## 9 - Physical Security

## Physical Access Controls

* Physical security involves the protection of physical items, objects, or areas from unauthorized access and misuse.
* 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. Parkers 7 major sources of physical loss**
  + **Extreme temperature**: heat, cold
  + **Gases**
    - War gases
    - Commercial vapors
    - Humid or dry air
    - Suspended particles
  + **Liquids**
  + **Living organisms**
    - Viruses
    - Bacteria
    - People
    - Animals
    - Insects
  + **Projectiles**
    - Tangible objects in motion
    - Powered objects
  + **Movement**
    - Collapse
    - Shearing
    - Shaking
    - Vibration
    - Liquefaction
    - Flow waves
    - Separation
    - Slide
  + **Energy anomalies**
    - Electrical surge or failure
    - Magnetism
    - Static electricity
    - Aging circuitry
    - **Radiation**
      * Sound
      * Light
      * Radio
      * Microwave
      * Electromagnetic
      * atomic
* **Physical Security Controls**
  + 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
  + Walls, fencing, and gates
  + Guards
  + Dogs
  + ID cards and badges
  + Locks and keys
    - Manual
    - Programmable
    - Electronic
    - Biometric
    - Fail in two ways
      * Fail-safe lock
      * Fail-secure lock
  + 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
  + 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.
  + Alarms and alarm systems
    - Detect fire, intrusion, environmental disturbance, or an interruption in services.
    - Motion detectors
    - Thermal detectors
    - Contact and weight sensors
    - Vibration sensors.
  + Computer rooms and wiring closets
    - Require special attention to ensure confidentiality, integrity and availability of information
  + Interior walls and doors
    - High-security areas must have firewall-grade walls to provide physical security against potential intruders and fires.
    - Doors should be evaluated
      * Push or crash bars on computer rooms and closets

## Fire Security and Safety

* Fire Suppression systems work by denying an environment one of three elements for fire
  + Temperature (ignition source)
  + Fuel
  + Oxygen
  + Water and water mist
  + Carbon Dioxide systems
  + Soda acid systems
  + Gas-based systems
* **Fire Detection and Response**
  + **3 basic types of fire detection:**
    - Thermal detection systems
      * Fixed-temperature sensors
      * Rate-of-rise sensors
    - Smoke detection systems
    - Flame Detection
  + Photoelectric sensors
  + Ionizations sensors
  + Air-aspirating detectors
* **Fire Suppression.**
  + Class A
    - Ordinary combustible fuels: wood, paper, textiles, rubber, cloth, trash
    - Water and multipurpose dry chemical fire extinguishers.
  + Class B
    - Combustible liquids: solvents, gasoline, paint, lacquer, oil.
    - Extinguished by agents that remove oxygen from the fire.
      * Carbon Dioxide, multipurpose dry chemical, Halon fire.
  + Class C
    - Energized electrical equipment or appliances.
    - Extinguished with non-conducting agents.
      * Carbon dioxide, multipurpose dry chemical, halon.
  + Class D
    - Combustible metals: magnesium, lithium and sodium
    - Requires special extinguishing agents and techniques
  + Class K
    - Combustible cooking oil and fats in commercial kitchens.
    - Extinguished by special water mist, dry powder or CO2 agents.
  + Sprinkler systems
    - Activates between 140-145F
    - Wet-pipe systems
      * Contains pressurized water in all pipes and has some form of valve in each protected area.
      * Best used where a fire is a risk for people.
    - Dry-pipe systems
      * Designed to work in areas where electrical equipment is used.
      * Contains pressurized air until activated and fills with water.
      * Deluge systems
        + Keeps the pipes empty and all of the individual sprinkler heads open.
        + Water applied to all areas once activated
        + Can damage electrical equipment.
      * Pre-action system
        + 2-phase response

Fire detected, valves allow water to enter the system

Water is not activated until the heads are triggered.

Water only flows into the area of the activated sprinkler system.

* + - Water mist sprinklers
      * Ultra-fine mists instead of traditional shower-type systems
      * Lowers temperature around the flame.
      * Fog-like mist stays buoyant much longer.
      * Uses much less water
      * Extinguishes more quickly and causes less collateral damage
      * Less expensive, non-toxic than gaseous systems
  + Gaseous Emission Systems
    - Used to protect chemical and electrical processing areas as well as facilities that house computing systems
    - Self-pressurizing or pressurized with an additional agent.
    - System Components
      * Discharge nozzles
      * Piping
      * Control panel
      * Discharge or warning alarms
      * Hazard warning or caution signs
      * Automatic fire detection devices
      * Manual discharge station
      * Storage container(s) and extinguishing agent.
    - Types of gaseous systems
      * Carbon Dioxide
        + Removes the supply of oxygen
        + Not commonly used in residential or office environments with people.
      * Halon
        + Clean Agent

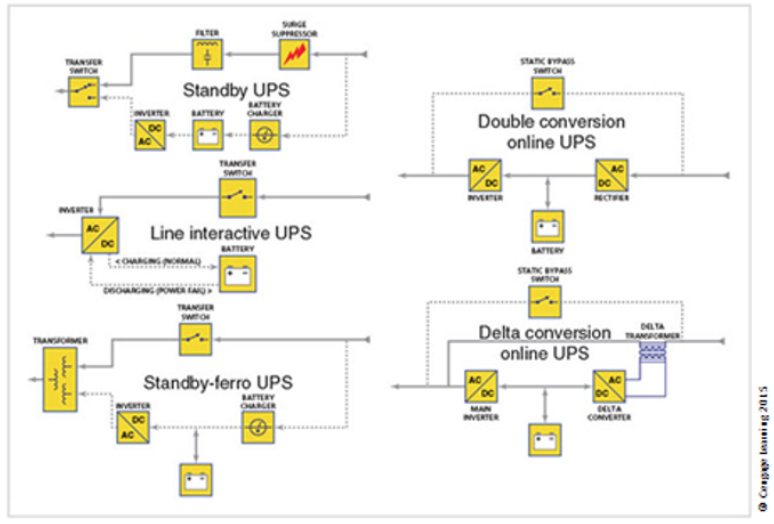
Does not leave any residue after use

Does not interfere with the operation of electric or electronic equipment.

* + - * + Dosage levels for suffocation much higher than CO2

But is ruled as Ozone depleting and not installed in commercial/residential buildings where people are expected to occupy.

## Failure of Supporting Utilities and Structural Collapse

* **HVAC**
  + Temperature and Filtration
    - 70-74F ideal temperature range for computer environments.
  + Humidity and Static Electricity.
    - High humidity creates condensation problems
    - Low humidity levels can increase the amount of static electricity in the environment.
  + Ventilation Shafts
    - Plenum riser more of a security risk than ventilation shafts.
* **Power Management and Conditioning**
  + Noise can interfere with internal clocks of computers.
  + Grounding and Amperage
    - Ground Fault Circuit Interruption (GFCI)
      * Anywhere water can accumulate.
    - Uninterruptible Power Supply
      * Protects against interruptions in the main power supply.
      * Basic UPS configurations
        + Standby
        + Line-interactive
        + Standby online hybrid
        + Standby ferroresonant
        + Double conversion online
        + Data conversion online
      * Types of UPS
        + Standby or Offline UPS

Offline battery backup that detects the interruption of power to equipment

Activates a transfer switch that provides power from batteries through a DC to AC converter until normal power is restored or computer is turned off.

Most cost-effective type of UPS

Limited run time

Slow time to switch from standby to active. (transfer delay too high for some sensitive computers.)

Do not have power conditioning.

Seldom used in critical systems.

* + - * + Standby ferroresonant UPS

Still an offline UPS.

Primary difference being the ferroresonant transformer that replaces the UPS transfer switch.

Transformer provides line filtering to the primary power sources

Reduces the effect of some power problems

Also reduces noise that may be present in the power source

Transformer has power stored in coils which provides a buffer to fill in the gap between interruption of service and the activation of an alternate source of power (battery typically)

* + - * + Line-interactive UPS
        + Double conversion online UPS

Primary power source is the inverter.

Power feed from utility is constantly charging the battery which powers the inverter.

Allows constant use of the system and eliminates power fluctuation

Considered top of the line and is the most expensive.

Generates a lot of heat

Constantly converts power from the utility’s AC feed to the DC used by the battery storage and then converts it back to AC for use by the system.

Delta Conversion UPS

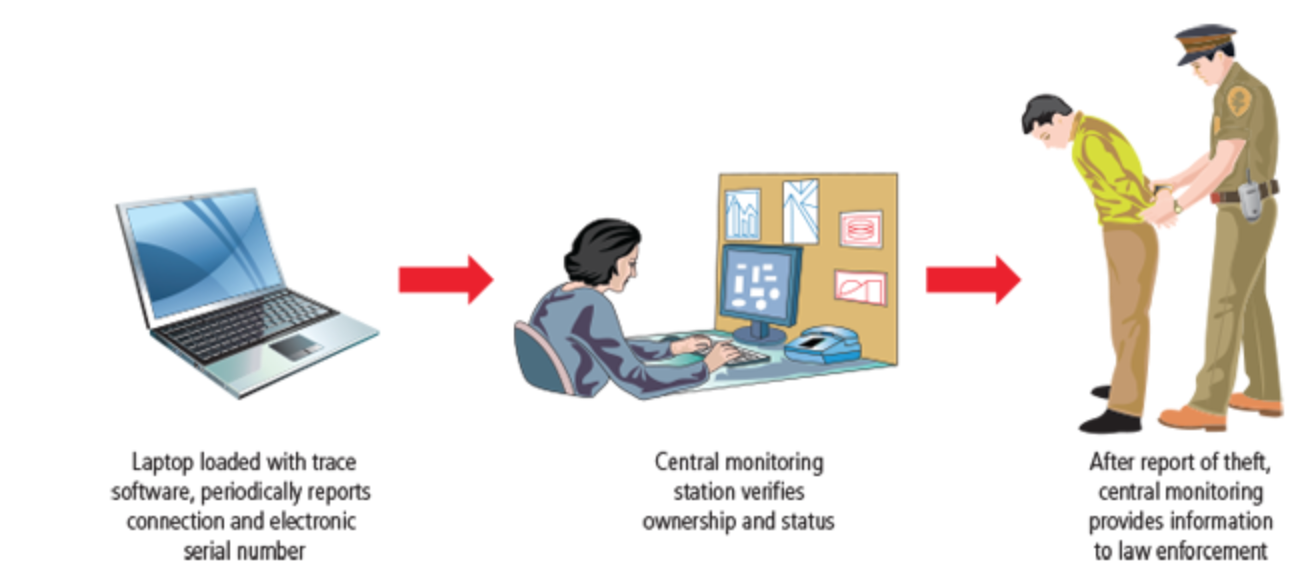
Incorporates a Delta-Conversion Unit

A device that resolves the previous issue by allowing some of the AC power to be used by the destination computers

Reduces the amount of energy wasted and heat generated.

* + - Emergency Shutoff
      * Must have the ability to stop power immediately
      * Most computer rooms and wiring closets are equipped with an emergency power shutoff
* Water Problems
  + Use water detection alarms
* Structural Collapse
  + Regular inspections with CE should be scheduled.
* 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

* **3 methods of data interception**
  + Direct observation
    - Requires that a person be close enough to the information to breach confidentiality.
    - Shoulder surfing
    - Worker taking documents home.
  + Interception of data transmission
    - Easier in the Internet Age
    - If attackers gain access to transmission media, location does not matter.
    - Packet sniffers
    - Tapping of LAN ports
    - Wireless wiretapping is not illegal (only cell phone communication)
  + Electromagnetic interception
    - EMR (Electromagnetic Radiation) can be detected
    - TEMPEST is a program to combat EMR interception
    - Mostly an urban myth, but possible. (not reliable)

Securing Mobile and Portable Systems

* Remote Computing Security
  + Variety of computing sites outside the organizations 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 organizations systems
* 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

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.

Chapter Summary

* Physical security requires the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization.
* Many threats to information security can also be classified as threats to physical security. An organization’s policy should guide the planning for physical security throughout the development life cycle.
* In facilities management, a secure facility is a physical location that has controls to minimize the risk of attacks from physical threats. A secure facility can use natural terrain, traffic flow, and urban development, and can complement these environmental elements with protection mechanisms, such as fences, gates, walls, guards, and alarms.
* The management of keys and locks is a fundamental part of general management’s responsibility for the organization’s physical environment.
* A fail-safe lock is typically used on an exit door when human safety in a fire or other emergency is the essential consideration. A fail-secure lock is used when human safety is not a factor.
* Monitoring equipment can record events that guards and dogs might miss, and can be used in areas where other types of physical controls are not practical.
* As with any phase of the security process, the implementation of physical security must be constantly documented, evaluated, and tested. Once the physical security of a facility is established, it must be diligently maintained.
* Fire detection systems are devices that detect and respond to a fire or potential fire. Fire suppression systems stop the progress of a fire once activated.
* The three basic types of fire detection systems are thermal detection, smoke detection, and flame detection.
* Four environmental variables controlled by HVAC systems can cause damage to information systems: temperature, filtration, humidity, and static electricity.
* Computer systems depend on stable power supplies to function; when power levels are too high, too low, or too erratic, computer circuitry can be damaged or destroyed. The power provided to computing and networking equipment should contain no unwanted fluctuations and no embedded signaling.
* Water problems and the weakening and subsequent failure of a building’s physical structure represent potential threats to personal safety and to the integrity and availability of information assets.
* Data can be intercepted electronically and manually. The three routes of data interception are direct observation, interception of data transmission, and interception of electromagnetic radiation.
* TEMPEST is a technology that prevents the possible loss of data from the emission of electromagnetic radiation (EMR).
* With the increased use of laptops, handhelds, and PDAs, organizations should be aware that mobile computing requires even more security than the average in-house system.
* Remote site computing requires a secure extension of the organization’s internal networks and special attention to security for any connected home or off-site computing technology.
* Like computing equipment, classified information should be inventoried and managed. If multiple copies are made of a classified document, they should be numbered and tracked.

Review Questions

1. What is physical security? What are the primary threats to physical security? How are they manifested in attacks against the organization?
2. What are the roles of an organization’s IT, security, and general management with regard to physical security?
3. How does physical access control differ from logical access control, which is described in earlier chapters? How are they similar?
4. Define a secure facility. What is the primary objective of designing such a facility? What are some secondary objectives of designing a secure facility?
5. Why are guards considered the most effective form of control for situations that require decisive action in the face of unfamiliar stimuli? Why are they usually the most expensive controls to deploy? What is another issue with human guards, beyond the high cost? When should dogs be used for physical security?
6. List and describe the four categories of locks. In which situation is each type of lock preferred?
7. What are the two possible modes of locks when they fail? What implications do these modes have for human safety? In which situation is each preferred?
8. What is a mantrap? When should it be used?
9. What is the most common form of alarm? What does it detect? What types of sensors are commonly used in this type of alarm system?
10. Describe a physical firewall that is used in buildings. List reasons that an organization might need a firewall for physical security controls.
11. What is considered the most serious threat within the realm of physical security? Why is it valid to consider this threat the most serious?
12. What three elements must be present for a fire to ignite and continue to burn? How do fire suppression systems manipulate the three elements to quell fires?
13. List and describe the three fire detection technologies covered in the chapter. Which is the most commonly used?
14. List and describe the four classes of fire described in the text. Does the class of the fire dictate how to control it?
15. What is Halon and why is its use restricted?
16. What is the relationship between HVAC and physical security? What four physical characteristics of the indoor environment are controlled by a properly designed HVAC system? What are the optimal temperature and humidity ranges for computing systems?
17. List and describe the four primary types of UPS systems. Which is the most effective and the most expensive, and why?
18. What two critical factors are affected when water is not available in a facility? Why are they important to the operation of the organization’s information assets?
19. List and describe the three fundamental ways that data can be intercepted.  
    How does a physical security program protect against each of these data interception methods?
20. What can you do to reduce the risk of theft of portable computing devices, such as smartphones, tablets, and notebooks?