures Manual
Empire State Building
aircraft collision, 67–68
elevators, 262
historical perspective, 12, 17
EOC, see Emergency operations center
Equitable Building, 8
Errors and omissions insurance, 457–458
Escalatable costs, 419, 443
Escalator
definition, 24, 266
incidents, 120–121
safety features, 266–267
Escort
hotel users, 530
office building, 478
residential and apartment buildings, 564–565
Espionage, 62, 179
Ethernet, 346
Ethics, 443
Evacuation drill, see Fire drill
Evacuation plan, illumination, 407
Evidence, 447, 458
Exit signs, 403–406, 545, 578–579
Explosives, 179
Extended coverage sidewall sprinkler, 373–374

F
Fact, 447, 458
Fail safe, 281, 346
Fail safe lock, 287, 346
Fail secure lock, 287, 346
False alarm, 346
Federal Emergency Management Association
FEMA, see Federal Emergency Management Association
Fence, barriers, 237–238
Fiber optic cable, 321, 346
Fiber optics, 327, 346
Fire alarm
definition, 143, 179
false alarms, 143–144
Fire authorities, building management liaison
overview, 596
relationship fostering
communication, 596
community service, 598
compliance, 597
crime reporting, 597
disaster exercises, 598
hospitality, 597
professional organizations, 598
public agency presentations, 598
public agency support, 597
Fireball, 72
Fire barrier, 251, 346
Fire brigade, 57
Fire command center, see also Command center
components, 354
definition, 413
Fire damper, 413
Fire drill, 54, 57, 499, 546, 579
Fire escape
building envelope, 245–246
definition, 346
Fire exit hardware, 346
Fire extinguisher, see Portable fire extinguisher
Fire hydrant, 370, 413
Fire incident data, 50, 464, 514
Fire life safety
balancing security and fire life safety, 283–287
definition, 28, 57
high-rise versus low-rise buildings, 29–31
laws, codes, and standards, 604
modern steel-framed high-rise office buildings, 40–44
systems and equipment maintenance, 412
sequence of operation in high-rise building system, 365
threats, 65–66
Fire life safety survey checklist, 201–202
fact-finding process, 200–201
objectives, 200
report writing, 203
Fire load, 17, 24
Fire prevention codes, 603
Fireproof, 5, 24
Fireproofing insulation, 42
Fire protection, 41, 57
Fire pump, 368–369, 413
Fire resistance
definition, 44, 57
modern steel-framed high-rises, 44–46
Fire-resistive building, 57
Fire risk
hotels, 514, 516–517
mixed-use buildings, 585–586
office buildings, 464, 466
residential and apartment buildings, 554–556
Fire safety director, 355, 443, 499
Fire safety plan, see Emergency management plan
Fire science, basics, 121–123
Fire service elevator, 413
Fire stop, 179
Fire warden, see Floor warden
Fire watch, 57, 499
First Interstate Bank Building, Los Angeles fire, 134–136, 465
hostage situation, 149
Flood, 166
Floor, raised, 258
Floor plan, 179
Floor plate, 232, 499
Floor warden, 500
Fluorescent light, 316, 407
Footpath, see Sidewalk
Footprint, 232
Forensic analysis, 450
Foreseeeability, 607, 612
Formal investigation, 449
Freight elevator, 264
Freight/service elevator operator, 426, 443
Fuel load, see Fire load
Fujita scale, 164
Fuller Building, 10
G
Galloway v. Bankers Trust Company and Trustee Midlands Mall, 608
GAN, see Global area network
Gap analysis, 232
Garley Office Building, fire, 138–139, 465
Gas detector, 366, 413
Geared traction electric elevator, 263
Gearless traction electric elevator, 262–263
General ledger, 443
General Services Administration (GSA), response to Murrah Federal Building bombing, 104
Gilbert, Cass, 45
Gips, Michael, 37
Glasgow International Airport, bombing, 111–112
Glass, types for windows, 253–255
Global area network (GAN), 328, 346
Goldmark, Peter, 101
Goldsmith, Myron, 19
Gomez v. Ticor, 607–608
Governor, 263, 413
Gravity tank, 367
GSA, see General Services Administration
Guard booth, 243–244
Guest, 548, 580, 592
Guest folio, 512, 548
Guestroom key, 535–536
Guideline, 601, 612
Gurney, 264, 346, 413
H
Hall, John, 50–52, 158, 464, 514, 518, 555, 557, 586–587
Halon ban, 381
extinguishing systems, 381–382
fire extinguishers, 402
replacements, 382
Hard disk, 346
Hazard, see also Threat
definition, 232
Hazardous materials, 144–146
Heat detector, 364, 413
Heat transfer, mechanisms, 121–122
Heat wave, 163–164, 179
Heating, ventilation, and air-conditioning (HVAC)

- air-conditioning historical perspective, 7–8
- chemical, biological, and radiological agent control, 385–387
- layers of defense, 189
- oxygen supply for fires, 121
- requirements, 384–385
- smoke control, 385
- smoke spread, 123

High-pressure sodium vapor light, 316

High-rise
- deadliest fires, 124–126
- definitions, 1–2, 24
- fire risk, 50–51
- generations
  - fire resistance comparison of generations, 44–52
    - first generation, 16–17
    - second generation, 17–18
    - third generation, 18–21
- historical perspective, 2–8
- opening, 252
- types, 21–22

Hirsch ScramblePad Secure Electronic Keypad, 290

Hoistway, 179

Home Insurance Building, 8–9, 12

Hose station, 379

Hostage
- definition, 149, 179
- incidents, 149–150

Hotel
- definition, 21, 24, 505, 548, 592
- emergency planning
  - concepts, 494–496
  - door signage, 543–545
  - emergency staff organization, 541–542
    - evacuation drills, 546
    - occupant documentation and training, 542–545
    - plan development, 541–546
- occupancy characteristics, 506–508
- risk assessment
  - assets, 508
  - countermeasures, 517–519
  - fire risk, 514, 516–517
  - historical incidents, 514–515
  - overview, 507–508
  - threats, 508–513
  - vulnerabilities, 517

safety committee, 546

security programs
- access control
  - guest rooms, 524–526
  - maintenance and storage areas, 523–525
  - parking, 520–521
  - pedestrians, 519–523
  - stairwell access, 523
- escorts, 530
- eviction of guests, 529–530
- guest room security, 526–528
- housekeeping staff
  - screening, 533–534
  - security role, 534
- intoxicated persons, 529
- key control, 534–536
- patrols, 536–538
- property control
  - construction and remodeling, 532
  - couriers, 531
  - lost and found property, 532–533
  - objectives, 530–531
  - special exhibits, 531–532
- VIP guests, 528–529
- security staff levels, 425

Hotel Lasalle, fire, 128

Hotel-residence, see also Mixed-use building
- definition, 548, 592
- overview, 24

Housekeeping staff
- screening, 533–534
- security role, 534

Hurricane, 165–166, 180

Hurricane Katrina, 165

HVAC, see Heating, ventilation, and air-conditioning

Hydraulic elevator, 24, 264

I

IACP, see International Association of Chiefs of Police

ICC, see International Code Council
Identification card, 298–299
IDS, see Intrusion detection system
IED, see Improvised explosive device
IFTSA, see International Fire Service Training Association

Improvised explosive device (IED), 96, 180

Imputed negligence, 608–609

Incandescent light, 315–316
Incendiary devices, 180
Incident, 538, 573
Incident report, 430
Influenza pandemic, 167–168, 180
Informal investigation, 449
In-house security, see Proprietary security
Inn, 549
Innkeeper, 509, 549
Insertion-type card reader, 293–294
InstaKey, 275–276
Insulation, see Fireproofing insulation
Insurance industry, terrorism impact, 194
Intercom, 319–320, 356
Interlock, 288, 347
International Association of Chiefs of Police (IACP), 595
International Code Council (ICC), code changes after 9/11, 95
International Fire Service Training Association (IFSTA), 30
International Organization for Standardization (ISO), 610–611
Internet protocol (IP), 328, 346
Interoperability, 347
Interrogation
access card, 525
questioning, see Interview investigation
Interview investigation
conducting, 452–454
conversation encouraging, 455
ending of interview, 455–456
obstacles, 454
overview, 451
planning, 452
Intrusion detection system (IDS) components
annunciation device, 313
control unit, 312–313
sensors, 310–312
design, 309
offsite monitoring, 310
onsite monitoring, 309
Investigation
definition, 447, 458
electronic surveillance, 450
forensic analysis, 450
formal investigation, 449
informal investigation, 449
interview investigation conducting, 452–454
conversation encouraging, 455
ending of interview, 455–456
obstacles, 454
overview, 451
planning, 452
physical surveillance, 450
private investigators
investigation criteria, 457–458
selection criteria, 456–457
sources, 456
research and audit, 450
rights of investigators, 448
undercover investigation, 450–451
Ionization smoke detector, 361–362, 413
IP, see Internet protocol
Iris, 347
Islamabad JW Marriott Hotel, bombing, 112
ISO, see International Organization for Standardization
Istanbul, HSBC bank and British Consulate bombings, 108
Ivins, Bruce, 147
J
Jackson, Joe, 150
Jakarta JW Marriott Hotel, bombing, 108
Janitorial staff, screening, 486–487
Jin Mao Building, 14
Job description, 426, 444
Job specification, 426, 444
Jockey pump, 414
Joelma Building, fire, 129–130, 465
K
Karachi Sheraton Hotel, bombing, 106
Karpiloff, Doug, 37, 101
Kavanaugh, 11
Key bumping, 268–269
Keycard, 261, 266, 291, 344, 511, 523–527, 535, 543
Key control
audits, 279
blanks, 279
cabinet, 277–278
hotel, 534–536
inventories, 279
office building, 488–490
record, 279
residential and apartment buildings, 568–570
Key fob, 562
Key Performance Indicators (KPI), 419–420, 444
Khan, Fazlur, 19
Khubar Towers, bombing, 105
Kidnapping
   definition, 62, 149, 180
   incidents, 149–150
Kitteringham, Glen W., 29
*Klein v. 1500 Massachusetts Avenue Corporation*, 606
KPI, see Key Performance Indicators

L
Labor disputes, 150
Laminated glass, 254
LAN, see Local area network
Landlord, 500, 549, 551, 580
Landslide, 166, 500
Laptop, securing in hotel room, 527
Larceny, 62, 180
Las Vegas Hilton Hotel, fire, 131–132, 515
Latch, 347
Latch bolt, 270–271
Law, 601, 612
Law enforcement, building management liaison
   overview, 595
   relationship fostering
      communication, 596
      community service, 598
      compliance, 597
      disaster exercises, 598
      hospitality, 597
      professional organizations, 598
      public agency presentations, 598
      public agency support, 597
Layers of defense
   overview, 188–191
   risk assessment in terrorism risk mitigation, 208, 224–226
LCD, see Liquid crystal display
Leading question, 454
LED, see Light-emitting diode
Lens
   definition, 347
   types for closed-circuit television, 322–323
Lessee, 24, 500, 580
Lewd behavior, 62, 180

Liability
   definition, 604, 612
   security
      criminal liability, 610
      imputed negligence, 608–609
      nondelegable duty, 608
      protection of third party from crime, 606–608
      vicarious liability, 609–610
   Liability insurance, 419, 444
Lidle, Cory, 69
Light-emitting diode (LED), 317, 347
Lighting
   parking lots and garages, 314–315
   photoluminescent lighting, 406
   selection factors, 314–315, 317
   types, 315–317
Liquid crystal display (LCD), 259, 347
Load-bearing wall, 19, 24
Lobby director, 425, 444
Lobby doors, 246–248
Local area network (LAN), 328, 347
Locks
   biometric identification system-operated locks, 299–300
   bolts, 270–271
   credential-operated locks, 291–299
      key control, 277–279
   perimeter locking devices
      combination locks, 288–290
      electric locks, 287–288
      electromagnetic hold-open devices, 290–291
   electromagnetic locks, 280–281
   panic hardware, 279–280
   stairwell locking devices, 281–287
   pin tumbler lock
      key bumping, 268–269
      master keying
         mechanisms, 272–273
         problems, 275–276
         systems, 273–274
      overview, 266–269
      strikes, 271–272
Lodging facility, 549
London Tiger Tiger nightclub, bombing, 110–111
London transportation system, bombing, 109–110
Loomis, Dana, 175
Lost and found property
hotels, 532–533
log, 485, 533, 567
office buildings, 484–485
residential and apartment buildings,
567–568
Low-pressure sodium vapor light, 316

M
Machine roomless elevator, 264
Madrid train bombing, 109
Magnetic contact switch, intrusion detection
system, 310
Magnetic sandwich card, 292
Magnetic slug card, 293
Magnetic stripe card, 293
Mail room
chemical, biological, and radiological agent
control, 385–387
pedestrian access, 475–476
Maintenance
fire life safety equipment, 412
reports by security staff, 431
security equipment, 343
Manadnock Building, 6
Manhattan Company, 12
Manhattan Life Insurance Building, 12
Manslaughter, 62, 180
Mantrap, 347
Manual fire alarm station
definition, 358, 414
sequence of operations, 358–360
Masonic Temple Building, 12
Masonry, 237, 347
Mass notification system (MNS), 320–321, 347
Master key, hotel, 535
Master keying
definition, 347
mechanisms, 272–273
problems, 275–276
systems, 273–274
Matrix switcher, 332–333, 348
Maxa, Ruda, 513
Mayhem, 62, 180
McVeigh, Timothy, 104
Means of egress, 42, 57, 81, 281, 403
Mechanical clock, 340
Medical alert system, 410
Medical emergencies, 151
Megaphone, 320
Mega-high-rise, 54, 57–58
Mercantile occupancy, 506, 549
Mercury vapor light, 316
Metal detector
people and property screening, 305–307
vehicle and container screening, 308
Metal halide light, 316
Methamphetamine, manufacture in hotels,
513
Metrics, 419, 444
Metropolitan Life Insurance Building,
10, 17
Metropolitan Life Tower, 12
MGM Grand Hotel, Las Vegas fire, 130–131,
515
Microwave motion detector, intrusion
detection system, 312
Mitigation measure, see Countermeasure
Mixed-use building
definition, 22, 25, 592
emergency planning, 589–590
occupancy characteristics, 583
overview, 583
risk assessment
assets, 584–585
countermeasures, 587–588
overview, 583–584
threats, 585–586
vulnerabilities, 586–587
security
programs, 588–589
staff levels, 425
MNS, see Mass notification system
Mobile phone, 317, 321, 348, 414
MobileSearch, 483
Mobility impaired, 180
Monbassa hotel, bombing, 107
Morrison, et al. v. MGM Grand Hotel, et. al.,
606–607
Mortise cylinder lock, see Pin tumbler lock
Motel, 50, 514, 549, 555, 585
Mullion, 18, 25
Multiple-tenant/multiple-use building, 462
Multiple-tenant/single-use building, 461
Multiplexer, 333, 348
Multiplex video recording, 333–334
Mumbai
Taj Mahal Palace and Hotel and Oberoi
Hotel bombing, 112–115, 531
train bombing, 110
Municipal fire alarm box, 360, 414
Murder, 62, 181
Murrah Federal Building, bombing, 103–105, 465
Mutual aid agreement, 496, 500, 546, 549, 579

N
Nairobi Embassy, bombing, 105–106, 256
National Earthquake Hazard Reduction Program, 159
National Fire Incident Reporting System (NFIRS), 50, 52, 464, 467, 514, 555
National Fire Protection Association (NFPA), 50, 201, 282, 367, 353, 514, 555, 598, 603
National Institute of Standards and Technology (NIST) functions, 76
investigation of World Trade Center building collapse, 46–49, 76, 82–95
Natural disasters, see Disease; Earthquake; Flood; Heat wave; Storms; Tsunami; Volcano
Negligence, 606, 612
Network video recorder (NVR), 334–335
NFPA, see National Fire Protection Association
NFIRS, see National Fire Incident Reporting System
NIST, see National Institute of Standards and Technology
Noncyclone, 164
Nondelegable duty, 608
Nonescalatable costs, 419, 444
Nonsprinklered, 414
Nordenson, Guy, 54–55
North York, Ontario residential building fire, 138
Northridge earthquake, 157–160
Nuclear attack, 147–149
Nuisance alarm, 414
NVR, see Network video recorder

emergency planning
concepts, 494–496
plan development, 496
occupancy development, 496
risk assessment
assets, 463
countermeasures, 466–467
fire risk, 464, 466
historical incidents, 464–465
overview, 462–463
threats, 463
vulnerabilities, 466
security programs
building access control, 467–469
key control, 488–490
patrols, 490–492
pedestrian access
after-hours access register, 474
authorization documents, 472
business hours, 470–471
electronic access cards, 473
escorts, 478
identification cards, passes, and badges, 472–473
right to pass signs, 474
solicitor handling, 476–477
tenant access controls, 474–478
visitor management software, 473–474
visual recognition, 471–472

property control
asset tracking system, 481–482
controlled ingress and egress, 487–488
couriers and delivery persons, 483–484
explosive device screening, 482–483
janitorial staff screening, 486–487
lost and found property, 484–485
objectives, 479
package acceptance policy, 484
property removal pass, 479–481
trash removal control, 485–486
tenant security education, 492–494
vehicle access
docks and receiving, 469–470
parking lots and garages, 469
security staff levels, 424
O'Hagan, John T., 16, 44–45, 49, 51, 517, 556
Oklahoma City bombing, see Murrah Federal Building
One Meridian Plaza, fire, 137, 465
One-step exit, 283
Otis, Elisha Graves, 4–5
Outsourcing, 444

**P**
PA, see Public address system
Pacific Tower Plaza, 462
Pacific Tsunami Warning System (PTWC), 162
Pad detector, intrusion detection system, 310
Pager, 319
Pan/tilt mechanisms, 325–326, 348
Panic, 181, 500
Panic alarm, 244, 313, 345, 410, 491, 536, 570
Panic hardware, 279–280, 348
Park Hotel, 11
Park Row Building, 12
Parking
  closed-circuit television in lots and garages, 337–339
  controllers and barriers, 241–243
  hotel security, 520–521
  lighting, 314–315
  office building access, 469
  residential and apartment building security, 558–559
  violations, 490, 537, 570
Parque Central, fire, 141, 465
Partial evacuation, 181, 500
Passive infrared detector, intrusion detection system, 311
Passive vehicle barrier, 348
Patrol management
  electronic guard tour system, 340–341
  hotels, 536–538
  mechanical clock, 340
  office buildings, 490–492
  vehicles, 341
  virtual guard tour, 341–342
Patrol officer, 426, 444
Patron, 549, see also Guest
Pavement, see Sidewalk
PBX operator, 507, 549
PDA, see Personal data assistant
Peachtree 25th Building, fire, 136–137, 465
Peephole, 259, 350, 526
Penetration testing, 194, 232
Penthouse, 522, 549
Performance-based codes, 181, 603, 612
Performance-based design, 181
Perimeter
  barriers and physical control, 237–239
  signage, 244
  Personal alarm system, 409–410
  Personal data assistant (PDA), 320
  Personal protection device, 410
  Petronas Towers, 12–14
  Phase I operation, 414
  Phase II operation, 414
  Phased evacuation, 500
  Photoelectric smoke detector, 362–363, 414
  Photoelectric detector, intrusion detection system, 312
Photoluminescent markers, 406–408
Physical security, 28, 58, 181
Physical security survey, see Security survey
Physical surveillance, 450
Piggybacking, 298, 348
Pin tumbler lock
  cylinder, 348
  key bumping, 268–269
  master keying
    mechanisms, 272–273
    problems, 275–276
    systems, 273–274
  overview, 266–269
Pinhole lens, 323, 348
Pirelli Tower, aircraft collision, 68–69
Pixels, 348
Plaintiff, 606, 613
Plan, 500, 539
Planter, barriers, 239
Plenum, 42, 45, 58
Plinth, 191, 232
PLUS, see Promoting Logical Unified Security
Poke-throughs, 181
Policy, 427, 444
Portable controlled descent device, see Stair descent device
Portable fire extinguisher
  carbon dioxide fire extinguishers, 401–402
  definition, 398, 414
  dry chemical fire extinguishers, 402–403
  fire classes and extinguishing agents, 398–400
  halon fire extinguishers, 402
  markings, 399
  mounting, 403–404
  placement, 403
  water-based fire extinguishers, 400–401
  wet chemical fire extinguishers, 403

safetymessage.com
Portable two-way radio
base station, 318
repeaters, 318–319
transmitter and receiver, 318
Portal, 348
Port Authority, see World Trade Center
Post orders, 427–429, 444
Power failure, 176
Power transformer room, 348
Pratt, Philip, 366
Preaction system, 375–376
Premises security, 549
Prescriptive design approach, 181
Prescriptive-based codes, 181, 603, 613
Preset positioning, 349
Pressure mat, intrusion detection system, 310
Pressure tank, 368
Private investigator
investigation criteria, 457–458
selection criteria, 456–457
sources, 456
Private security, 27, 58
Procedure, 427, 444
Progressive collapse, 58, 73, 182
Promoting Logical Unified Security (PLUS), 227–228
Property control, see Apartment building; Hotel; Office building
Property removal pass
overview, 479–480
permanent pass, 480–481
required information, 480
sample, 481
Proprietary security, 445
Prostitution, control in hotels, 511–512
Protection Officer Training Manual, 431–432
Protection-in-depth, 188, 232
Protestors, 117
Proximity card
dual technology cards, 295–296
overview, 295
PTWC, see Pacific Tsunami Warning System
Public address system (PA), 319, 355, 414
Public housing, 552
Public relations, security department, 441–442
Public security, 27, 58
Public telephone emergency telephone number, 360, 414–415

Q
Quick-response sprinkler, 371–372

R
Radiation dispersal device (RDD), 148–149
Radiation, heat transfer, 122
Radio frequency identification (RFID)
asset tracking, 308
dual technology cards, 296
overview, 295
Raised floor, 349
Rape, 182
Rapid entry systems, 302–304
RDD, see Radiation dispersal device
Reasonable care, 607, 613
Rebar, 237, 349
Reinforced concrete, 20–21, 25
Rembrandt Tower, hostage situation, 149–150, 465
Rent, 21, 25, 474, 501, 581
Repeater, 318–319, 349
Residence, 25, 581, 592
Resident, 25, 581
Residential building, see also Apartment building
definition, 25, 551, 581, 592
emergency planning
concepts, 573–575
emergency staff organization, 576–577
evacuation drills, 579
exit signs, 578–579
occupant documentation, 577–578
occupant training, 578
plan development, 575–579
occupancy characteristics, 552–553
overview, 21–22
risk assessment
assets, 533–534
countermeasures, 556–557
fire risk, 554–556
overview, 553
threats, 554–556
vulnerabilities, 556
security programs
access control
locks, 564
overview, 558
parking, 558–559
pedestrians, 559–563
solicitors, 563–564
visitor systems, 562–563
escorts, 564–565
property control
construction and remodeling, 567
couriers, 566–567
key control, 568–570
lost and found property, 567–568
objectives, 565–566
patrols, 570–572
trash removal control, 568
resident security education, 572–573
Residential sprinkler, 372
Restroom, 41, 58
Restroom doors, 261
Retention rate, 420, 445
RFID, see Radio frequency identification
Richter scale, 152
Right to pass sign, 474, 522, 563
Riot, 182
Risk
definition, 185, 232
equation for terrorism risk mitigation, 215
Risk assessment, see also Fire life safety survey; Promoting Logical Unified Security; Security survey; Terrorist attack mitigation
consultant and specialist utilization
rationale, 229–230
sources, 230
definition, 185–186, 233
hotels
assets, 508
countermeasures, 517–519
fire risk, 514, 516–517
historical incidents, 514–515
overview, 507–508
threats, 508–513
vulnerabilities, 517
methodologies, 187
mixed-use buildings
assets, 584–585
countermeasures, 587–588
overview, 583–584
threats, 585–586
vulnerabilities, 586–587
office building
assets, 463
countermeasures, 466–467
fire risk, 464, 466
historical incidents, 464–465
overview, 462–463
threats, 463
vulnerabilities, 466
residential and apartment buildings
assets, 553–554
countermeasures, 556–557
fire risk, 554–556
overview, 553
threats, 554–556
vulnerabilities, 556
systematic viewing of building
interior spaces, 188
layers of defense, 188–191
rings, 188
Risk management, definition, 186–187, 233
Riyadh residential compounds, bombing, 107–108
Robbery, 62, 182
Robertson, Leslie E., 55
Rome, ancient buildings, 3–4, 7
Roth, Emery, 11
Royal Jomtien Resort, fire, 139, 515
Runners/messengers, 501
Sabotage, 62, 182
Safe, hotel room, 305
Safe refuge area, 501
Safe room, 304–305, 349
Safety
definition, 28, 58
World Trade Center attacks and impact, 53–55
Safety hazard report, 430
Saflok Messenger Wireless Lock Access Network, 292, 525
St. Paul Building, 12
Sallyport, 347
Sarin gas attack, 147
SARS, see Severe acute respiratory syndrome
SCEPP, see Southern California Earthquake Preparedness Project
Schnabolk, Charles, 101
Scissor stairs, 349
Seabrook, John, 45
Search monitor, 501
Sears Tower, 12, 14, 266
Security
adequate security concept, 611
definitions, 27–28, 58
guidelines and standards, 610–611
high-rise versus low-rise buildings, 28–29
hotel, see Hotel
law, 605
liability, 605–610
safetymessage.com
Security (Continued)
modern steel-framed high-rise office
buildings, 31–33
office building, see Office building
rating, see Promoting Logical Unified
Security
Security assessment, see Security survey
Security audit, 233
Security barrier, 349
Security budget
items, 418–418
Key Performance Indicators, 419–420, 444
Security command center, see also Command
center
definition, 349
equipment, 235–236
standards, 342–343
Security department
budget, see Security budget
computerized incident reporting, 432
contract staff, 420–421
forms, records, and reports, 429–432
members, 417, 425–426
notebooks, 431
post orders
contents, 427–428
definition, 427
writing, 429
proprietary staff, 420–421
public relations, 441–442
security service, see Contract security service
selection of staff, 433–434
staffing levels by building type, 424–425
supervision
discipline, 438–440
motivation, 437–438
overview, 436
supervisor training, 440
tools, 437
training, 434–436
uniforms and equipment, 440–441
World Trade Center attacks and impact, 36–40
Security director, see Director of security
Security function, 445
Security guard, see Security officer
Security-in-depth, 188, 233
Security key, safe, 305
Security master plan, 233, 592
Security mirror, 313–314
Security officer, 417, 426, 445
Security program, 233
Security service, see Contract security service
Security survey
balancing security and fire life safety,
283–287
checklist, 194
definition, 186, 233
fact-finding process, 192–194
presentation of report, 199
report contents
appendices, 199
asset identification, 196
cover letter, 195
description of areas, 196–197
executive summary, 198
introduction, 195
method of compilation, 196
security measures and recommendations,
197
summary of recommendations, 198
table of contents, 195
title pages, 195
word of caution, 199–200
Security threat, see Threat
Security window film, 255–256
SecuScan, see Under Vehicle Monitoring
System SecuScan
Segway PT, 341
Self-evacuation, 501
Sensors, intrusion detection system, 310–312
September 11 attack, see World Trade Center
Service panel, elevator, 389–390
Setback, 59, 233–234
Severe acute respiratory syndrome (SARS),
168, 182
Sexual harassment, 62, 182
Shanghai World Financial Center, 13–14
Shear wall, 20, 25
Shelter-in-place, see Defend-in-place
Shift activity report, 429–430
Shift supervisor, 425, 445
Sidelight panel, 254, 349
Sidewalk, 13, 25, 191
Sidewall sprinkler, 233, 592
Signage
exit signs, 403–406, 578–579
hotel door, 543–545
perimeter, 244
photoluminescent, 406–408
right to pass signs, 474, 522, 563
Signature Building, 234
Singer Building, 12
Single-tenant/multiple-use building, 461
Single-tenant/single-use building, 461
Situation awareness, 501, 540, 575
Skateboard, barriers, 241
Skilling, John, 55
Sky-lobby, 59, 265–266
Skyscraper
definition, 25
driving forces, 15–16
historical perspective, 2, 4, 8–12
race for world's tallest building, 12–15
Slab, 25–26
Slab floor, 26
Slander, 549
Slip-and-fall, 169
Smart card, 296–298, 349
Smoke
definition, 43, 59
daylight safety threat, 123–124
Smoke detector
addressable device, 364
definition, 361, 415
ionization smoke detector, 361–362
photoelectric smoke detector, 362–363
placement, 363–364
Solicitor
definition, 467, 501, 519
handling
office buildings, 476–477
residential and apartment buildings, 563–564
Solomon, Robert, 95, 372
Southern California Earthquake Preparedness Project (SCEPP), 41
Span of control, 445
Split lens, 323
Split screen unit, 349
Sprinkler, see Automatic sprinkler
Sprinkler system, 415
Stack effect, 18, 26, 44, 123, 501
Stacking plan, 192, 234
Staged evacuation, see Partial evacuation
Stair descent device, 501
Stairs, 349
Stair tread, 406, 415
Stairway, 349
Stairwell
definition, 349
doors
exterior fire doors, 248–249
interior doors, 260
hotel access, 523
intercom systems, 356
locking devices
balancing security and fire life safety, 283–287
building roof exits, 286–287
ground level exits, 284–286
simultaneous unlocking controls, 397
Stairwell monitor, 501
Stalking, 62, 169–170, 182
Stand-off distance, 234, 239, 350
Standard
definition, 601, 613
types, 601–602
Standard of care, 509, 549, 613
Standard operating procedures, 146, 427
Standard spray sprinkler, 370–371
Standards of conduct, security, 428
Standby power
elevators, 395
systems, 396–397
Standpipe system
classes
Class I, 377–378
Class II, 378
Class III, 378–379
definition, 376, 415
fire department connections, 380
monitoring, 380
types, 379
zoning in tall buildings, 379
Stanger, Tyler, 69
Steel, production, 5
Steel-framed construction
advantages, 7
core construction, 18–19
steel-framed reinforced concrete construction, 21
tube construction, 19–20
Steel moment frames, 182
Storms
noncyclone, 164
tornado, 164–165
tropical cyclone, 165–166
Strike, locks, 271–272
Suction tank, 368
Suicide, 62, 118, 182
Suicide bomber, 96–97
Suite warden, 501
Supervise, 445
Swipe-type card reader, 293–294
System riser, 415

T
Tabletop exercise, 502
Tae Yon Kak Hotel, fire, 515
Tailgating, 298
Taipei 101, 12–14
Taj Mahal Palace and Hotel, bombing, 112–115, 515
Tanzania Embassy, bombing, 106
Telephone
communication systems, 317–318
public telephone for fire department use, 356
Telephone monitor, 502
Tempered glass, 253
Temporary access card, 299
Temporary identification badge, 299
Tenant
definition, 26, 502, 581
security education, 492–494
Tenant manual, 492–493, 502
Tenant/resident security notice, 431
Terrorism, definition, 182
Terrorist attack mitigation
steps in risk assessment
overview, 203–205
step I
design base threat determination, 206
information collection, 205–206
rating of threat, 207
threat identification, 205
step II asset value assessment, 207–210
step III vulnerability assessment
evaluation of site and building, 212–213
portfolio preparation, 213–214
rating, 214–215
resource organization for preparation, 210–212
tiers of assessment, 211–212
step IV risk assessment, 214–215
step V consider mitigation options
cost estimation, 221–224
layers of defense review, 224–226
overview, 215–217
preliminary option identification, 217–219
review of options, 219–221
Terroristic threat, 64, 182–183
Tessler, Herb, 263
Testing, 502
Theft, 62, 183
Threat assessment, 234
Threat
definition, 28, 59, 183, 185, 234
risk assessment
mixed-use buildings, 585–586
office buildings, 463
hotels, 508
residential and apartment buildings, 555–556
terrorist attack mitigation
design base threat determination, 206
information collection, 205–206
rating of threat, 207
threat identification, 205
types
fire life safety threats, 65–66
security threats, 61–65
Threat rating, 234
Tiger Tiger nightclub, bombing, 110–111
Token, 350
Tokyo subway, sarin gas attack, 147
Tornado, 164–165, 183
Tornado alley, 165
Tort, 605, 613
Total evacuation, 502
Tower of Babel, 2, 15
Traffic accident, 176
Train, 445, 502
Training
definition, 445
security staff, 434–436, 440
Training officer, 426, 445
Transom, 254, 350
Transponder, 350
Trash bin, barriers, 238
Trash compactor, 482
Trash removal, control in office buildings, 485–486
Trespass, 62, 183
Triangle Shirtwaist Company, fire, 126–128
Tropical cyclone, 165–166, 183, see also Cyclone
Tsunami, 160–162, 183
Tube structure, 19
Tuberculosis, 168–169, 183
Turnover rate, 420, 445
Turnstile, 300–302
Two International Finance Centre, 14
Two-way radio, see Portable two-way radio
Typhoon, 165–166, 183–184

U
Ultrasonic motion detector, intrusion detection system, 311
Unabomber, 96
Undercarriage, camera and scanning systems, 339
Undercover investigation, 450–451
Under Vehicle Monitoring System SecuScan, 339, 483
Uninterruptible power supply (UPS), 357, 396, 415
Unsprinklered, 51, 59, 415
Upgrading, security equipment, 343–344
UPS, see Uninterruptible power supply

V
Vandalism
definition, 63, 184
elevators, 119
VBIED, see Vehicle-borne improvised explosive device
VCR, see Videocassette recorder
Vehicle accident report, 430
Vehicle-borne improvised explosive device (VBIED)
definition, 96, 184
overview, 97–98
screening at office buildings, 483
Ventricular fibrillation (VF), automated external defibrillator, 410
Very important person (VIP), hotel security, 528–529
VF, see Ventrilcular fibrillation
Vibration detector, intrusion detection system, 311
Vicarious liability, 609–610
Victoria Hotel, fire, 515
Video analytics, 331–332, 350
Video monitor
controls, 329
definition, 328
lifetime, 329
mounting, 330
onscreen displays, 329
operator viewing effectiveness, 330–331
size, 329
Video monitor, definition, 350
Video motion detector (VMD), intrusion detection system, 312, 333
Video printer, 332, 350
Video switcher
definition, 332, 350
matrix switcher, 332–333
multiplexer, 333
multiplex video recording, 333–334
Videocassette recorder (VCR), 333–334
View port, 259, 350, 526
VIP, see Very important person
Virtual guard tour, 341–342
Visitor badge, 560
Visitor log, 430
Visitor management software, 39, 59
VMD, see Video motion detector
Voice-over Internet protocol (VoIP)
definition, 300, 350
door entry system, 300
residential and apartment buildings, 562
VoIP, see Voice-over Internet protocol
Volcano, 162–163, 184
Vulnerability
definition, 185, 234
risk assessment
hotels, 517
mixed-use buildings, 586–587
office buildings, 466
residential and apartment buildings, 556
terrorist attack mitigation
evaluation of site and building, 212–213
portfolio preparation, 213–214
rating, 214–215
resource organization for preparation, 210–212
tiers of assessment, 211–212
Vulnerability assessment, 234

W
Waldorf-Astoria Hotel, 10
Wall, barriers, 237–238
WAN, see Wide area network

safetymessage.com
Watch clock, see Mechanical clock
Watch commander, 445
Water leak, 176
Water-based fire extinguishers, 400–401
Webb, Bill, 358
Wet chemical fire extinguishers, 403
Wet chemical system, 383–384
Wet-pipe system, 375
Wide area network (WAN), 328, 350
Wiegand effect card, 293
Windows
bars, grilles, screens, and shutters, 256–257
blast curtains, 256
decals, 252–253
glass types
annealed glass, 253
bullet-resistant glass, 255
burglar-resistant glass, 255
laminated glass, 254
tempered glass, 253
wired glass, 254
security film, 255–256
weakness, 255
Windsor Building, fire, 141–143, 465
Winecoff Hotel, fire, 128–129, 515
Wired glass, 254
Won door, 260–261, 350
Woolworth Building, 12, 17
Worker’s compensation insurance, 419, 445
Workplace violence
categories, 171
definition, 171, 184
geographic distribution, 171–173
prevention, 174–176
profiles, 173–174
World Building, 12
World Trade Center (WTC)
bombing in 1993
building safety response, 53–54
features and security response, 36–38
Port Authority liability, 101
security staff response, 100–101
sequence of events, 98–100
buildings, 33–34
daredevils, 116–117
elevators, 262
evacuation
WTC1, 86–88
WTC2, 88–91
historical perspective, 12
occupant population and demographics, 83–86
recommendations for buildings being evaluated for extreme events, 80–82
security profile, 35
September 11 attack
building performance study, 75–79
building safety response, 54–55
decedent characteristics, 84–86
features and security response, 38–40
National Institute of Standards and Technology investigation of collapse, 46–49, 82–95
overview, 69–71
sequence of events, 71–75
sky-lobby, 265
Wrought iron, 237
WTC, see World Trade Center

X
X-ray
people and property screening, 305–307
vehicle and container screening, 308

Y
Yard, layer of defense, 191

Z
Zoned evacuation, see Partial evacuation
Zoom lens, 323, 350