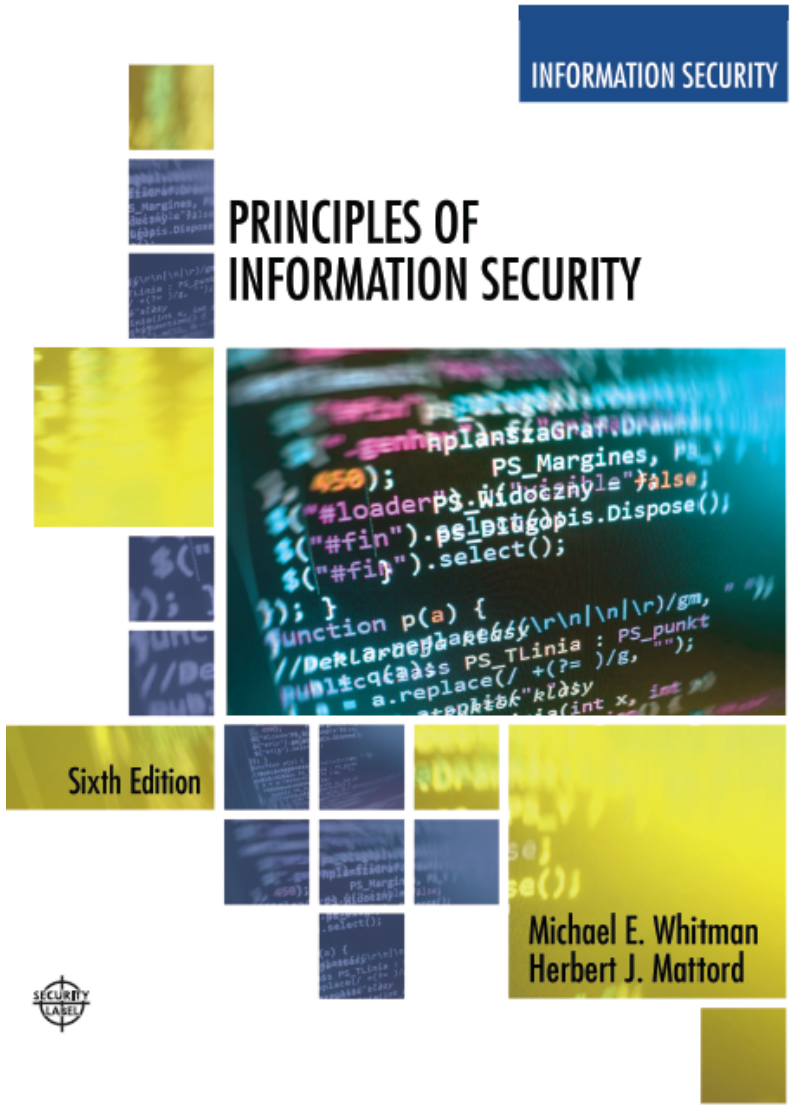


Source: Principles of Information Security

Chapter 9

Physical Security

Dr. Ibrahim Waziri Jr.

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. Physical security is as important as logical security.

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

Donn B. Parker's seven major sources of physical loss:

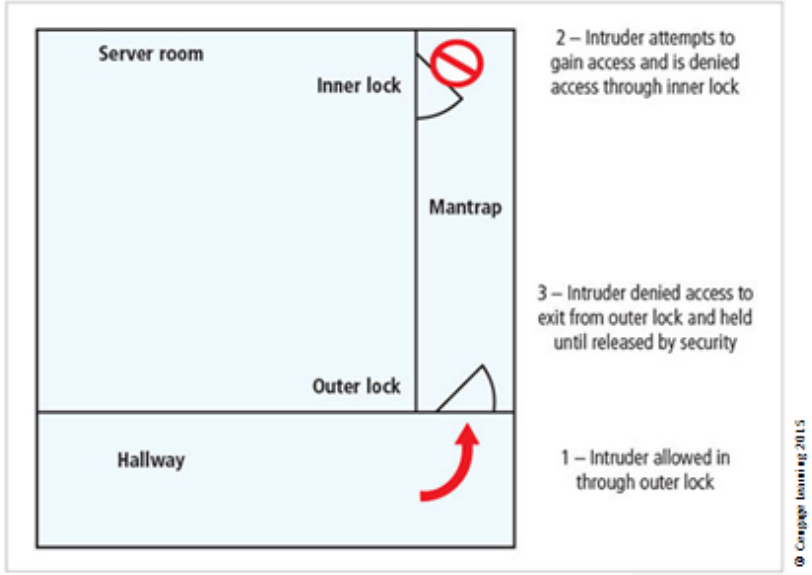
- Extreme temperature
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement
- Energy anomalies

Physical Access Controls

Secure facility: physical location with controls implemented to minimize the risk of attacks from physical threats.

Controls:

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



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.

Fire suppression systems: devices installed and maintained to detect and respond to a fire, potential fire, or combustion danger.

Flame point: temperature of ignition.

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

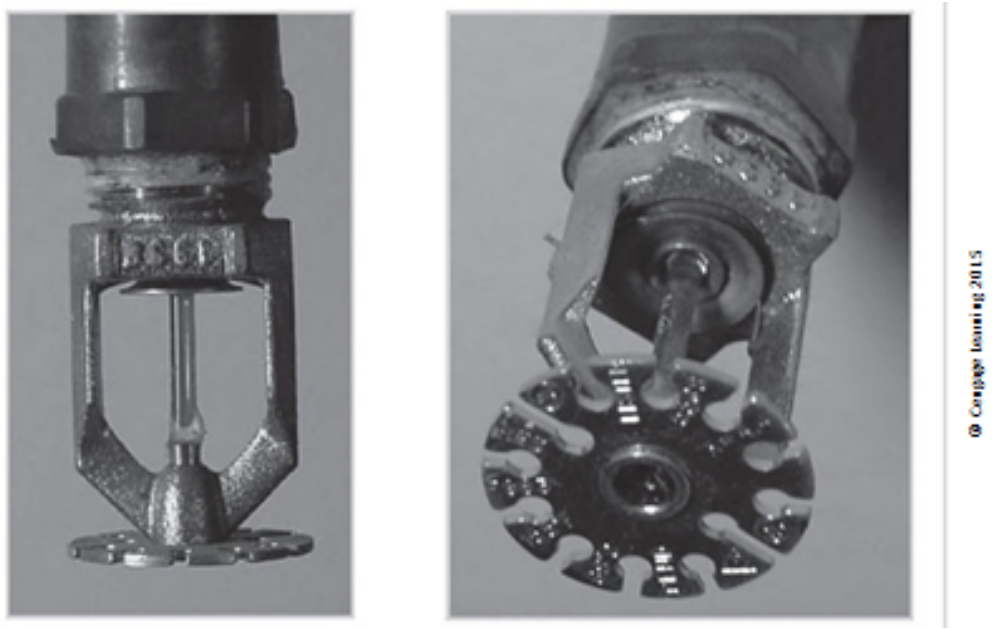
Fire suppression deny an environment of temperature, fuel, or oxygen: (Water and water mist systems, Carbon dioxide systems, Soda acid systems, and Gas-based systems)

- 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

Gaseous emission systems

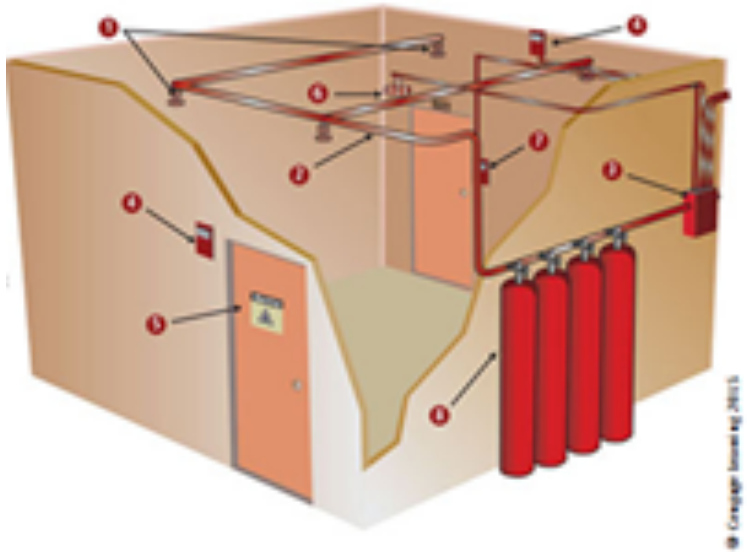
- Until recently, two types of systems: carbon dioxide and Halon
- Carbon dioxide removes fire's oxygen supply
- Halon is clean but has been classified as an ozone-depleting substance; new installations are prohibited

Fire Security and Safety



Water Sprinkler System

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, spaying water throughout the area



Gaseous Fire Suppression

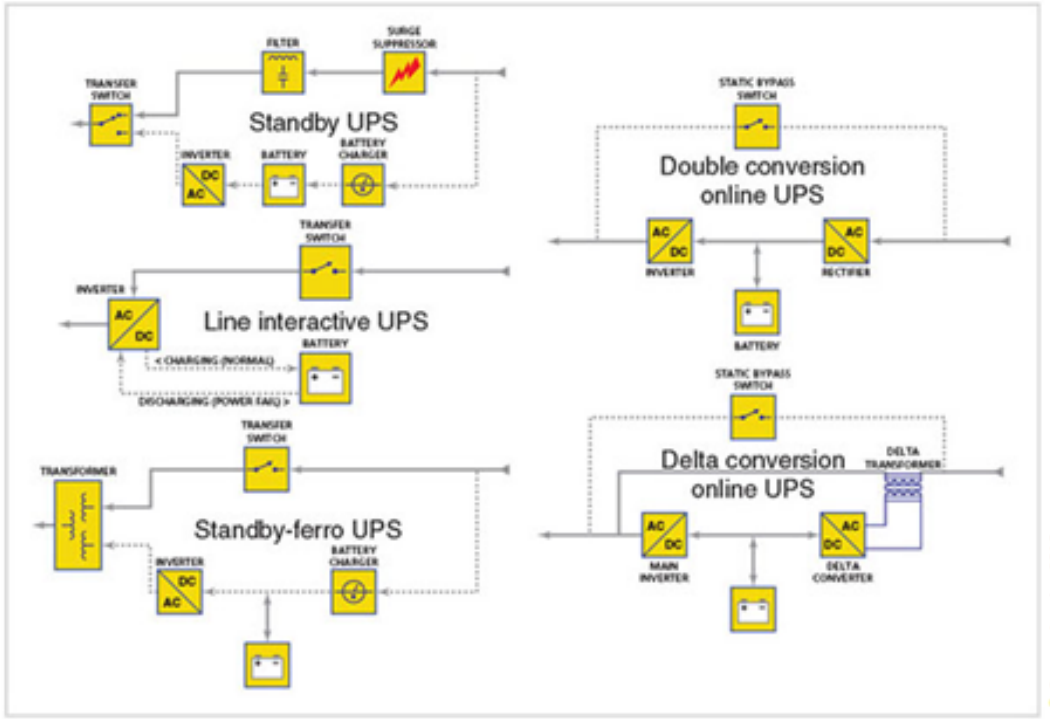
System Components:

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

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

- Ventilation shafts
- Power management and conditioning
- Grounding and amperage
- Uninterruptible power supply (UPS)
- Emergency shutoff



Types of UPS

Water Problems & Structural Collapse

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).

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.

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.

Data Interception/Securing Portable Systems

Three methods of data interception: Direct observation, Interception of data transmission and Electromagnetic interception - TEMPEST program reduce the risk of EMR monitoring.

- Remote site computing involves variety of computing sites outside the organization's main facility 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.
- CompuTrace software, stored on laptop; reports to a central monitoring center

Special Considerations for Physical Security Threats

- Develop physical security in-house or outsource?
- 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.

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