COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fifth Edition

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 involves the protection of physical items, objects, or areas from unauthorized access and misuse.
- Most technology-based 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 with controls implemented to minimize the risk of attacks from physical threats
- Secure facility can take advantage of natural terrain, local traffic flow, and surrounding development and 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)

- Walls, Fencing, and Gates
  - Some of the oldest and most reliable elements of physical security; the essential starting point for perimeter control
- Guards
  - Can evaluate each situation as it arises to make reasoned responses; most have standard operating procedures
- Dogs
  - Keen sense of smell and hearing can detect intrusions that human guards cannot

Physical Security Controls (cont'd)

- ID Cards and Badges
  - ID card is typically concealed and name badge is visible.
  - Serve as a simple form of biometrics (facial recognition)
  - Should not be the only means of control as cards can be easily duplicated, stolen, and modified
  - Tailgating occurs when an authorized individual opens a door and other people also enter.

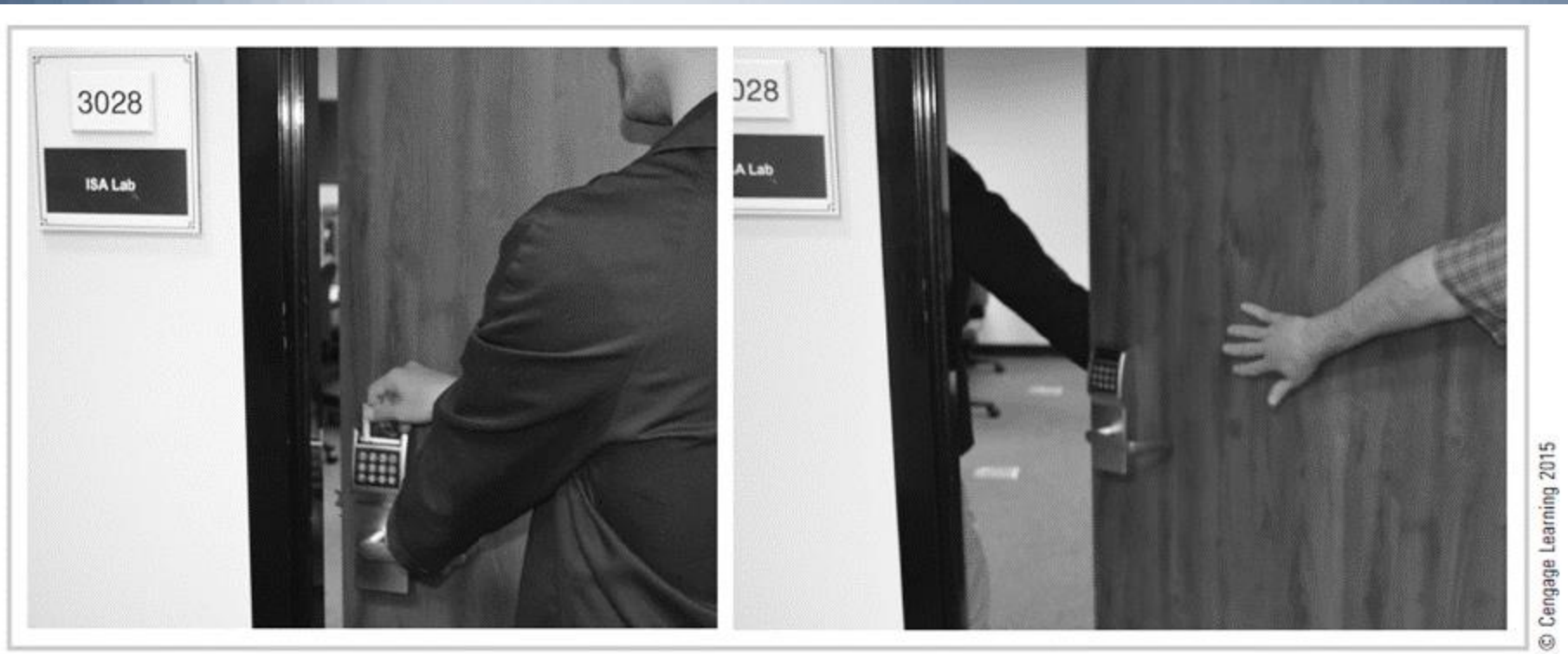


Figure 9-1 Tailgating

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 9-2 Locks

Physical Security Controls (cont'd)

- Mantraps
  - Small enclosure that has an entry point and a 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 the security official overrides automatic locks of the enclosure.

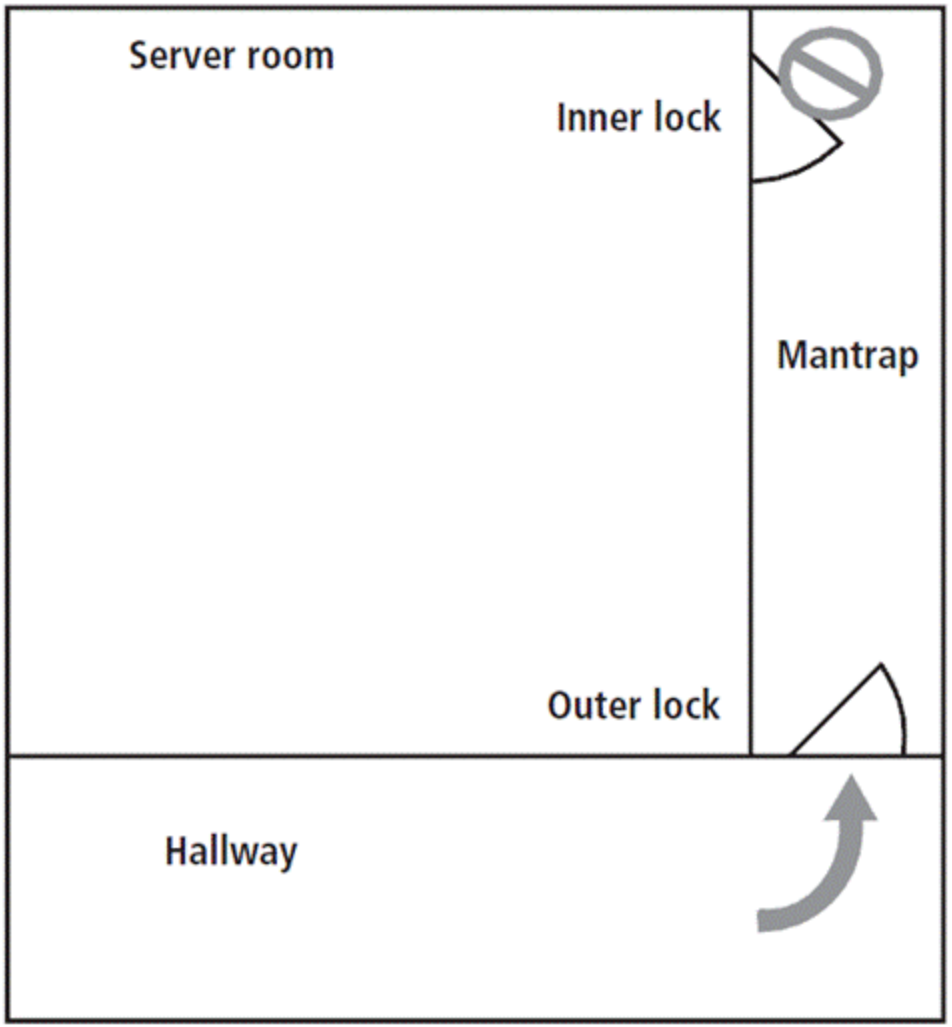


Figure 9-3 Mantraps

Physical Security Controls (cont'd)

- Electronic Monitoring
  - Equipment can record events in areas where other types of physical controls are impractical.
  - May use cameras with video recorders; includes closed-circuit television (CCT) systems
  - Drawbacks
    - Passive; 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 people/systems when an event occurs.
  - Detect fire, intrusion, environmental disturbance, or an interruption in services
  - Rely on sensors that detect an event, for example, motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors

Physical Security Controls (cont'd)

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

Physical Security Controls (cont'd)

- Interior walls and doors
  - Information asset security is sometimes compromised by improper construction of facility walls and doors.
  - Facility walls are typically either standard interior or firewall.
  - High-security areas must have firewall-grade walls to provide physical security against potential intruders and fires.
  - Doors allowing access to high-security rooms should be evaluated.
  - To secure doors, install push or crash bars on computer rooms and closets.

Fire Security and Safety

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

Fire Detection and Response

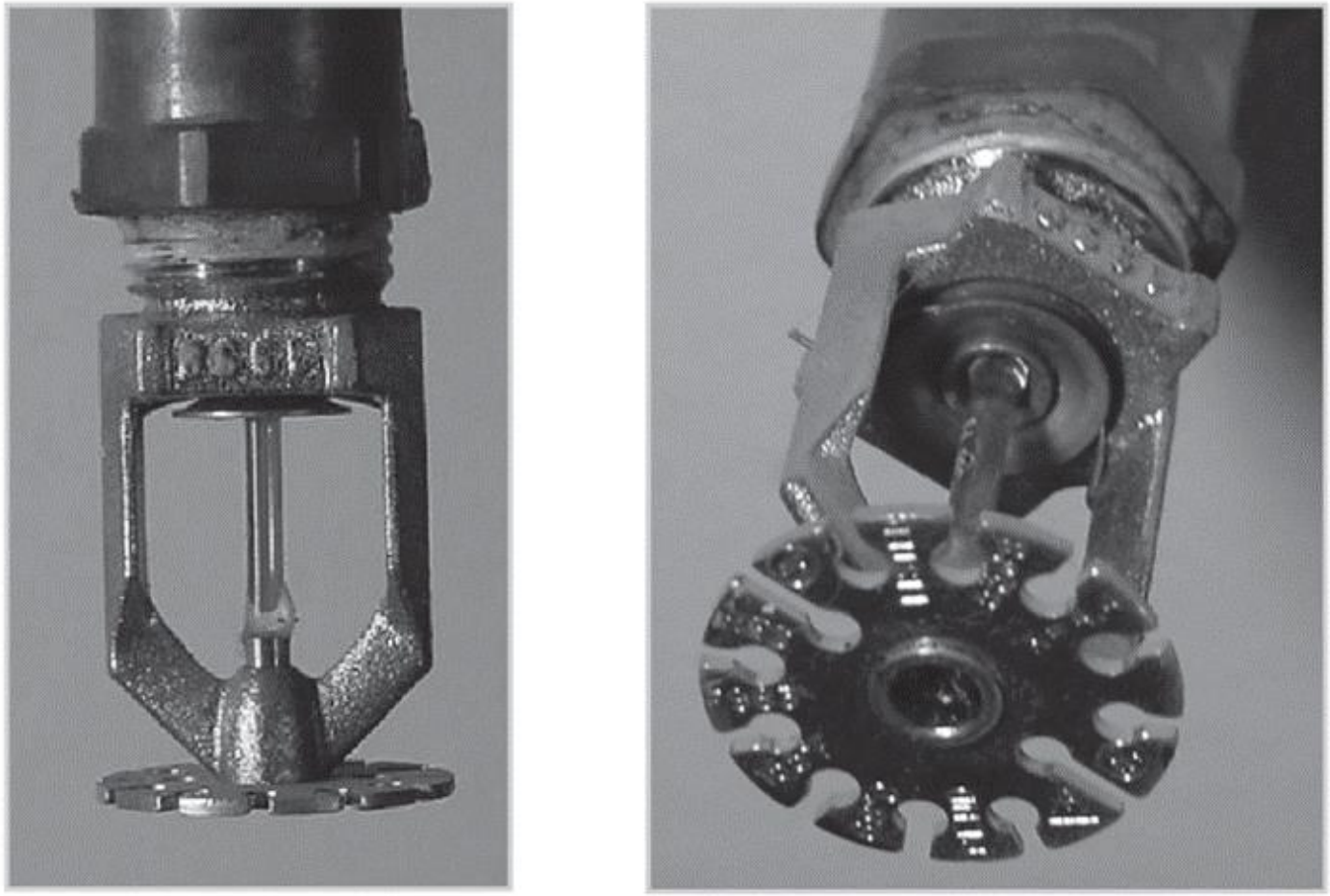
- Fire suppression systems: devices installed and maintained to detect and respond to a fire, potential fire, or combustion danger
- Flame point: temperature of ignition
- Deny an environment of temperature, fuel, or oxygen
  - Water and water mist systems
  - Carbon dioxide systems
  - Soda acid systems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

Fire Detection and Response (cont'd)

- Fire detection
  - Fire detection systems fall into two general categories: manual and automatic
  - To prevent an attacker slipping into offices during an evacuation, programs often designate a person from each office area to serve as a floor monitor.
  - There are three basic types of fire detection systems: thermal detection, smoke detection, flame detection

Fire Detection and Response (cont'd)

- Fire suppression
  - Systems can consist of portable, manual, or automatic apparatus.
  - Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D, Class K.
  - 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 9-4 Water sprinkler system

Fire Detection and Response (cont'd)

- Gaseous emission systems
  - Until recently, two types of systems: carbon dioxide and Halon
  - Carbon dioxide removes fire's oxygen supply.
  - Halon is clean but has been classified as an ozone-depleting substance; new installations are prohibited.
  - Alternative clean agents presented in Table 9-1 (found on pages 484-485 in the text) are reported to be less effective than Halon.

System Components

1. Discharge nozzles
2. Piping
3. Control panel
4. Discharge or warning alarm(s)
5. Hazard warning or caution signs
6. Automatic fire detection device(s)
7. Manual discharge station(s)
8. Storage container(s) & extinguishing agent

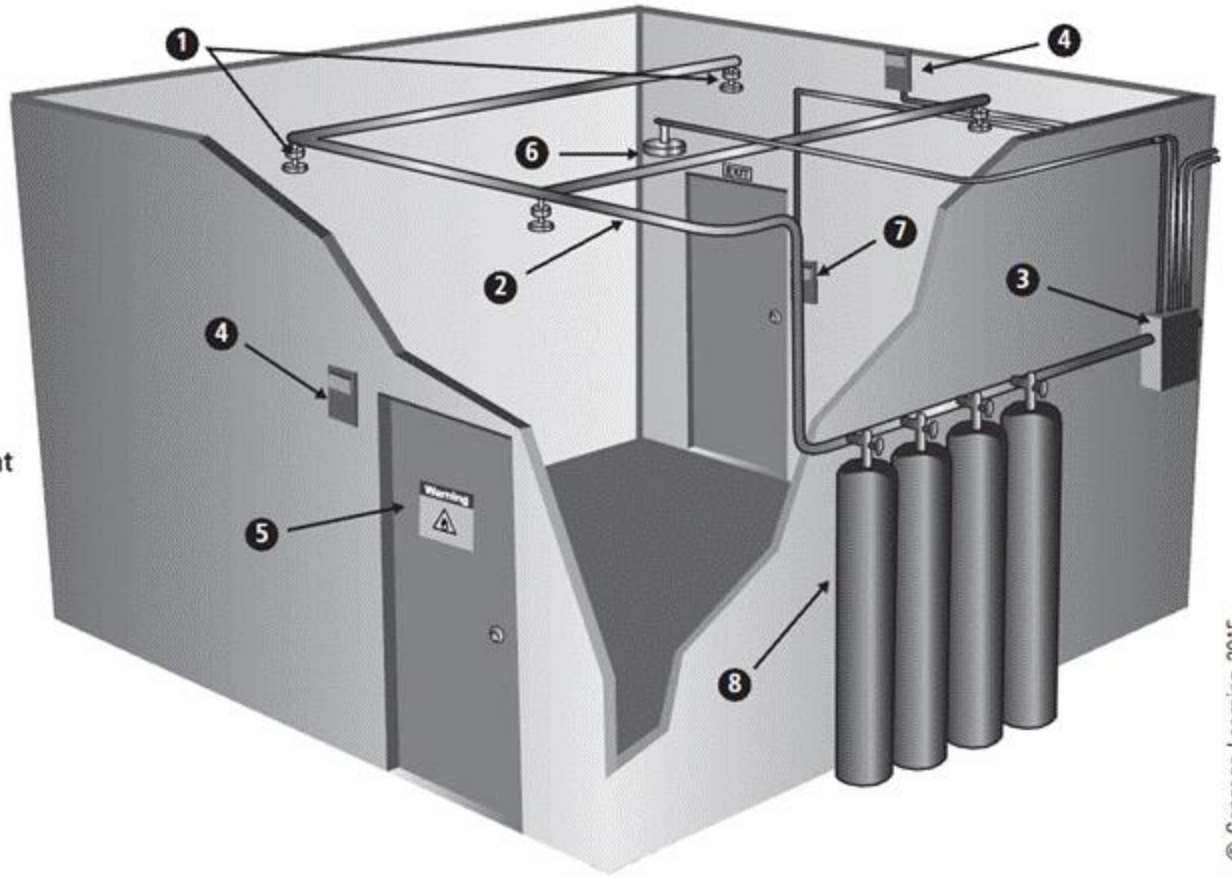


Figure 9-5 Gaseous fire suppression system

Failure of Supporting Utilities and Structural Collapse

- Supporting utilities (heating, ventilation, and air conditioning; power; water) 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

Voltage	Possible damage
40	High probability of damage to sensitive circuits and transistors
1,000	Scrambles monitor display
1,500	Can cause disk drive data loss
2,000	High probability of system shutdown
4,000	May jam printers
17,000	Causes certain and permanent damage to almost all microcircuitry

Table 9-2 Static Charge Damage in Computers[8]

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 through.
  - If ducts 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
  - Power systems used by information-processing equipment must be properly installed and correctly grounded.
  - 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
  - GFCI: capable of quickly identifying and interrupting a ground fault
  - Overloading a circuit can create a load exceeding electrical cable's rating, increasing the risk of overheating and fire.

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

- Uninterruptible power supply (UPS)
  - In case of power outage, UPS is the backup power source for major computing systems.
  - Basic UPS configurations:
    - Standby
    - Line-interactive
    - Standby online hybrid
    - Standby ferroresonant
    - Double conversion online
    - Data conversion online

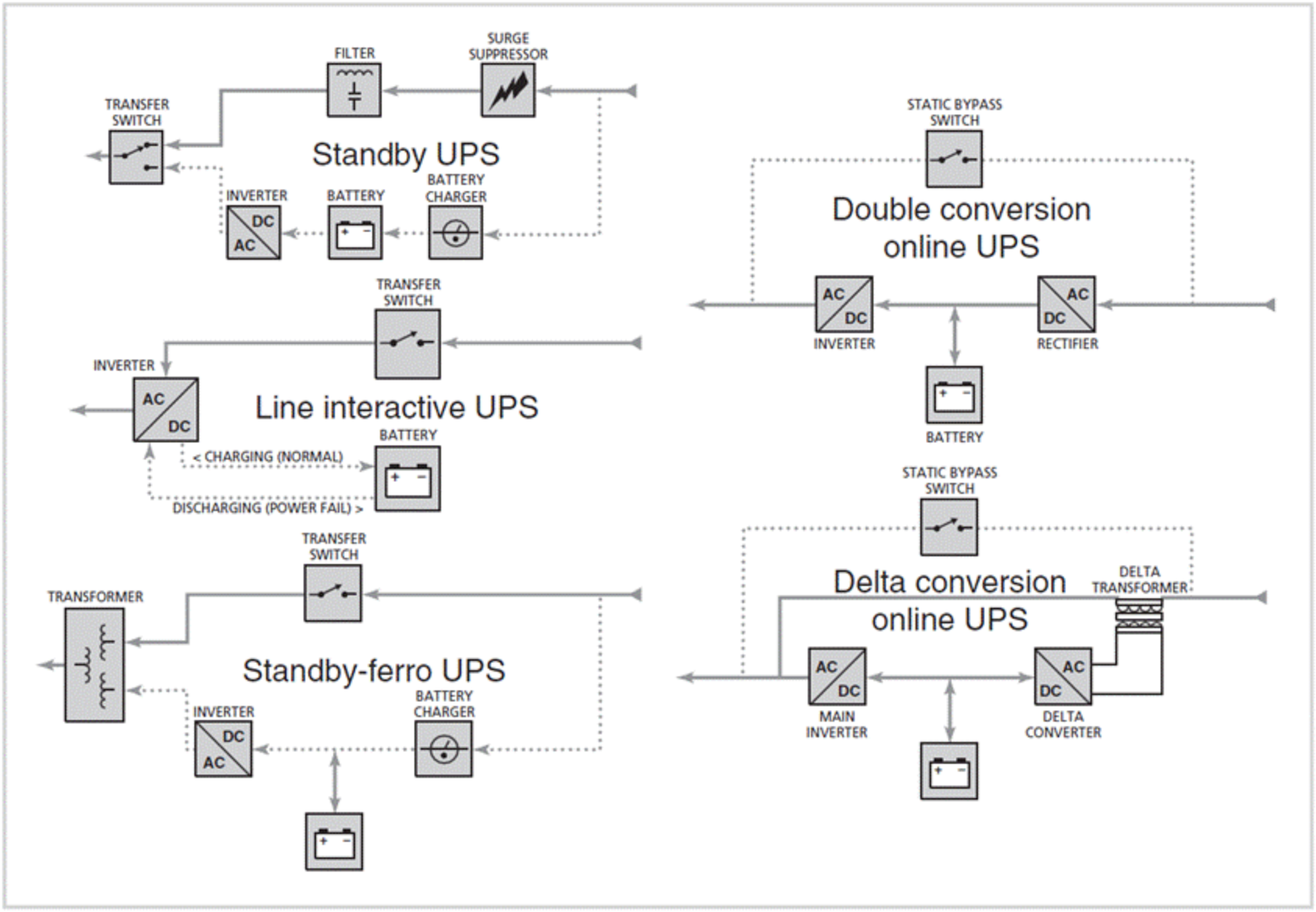


Figure 9-6 Types of uninterruptible power supplies[9]

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

- Emergency shutoff
  - Important aspect of power management is the ability to stop power immediately if the current represents 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 fire suppression and air-conditioning systems.
- 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 facility operations

Structural Collapse

- Unavoidable environmental factors/forces can cause failures in structures that house an organization.
- Structures are 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 standard operating procedures.
- Testing helps improve the facility's physical security and identify weak points.

Interception of Data

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

Securing Mobile and Portable Systems

- Mobile computing requires more security than typical computing infrastructures on the organization's premises.
- Many mobile computing systems
  - Have corporate information stored within them
  - Some are configured to facilitate user's access into organization's secure computing facilities.

Securing Mobile and Portable Systems (cont'd)

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

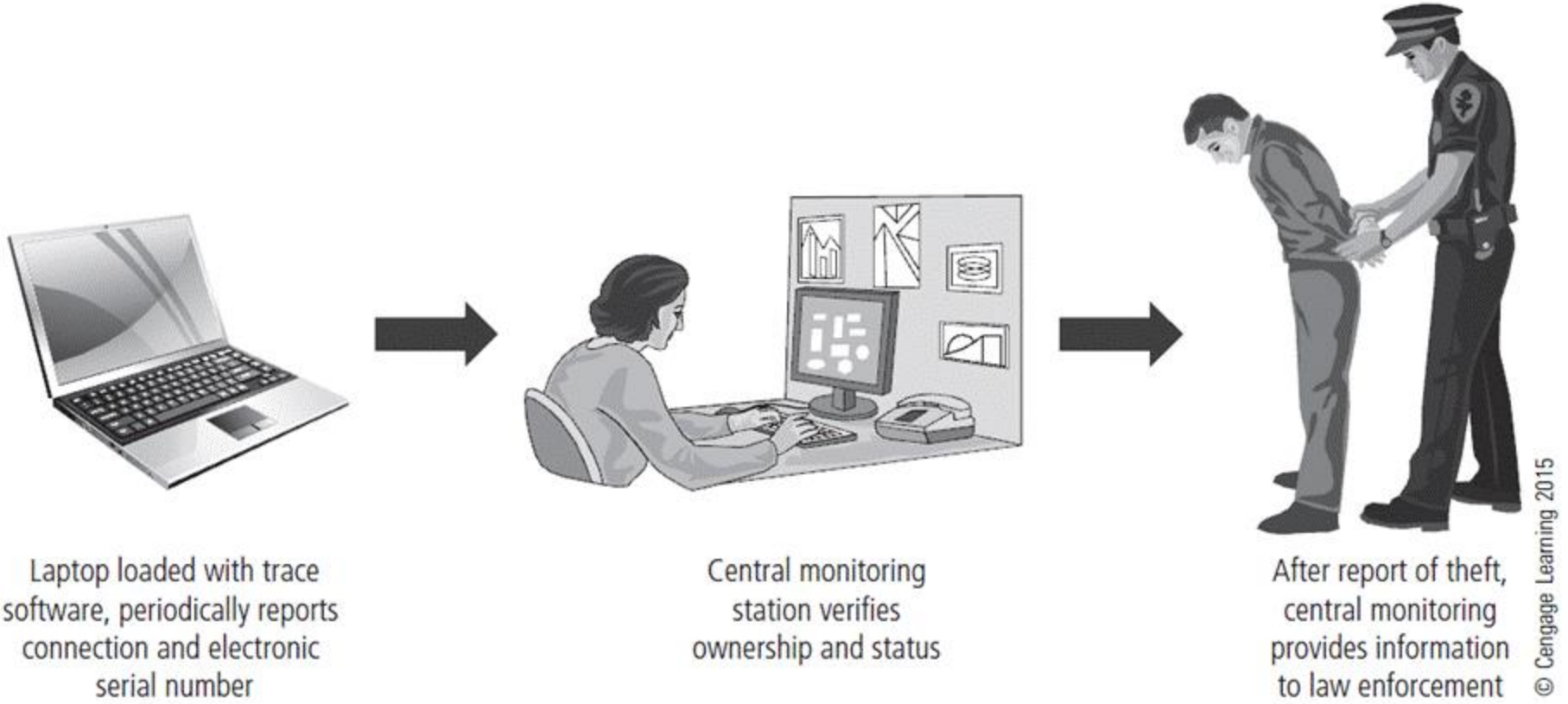


Figure 9-7 Laptop theft deterrence

Remote Computing Security

- Remote site computing involves variety of computing sites outside the organization's main facility.
- Telecommuting: off-site computing using 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.
- Telecommuter's computers must be made more secure than organization's systems.

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

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.

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