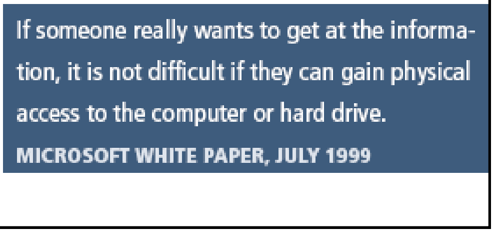
Principles of Information Security

Chapter 9

Physical Security

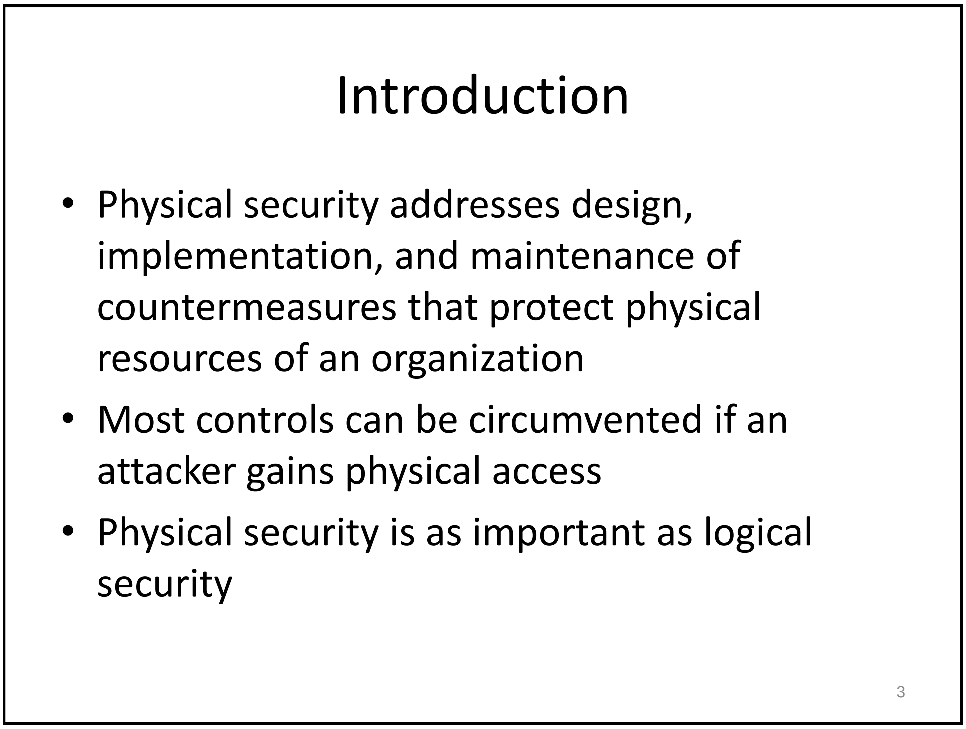


If someone really wants to get at the information, it is not difficult if they can gain physical access to the computer or hard drive.

MICROSOFT WHITE PAPER, JULY 1999

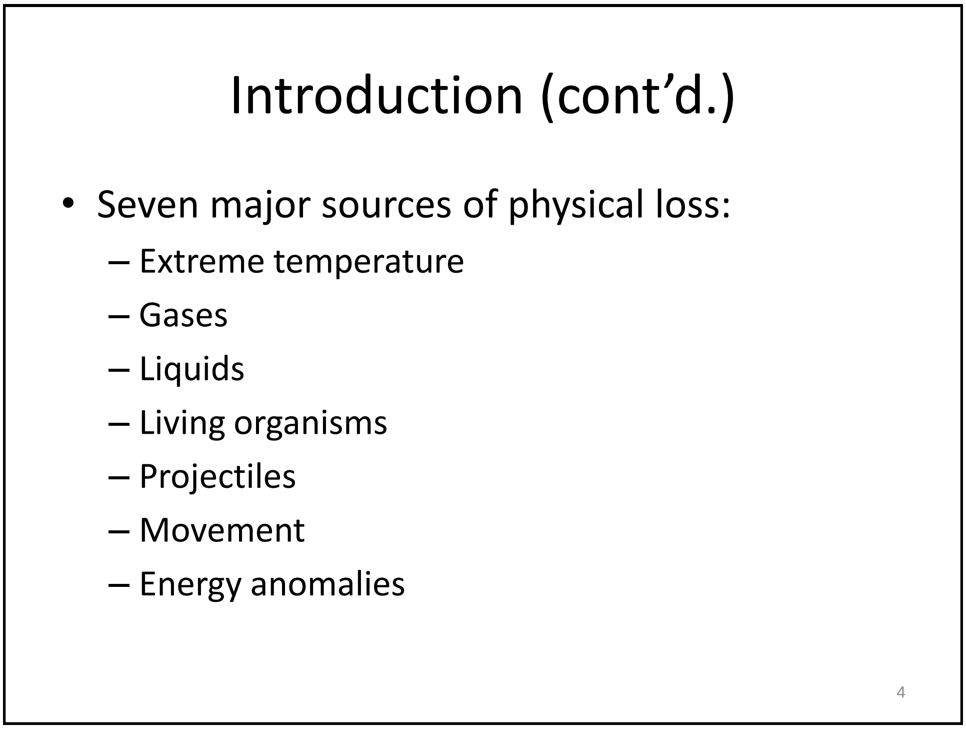
Learning Objectives

- Upon completion of this material, you should be able to:
  - Discuss the relationship between information security and physical security
  - Describe key physical security considerations, including fire control and surveillance systems
  - Identify critical physical environment considerations for computing facilities, including uninterruptible power supplies



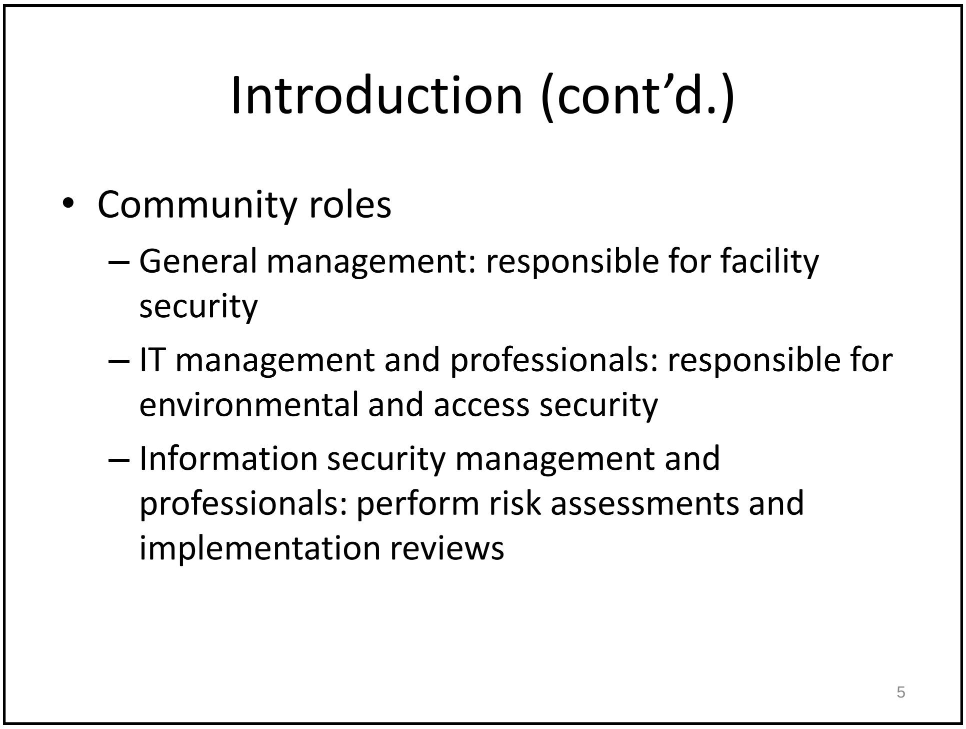
Introduction

- Physical security addresses design, implementation, and maintenance of countermeasures that protect physical resources of an organization
- Most controls can be circumvented if an attacker gains physical access
- Physical security is as important as logical security



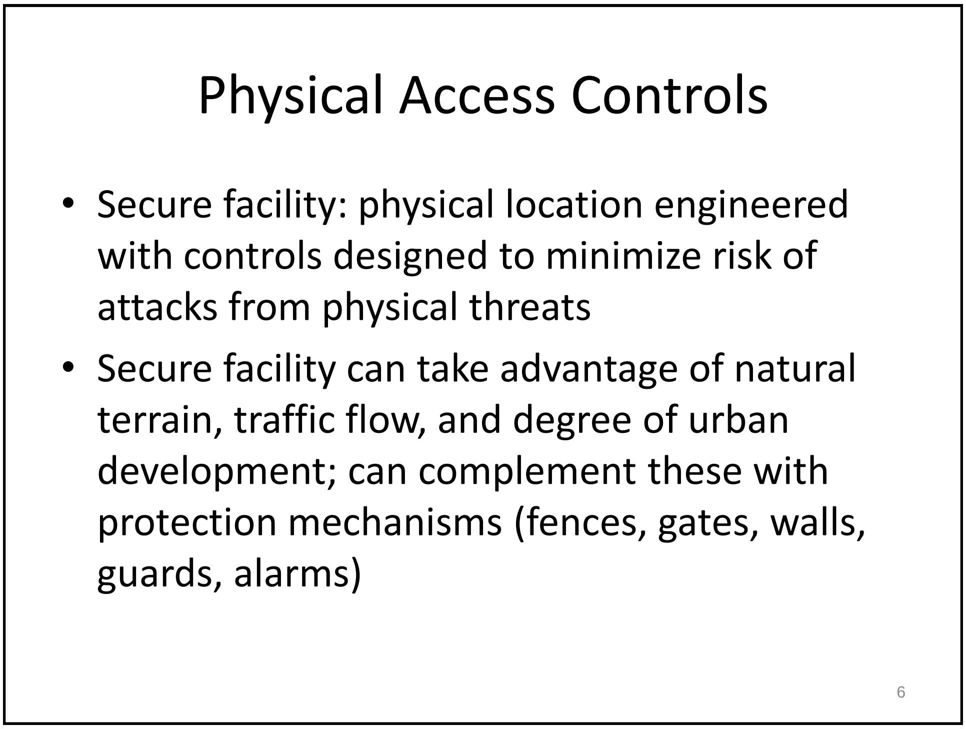
Introduction (cont'd.)

- Seven major sources of physical loss:
  - Extreme temperature
  - Gases
  - Liquids
  - Living organisms
  - Projectiles
  - Movement
  - Energy anomalies



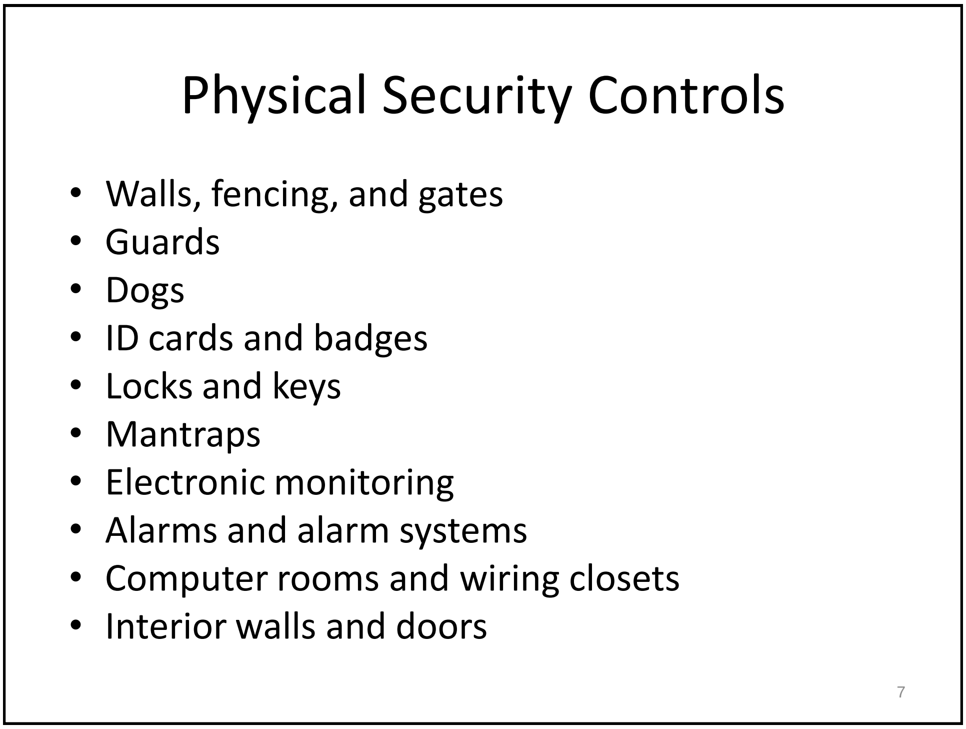
Introduction (cont'd.)

- Community roles
  - General management: responsible for facility security
  - IT management and professionals: responsible for environmental and access security
  - Information security management and professionals: perform risk assessments and implementation reviews



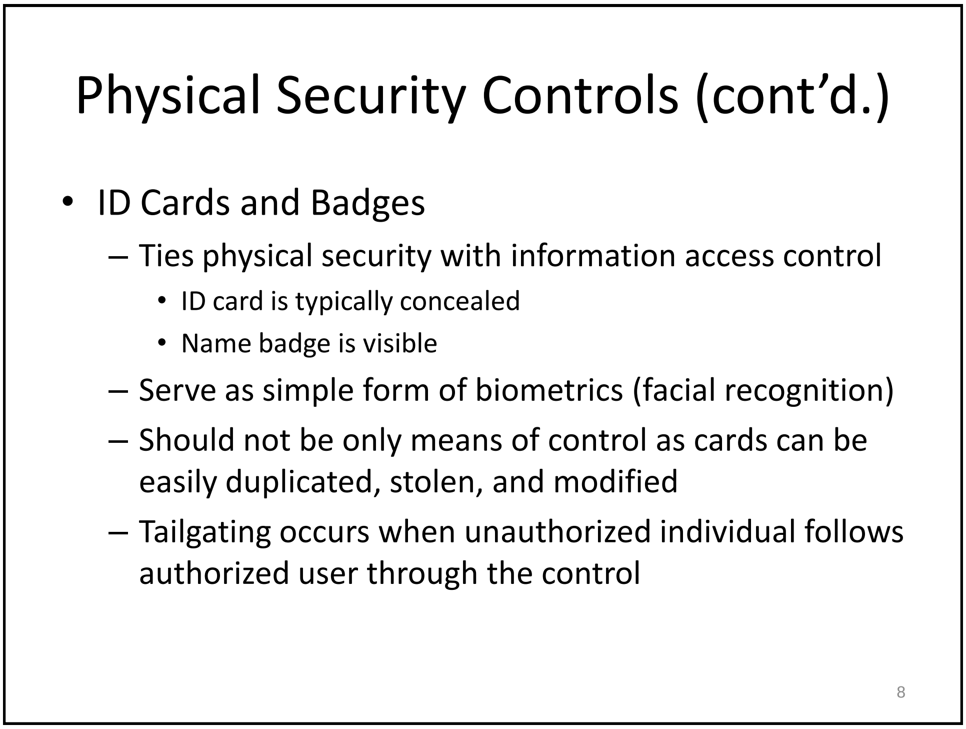
Physical Access Controls

- Secure facility: physical location engineered with controls designed to minimize risk of attacks from physical threats
- Secure facility can take advantage of natural terrain, traffic flow, and degree of urban development; can complement these with protection mechanisms (fences, gates, walls, guards, alarms)



Physical Security Controls

- Walls, fencing, and gates
- Guards
- Dogs
- ID cards and badges
- Locks and keys
- Mantraps
- Electronic monitoring
- Alarms and alarm systems
- Computer rooms and wiring closets
- Interior walls and doors

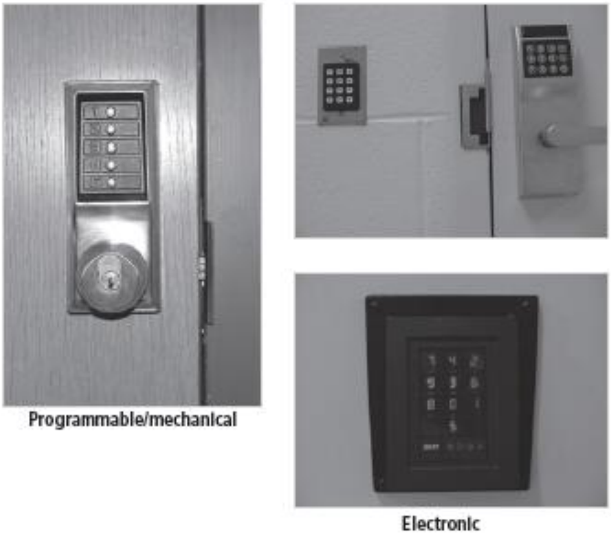


Physical Security Controls (cont'd.)

- ID Cards and Badges
  - Ties physical security with information access control
    - ID card is typically concealed
    - Name badge is visible
  - Serve as simple form of biometrics (facial recognition)
  - Should not be only means of control as cards can be easily duplicated, stolen, and modified
  - Tailgating occurs when unauthorized individual follows authorized user through the control

Physical Security Controls (cont’d.)

- Locks and keys
  - Two types of locks: mechanical and electromechanical
  - Locks can also be divided into four categories: manual, programmable, electronic, biometric
  - Locks fail and alternative procedures for controlling access must be put in place
  - Locks fail in one of two ways:
    - Fail-safe lock
    - Fail-secure lock



Programmable/mechanical

Electronic

Figure 9-1 Locks

Physical Security Controls (cont'd.)

- Mantrap
  - Small enclosure that has entry point and different exit point
  - Individual enters mantrap, requests access, and if verified, is allowed to exit mantrap into facility
  - Individual denied entry is not allowed to exit until security official overrides automatic locks of the enclosure

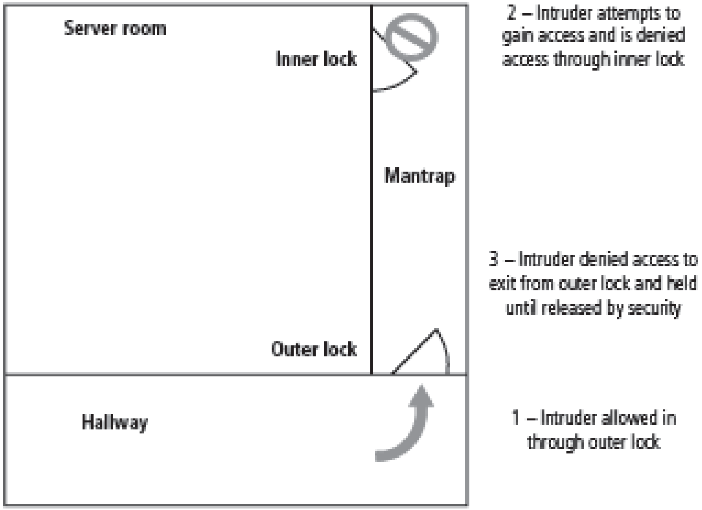

Server room
Inner lock
2 – Intruder attempts to gain access and is denied access through inner lock
Mantrap
3 – Intruder denied access to exit from outer lock and held until released by security
Outer lock
Hallway
1 – Intruder allowed in through outer lock

Figure 9-2 Mantraps

Physical Security Controls (cont'd.)

- Electronic Monitoring
  - Records events where other types of physical controls are impractical or incomplete
  - May use cameras with video recorders; includes closed-circuit television (CCT) systems
  - Drawbacks
    - Reactive; does not prevent access or prohibited activity
    - Recordings often are not monitored in real time; must be reviewed to have any value

Physical Security Controls (cont'd.)

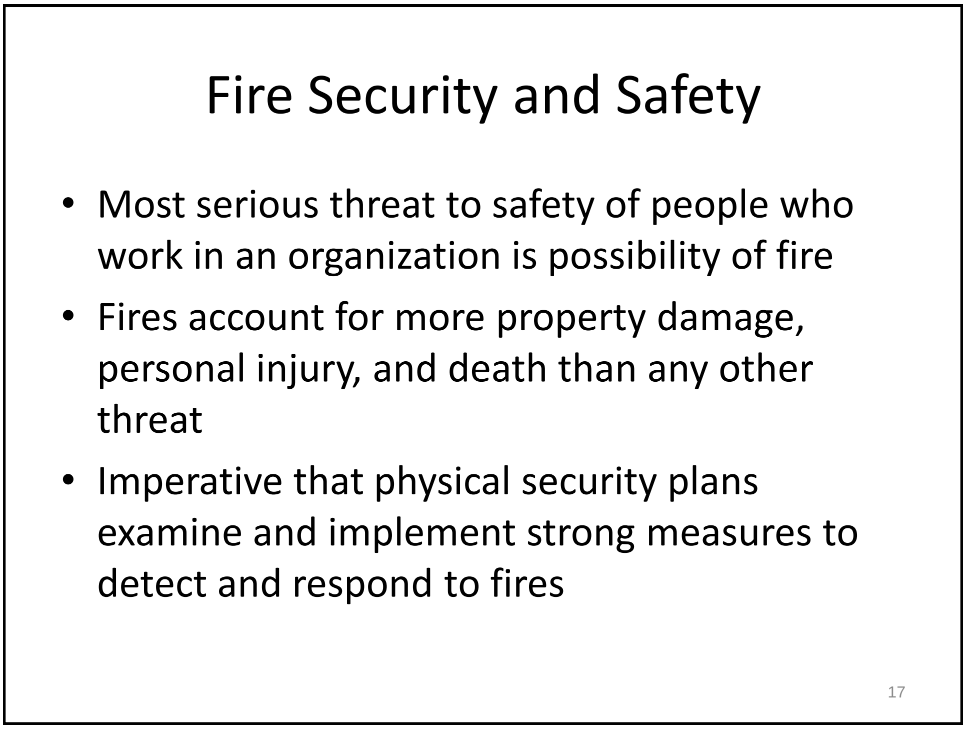
- Alarms and alarm systems
  - Alarm systems notify when an event occurs
  - Detect fire, intrusion, environmental disturbance, or an interruption in services
  - Rely on sensors that detect event; e.g., motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, contact sensors, vibration sensors

Physical Security Controls (cont’d.)

- Computer rooms and wiring closets
  - Require special attention to ensure confidentiality, integrity, and availability of information
  - Logical controls easily defeated if attacker gains physical access to computing equipment
  - Custodial staff often the least scrutinized persons who have access to offices; are given greatest degree of unsupervised access

Physical Security Controls (cont’d.)

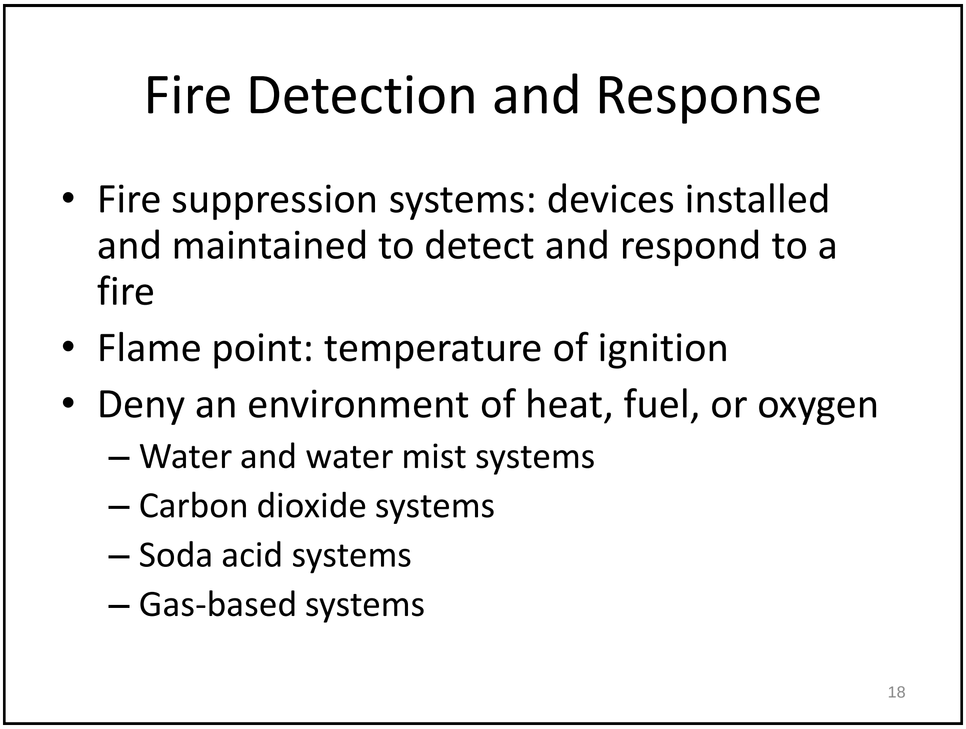
- Interior walls and doors
  - Information asset security sometimes compromised by construction of facility walls and doors
  - Facility walls typically either standard interior or firewall
  - High-security areas must have firewall-grade walls to provide physical security from potential intruders and improve resistance to fires
  - Doors allowing access to high security rooms should be evaluated
  - Recommended that push or crash bars be installed on computer rooms and closets



Fire Security and Safety

- Most serious threat to safety of people who work in an organization is possibility of fire
- Fires account for more property damage, personal injury, and death than any other threat
- Imperative that physical security plans examine and implement strong measures to detect and respond to fires

17



Fire Detection and Response

- Fire suppression systems: devices installed and maintained to detect and respond to a fire
- Flame point: temperature of ignition
- Deny an environment of heat, fuel, or oxygen
  - Water and water mist systems
  - Carbon dioxide systems
  - Soda acid systems
  - Gas-based systems

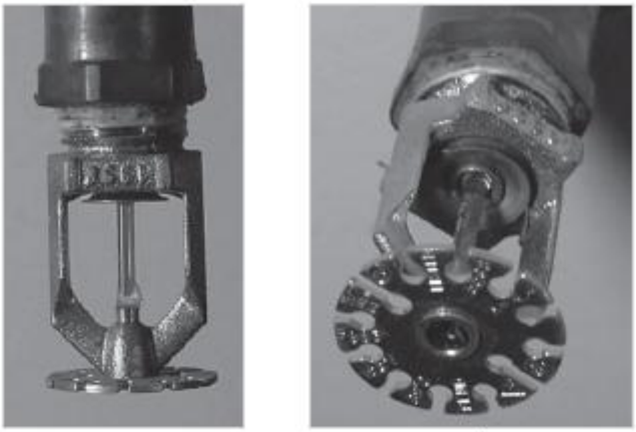
18

Fire Detection and Response (cont'd.)

- Fire detection
  - – Fire detection systems fall into two general categories: manual and automatic
  - – Part of a complete fire safety program includes individuals that monitor chaos of fire evacuation to prevent an attacker accessing offices
  - – There are three basic types of fire detection systems: thermal detection, smoke detection, flame detection

Fire Detection and Response (cont'd.)

- Fire suppression
  - – Systems consist of portable, manual, or automatic apparatus
  - – Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D
  - – Installed systems apply suppressive agents; usually either sprinkler or gaseous systems



When the ambient temperature reaches 140-150° F,
the liquid-filled glass tube trigger breaks, releasing the stopper and
allowing water to hit the diffuser, spraying water throughout the area

Figure 9-3 Water sprinkler system

Fire Detection and Response (cont’d.)

- Gaseous emission systems
  - Until recently, two types of systems: carbon dioxide and Halon
  - Carbon dioxide robs a fire of oxygen supply
  - Halon is clean but has been classified as an ozone-depleting substance; new installations are prohibited
  - Alternative clean agents include FM-200, Inergen, carbon dioxide, FE-13 (trifluromethane)

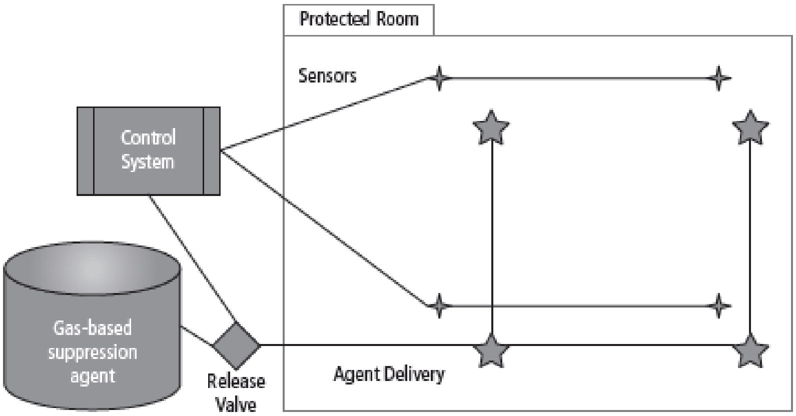


Figure 9-4 Gaseous fire suppression system

Failure of Supporting Utilities and Structural Collapse

- Supporting utilities (heating, ventilation, and air conditioning; power; water; and others) have significant impact on continued safe operation of a facility
- Each utility must be properly managed to prevent potential damage to information and information systems

Heating, Ventilation, and Air Conditioning

- Areas within heating, ventilation, and air conditioning (HVAC) systems that can cause damage to information systems include:
  - Temperature
  - Filtration
  - Humidity
  - Static electricity

Heating, Ventilation, and Air Conditioning (cont'd.)

- Ventilation shafts
  - While ductwork is small in residential buildings, in large commercial buildings it can be large enough for an individual to climb though
  - If vents are large, security can install wire mesh grids at various points to compartmentalize the runs

Heating, Ventilation, and Air Conditioning (cont’d.)

- Power management and conditioning
  - Electrical quantity (voltage level, amperage rating) and quality of power (cleanliness, proper installation) are concerns
  - Noise that interferes with the normal 60 Hertz cycle can result in inaccurate time clocks or unreliable internal clocks inside CPU

Heating, Ventilation, and Air Conditioning (cont’d.)

- Grounding and amperage
  - Grounding ensures that returning flow of current is properly discharged to ground
  - Overloading a circuit causes problems with circuit tripping and can overload electrical cable, increasing risk of fire
  - GFCI: capable of quickly identifying and interrupting a ground fault

Heating, Ventilation, and Air Conditioning (cont’d.)

- Uninterruptible power supply (UPS)
  - In case of power outage, UPS is backup power source for major computer systems
  - Four basic UPS configurations:
    - Standby
    - Ferroresonant standby
    - Line-interactive
    - True online (double conversion online)

29

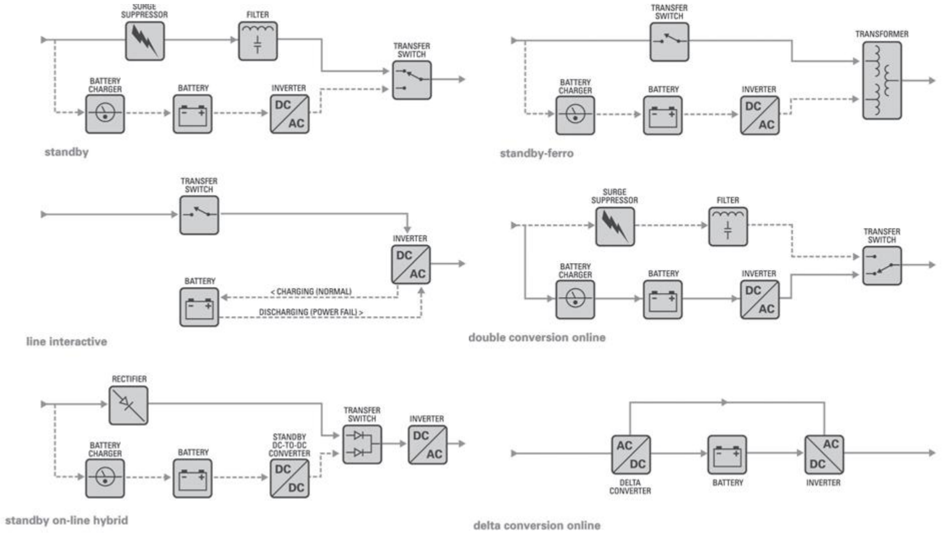
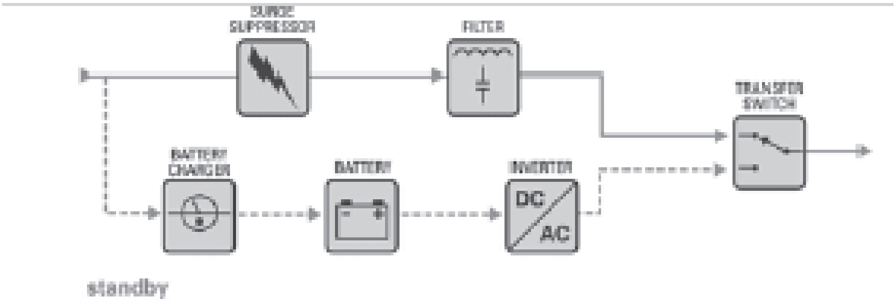


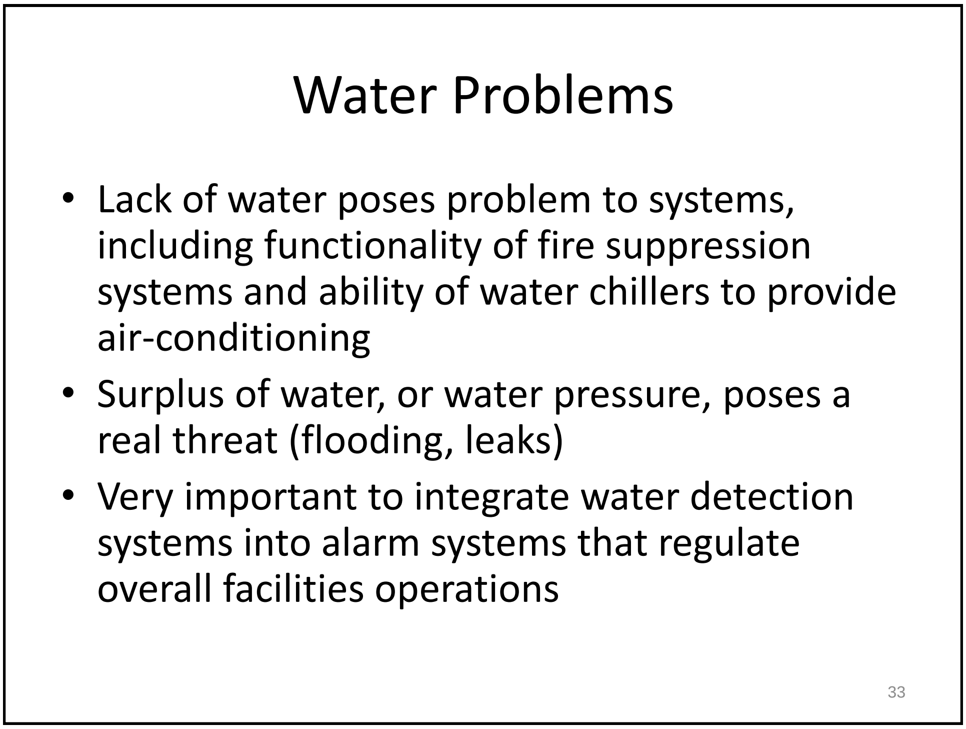
Figure 9-5 Types of uninterruptible power supplies[9]
Source: Courtesy of American Power Conversion Corporation

30



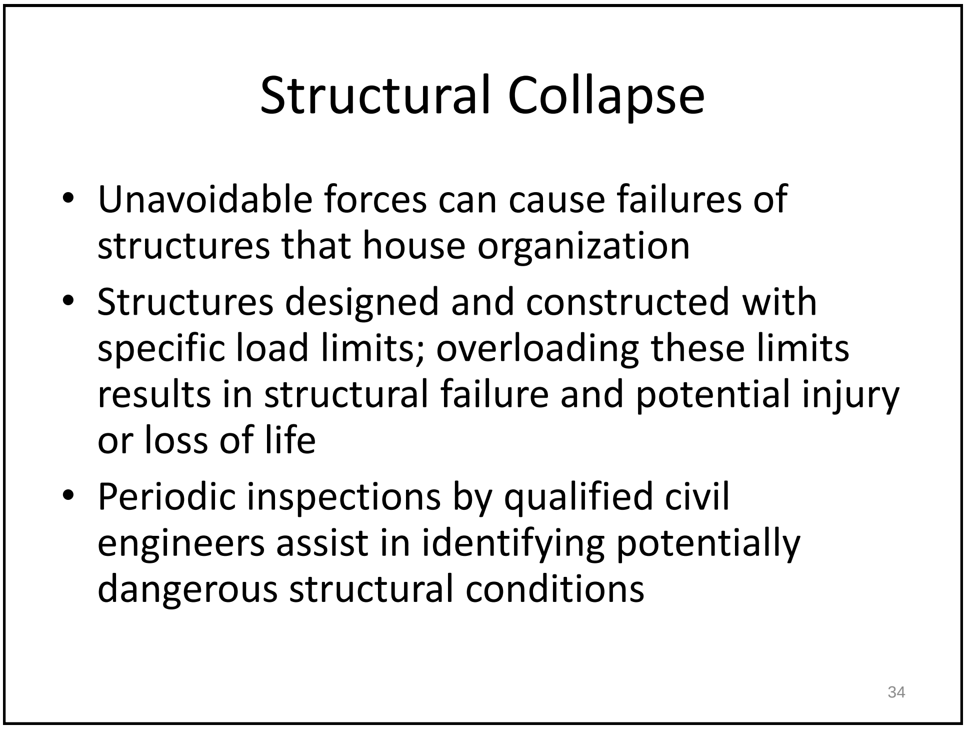
Heating, Ventilation, and Air Conditioning (cont'd.)

- Emergency shutoff
  - Important aspect of power management is the need to be able to stop power immediately should a current represent a risk to human or machine safety
  - Most computer rooms and wiring closets are equipped with an emergency power shutoff



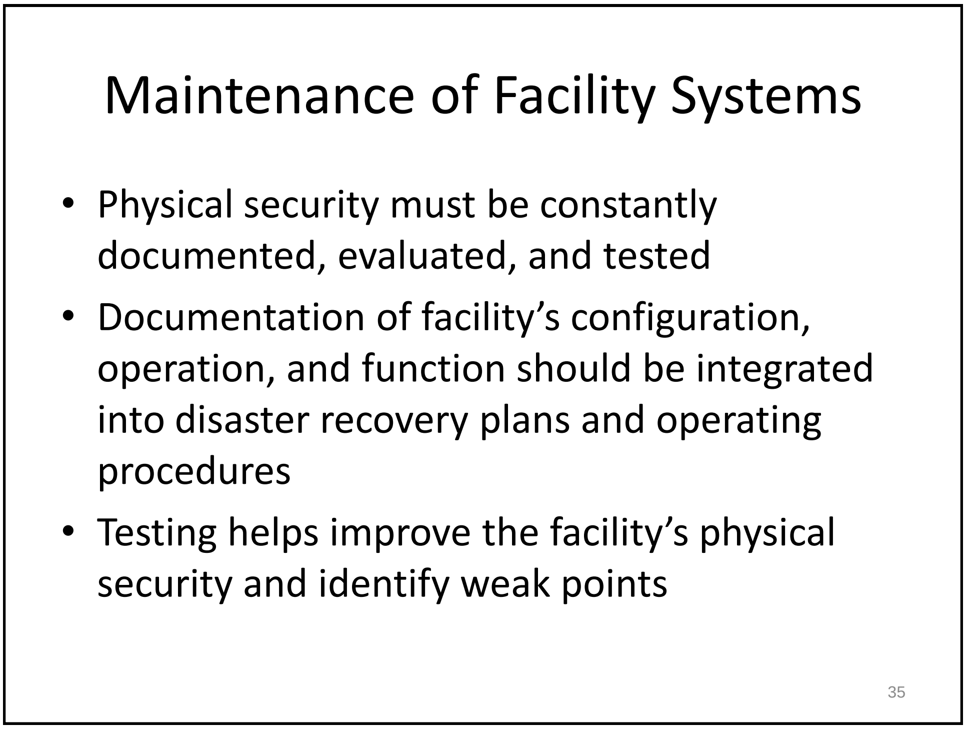
Water Problems

- Lack of water poses problem to systems, including functionality of fire suppression systems and ability of water chillers to provide air-conditioning
- Surplus of water, or water pressure, poses a real threat (flooding, leaks)
- Very important to integrate water detection systems into alarm systems that regulate overall facilities operations



Structural Collapse

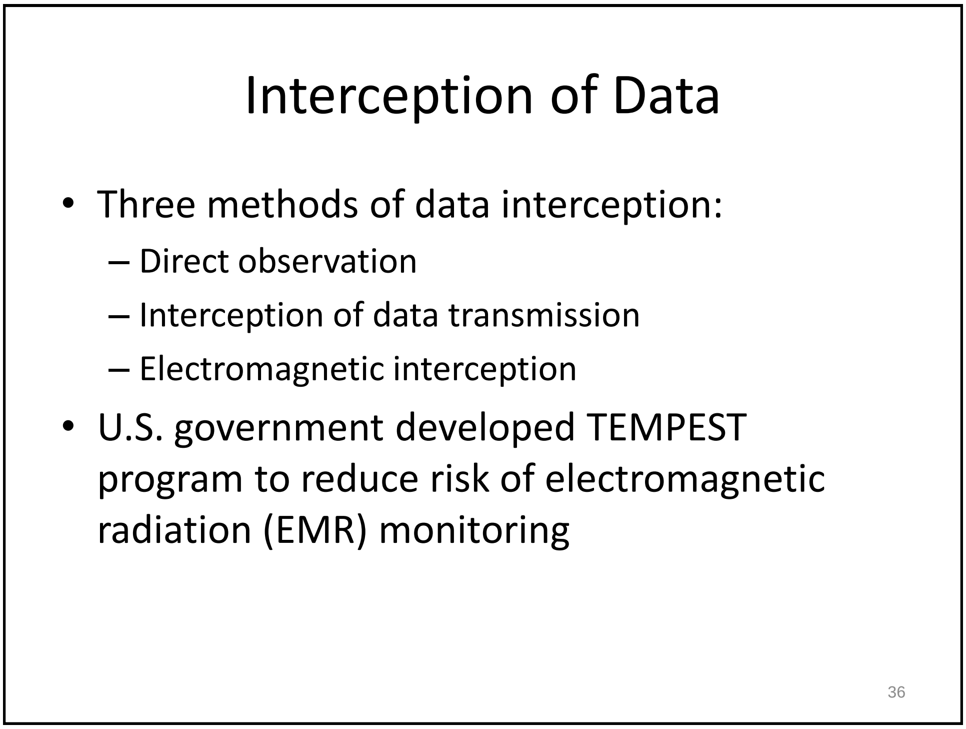
- Unavoidable forces can cause failures of structures that house organization
- Structures designed and constructed with specific load limits; overloading these limits results in structural failure and potential injury or loss of life
- Periodic inspections by qualified civil engineers assist in identifying potentially dangerous structural conditions



Maintenance of Facility Systems

- Physical security must be constantly documented, evaluated, and tested
- Documentation of facility’s configuration, operation, and function should be integrated into disaster recovery plans and operating procedures
- Testing helps improve the facility’s physical security and identify weak points

35



Interception of Data

- Three methods of data interception:
  - Direct observation
  - Interception of data transmission
  - Electromagnetic interception
- U.S. government developed TEMPEST program to reduce risk of electromagnetic radiation (EMR) monitoring

36

Mobile and Portable Systems

- With the increased threat to information security for laptops, handhelds, and PDAs, mobile computing requires more security than average in-house system
- Many mobile computing systems
  - Have corporate information stored within them
  - Some are configured to facilitate user’s access into organization’s secure computing facilities

Mobile and Portable Systems (continued)

- Controls support security and retrieval of lost or stolen laptops
  - CompuTrace software, stored on laptop; reports to a central monitoring center
  - Burglar alarms made up of a PC card that contains a motion detector

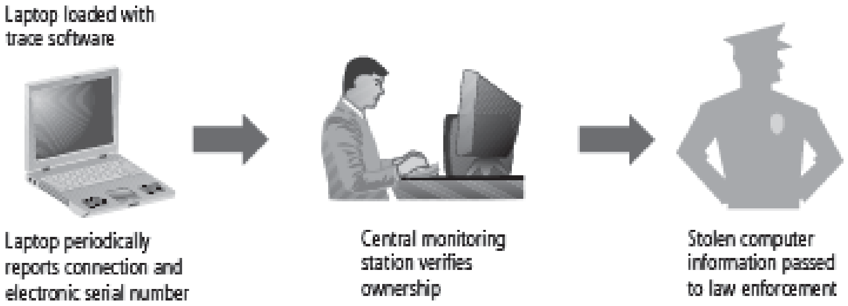

Laptop loaded with trace software
Laptop periodically reports connection and electronic serial number
Central monitoring station verifies ownership
Stolen computer information passed to law enforcement

Figure 9-6 Laptop theft deterrence

Remote Computing Security

- Remote site computing: away from organizational facility
- Telecommuting: computing using telecommunications including Internet, dial-up, or leased point-to-point links
- Employees may need to access networks on business trips; telecommuters need access from home systems or satellite offices
- To provide secure extension of organization’s internal networks, all external connections and systems must be secured

Special Considerations for Physical Security Threats

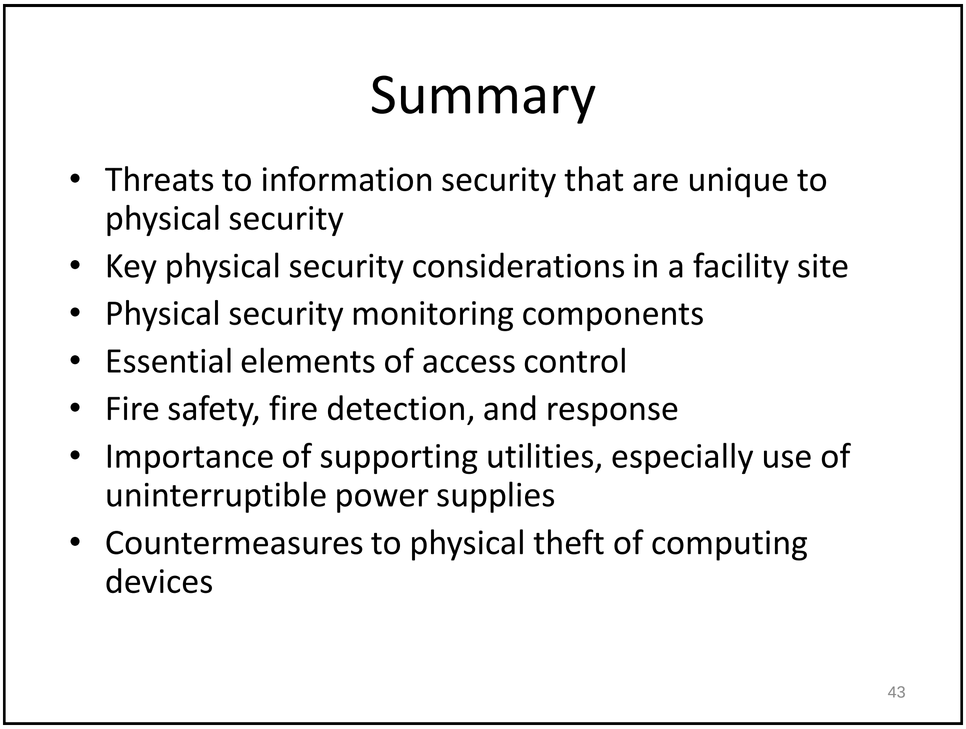
- Develop physical security in-house or outsource?
  - Many qualified and professional agencies
  - Benefit of outsourcing includes gaining experience and knowledge of agencies
  - Downside includes high expense, loss of control over individual components, and level of trust that must be placed in another company
- Social engineering: use of people skills to obtain information from employees that should not be released

41

Inventory Management

- Computing equipment should be inventoried and inspected on a regular basis
- Classified information should also be inventoried and managed
- Physical security of computing equipment, data storage media, and classified documents varies for each organization

42



Summary

- Threats to information security that are unique to physical security
- Key physical security considerations in a facility site
- Physical security monitoring components
- Essential elements of access control
- Fire safety, fire detection, and response
- Importance of supporting utilities, especially use of uninterruptible power supplies
- Countermeasures to physical theft of computing devices