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 chapter you should be able to:

- Understand the conceptual need for physical security.
- Identify threats to information security that are unique to physical security.
- Describe the key physical security considerations for selecting a facility site.
- Identify physical security monitoring components.
- Grasp the essential elements of access control within the scope of facilities management.
- Understand the criticality of fire safety programs to all physical security programs.
Learning Objectives:

Upon completion of this chapter you should be able to:

– Describe the components of fire detection and response.
– Grasp the impact of interruptions in the service of supporting utilities.
– Understand the technical details of uninterruptible power supplies and how they are used to increase availability of information assets.
– Discuss critical physical environment considerations for computing facilities.
– Discuss countermeasures to the physical theft of computing devices.
Seven Major Sources of Physical Loss

- Temperature extremes
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement
- Energy anomalies
Community Roles

• General management:
  – responsible for the security of the facility

• IT management and professionals:
  – responsible for environmental and access security

• Information security management and professionals:
  – perform risk assessments and implementation reviews
Access Controls

There are a number of physical access controls that are uniquely suited to the physical entry and exit of people to and from the organization’s facilities, including

– biometrics
– smart cards
– wireless enabled keycards
Facilities Management

• A secure facility is a physical location that has been engineered with controls designed to minimize the risk of attacks from physical threats.

• A secure facility can use the natural terrain; traffic flow, urban development, and can complement these features with protection mechanisms such as fences, gates, walls, guards, and alarms.
Controls for Protecting the Secure Facility

- Walls, Fencing, and Gates
- Guards
- Dogs, ID Cards, and Badges
- Locks and Keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors
ID Cards and Badges

• Ties physical security to information access with identification cards (ID) and/or name badges
  – ID card is typically concealed
  – Name badge is visible

• These devices are actually biometrics (facial recognition)

• Should not be the only control as they can be easily duplicated, stolen, and modified

• Tailgating/piggybacking occurs when unauthorized individuals follow authorized users through the control
Locks and Keys

• There are two types of locks
  – mechanical and electro-mechanical

• Locks can also be divided into four categories
  – manual, programmable, electronic, and biometric

• Locks fail and facilities need alternative procedures for access

• Locks fail in one of two ways:
  – when the lock of a door fails and the door becomes unlocked, that is a fail-safe lock
  – when the lock of a door fails and the door remains locked, this is a fail-secure lock
Figure 9-1  Locks

Programmable/mechanical

Biometric

Electronic

Biometric image courtesy of the BioThentica Corporation
Mantraps

• An enclosure that has an entry point and a different exit point
• The individual enters the mantrap, requests access, and if verified, is allowed to exit the mantrap into the facility
• If the individual is denied entry, they are not allowed to exit until a security official overrides the automatic locks of the enclosure
Figure 9-2 Mantraps

1 - Intruder allowed in through outer lock

2 - Intruder attempts to gain access and is denied access through inner lock

3 - Intruder denied access to exit from outer lock and held until released by security
Electronic Monitoring

• Records events where other types of physical controls are not practical

• May use cameras with video recorders

• Drawbacks:
  – reactive and do not prevent access or prohibited activity
  – recordings often not monitored in real time and must be reviewed to have any value
Alarms and Alarm Systems

• Alarm systems notify when an event occurs
• Used for fire, intrusion, environmental disturbance, or an interruption in services
• These systems rely on sensors that detect the event: motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors
Computer Rooms and Wiring Closets

• Computer rooms and wiring and communications closets require special attention
• Logical controls are easily defeated, if an attacker gains physical access to the computing equipment
• Custodial staff are often the least scrutinized of those who have access to offices and are given the greatest degree of unsupervised access
Interior Walls and Doors

• The walls in a facility are typically either:
  – standard interior
  – firewall

• All high-security areas must have firewall grade walls to provide physical security from potential intruders and improves the facility's resistance to fires

• Doors that allow access into secured rooms should also be evaluated

• Computer rooms and wiring closets can have push or crash bars installed to meet building codes and provide much higher levels of security than the standard door pull handle
Fire Safety

• The most serious threat to the safety of the people who work in the organization is the possibility of fire

• Fires account for more property damage, personal injury, and death than any other threat

• It is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards
Fire Detection and Response

• Fire suppression systems are devices installed and maintained to detect and respond to a fire

• They work to deny an environment of one of the three requirements for a fire to burn: heat, fuel, and oxygen
  – Water and water mist systems reduce the temperature and saturate some fuels to prevent ignition
  – Carbon dioxide systems rob fire of its oxygen
  – Soda acid systems deny fire its fuel, preventing spreading
  – Gas-based systems disrupt the fire’s chemical reaction but leave enough oxygen for people to survive for a short time
Fire Detection

• Before a fire can be suppressed, it must be detected
• Fire detection systems fall into two general categories:
  – manual and automatic
• Part of a complete fire safety program includes individuals that monitor the chaos of a fire evacuation to prevent an attacker accessing offices
• There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection
  – Smoke detectors operate in one of three ways: photoelectric, ionization, and air-aspirating
Fire Suppression

• Can be portable, manual, or automatic

• Portable extinguishers are rated by the type of fire:
  – Class A: fires of ordinary combustible fuels
  – Class B: fires fueled by combustible liquids or gases
  – Class C: fires with energized electrical equipment
  – Class D: fires fueled by combustible metals

• Installed systems apply suppressive agents, either sprinkler or gaseous systems
  – Sprinkler systems are designed to apply liquid, usually water
  – In sprinkler systems, the organization can implement wet-pipe, dry-pipe, or pre-action systems
  – Water mist sprinklers are the newest form of sprinkler systems and rely on microfine mists
When the ambient temperature reaches 140-150°F, the plastic pin melts, releasing the stopper and allowing water to hit the diffuser spraying water throughout the area.
Gaseous Emission Systems

• Until recently there were only two types of systems – carbon dioxide and halon
• Carbon dioxide robs a fire of its oxygen supply
• Halon is a clean agent but has been classified as an ozone-depleting substance, and new installations are prohibited
• Alternative clean agents include the following:
  – FM-200
  – Inergen
  – Carbon dioxide
  – FE-13 (trifluromethane)
Figure 9-4 Fire Suppression System
Failure of Supporting Utilities and Structural Collapse

• Supporting utilities, such as heating, ventilation and air conditioning, power, water, and other utilities, have a significant impact on the continued safe operation of a facility.

• Extreme temperatures and humidity levels, electrical fluctuations and the interruption of water, sewage, and garbage services can create conditions that inject vulnerabilities in systems designed to protect information.
Heating, Ventilation, & Air Conditioning

- HVAC system areas that can cause damage to information systems:
  - Temperature
    - Computer systems are subject to damage from extreme temperature
    - The optimal temperature for a computing environment (and people) is between 70 and 74 degrees Fahrenheit
  - Filtration
  - Humidity
  - Static
    - One of the leading causes of damage to sensitive circuitry is electrostatic discharge (ESD)
    - A person can generate up to 12,000 volts of static current by walking across a carpet
Ventilation Shafts

• Security of the ventilation system air ductwork:
  – While in residential buildings the ductwork is quite small, in large commercial buildings it can be large enough for an individual to climb through
  – If the vents are large, security can install wire mesh grids at various points to compartmentalize the runs
Power Management and Conditioning

• Electrical quantity (voltage level and amperage rating) is a concern, as is the quality of the power (cleanliness and proper installation)
• Any noise that interferes with the normal 60 Hertz cycle can result in inaccurate time clocks or unreliable internal clocks inside the CPU
• Grounding
  – Grounding ensures that the returning flow of current is properly discharged
  – If this is not properly installed it could cause damage to equipment and injury or death to the person
• Overloading a circuit not only causes problems with the circuit tripping but can also overload the power load on an electrical cable, creating the risk of fire
Uninterruptible Power Supplies (UPSes)

• In case of power outage, a UPS is a backup power source for major computer systems
• There are four basic configurations of UPS:
  – the standby
  – ferroresonant standby
  – line-interactive
  – the true online
Uninterruptible Power Supplies (UPSs)

- A standby or offline UPS is an offline battery backup that detects the interruption of power to the power equipment.
- A ferroresonant standby UPS is still an offline UPS
  - the ferroresonant transformer reduces power problems.
- The line-interactive UPS is always connected to the output, so has a much faster response time and incorporates power conditioning and line filtering.
- The true online UPS works in the opposite fashion to a standby UPS since the primary power source is the battery, with the power feed from the utility constantly recharging the batteries
  - this model allows constant feed to the system, while completely eliminating power quality problems.
Emergency Shutoff

• One important aspect of power management in any environment is the need to be able to stop power immediately should the current represent a risk to human or machine safety

• Most computer rooms and wiring closets are equipped with an emergency power shutoff, which is usually a large red button, prominently placed to facilitate access, with an accident-proof cover to prevent unintentional use
Electrical Terms

- Fault: momentary interruption in power
- Blackout: prolonged interruption in power
- Sag: momentary drop in power voltage levels
- Brownout: prolonged drop in power voltage levels
- Spike: momentary increase in power voltage levels
- Surge: prolonged increase in power voltage levels
Water Problems

- Lack of water poses problems to systems, including the functionality of fire suppression systems, and the ability of water chillers to provide air-conditioning
- On the other hand, a surplus of water, or water pressure, poses a real threat
- It is therefore important to integrate water detection systems into the alarm systems that regulate overall facilities operations
Structural Collapse

• Unavoidable forces can cause failures of structures that house the organization

• Structures are designed and constructed with specific load limits, and overloading these design limits, intentionally or unintentionally, inevitably results in structural failure and potentially loss of life or injury

• Periodic inspections by qualified civil engineers assists in identifying potentially dangerous structural conditions well before they fail
Testing Facility Systems

• Physical security of the facility must be constantly documented, evaluated, and tested

• Documentation of the facility’s configuration, operation, and function is integrated into disaster recovery plans and standing operating procedures

• Testing provides information necessary to improve the physical security in the facility and identifies weak points
Interception of Data

• There are three methods of data interception:
  – Direct observation
  – Data transmission
  – Eavesdropping on signals
    • TEMPEST is a technology that involves the control of devices that emit electromagnetic radiation such that the data cannot be reconstructed

• There are also *side-channel attacks* that monitor keystroke acoustics, screen displays, etc.
Mobile and Portable Systems

• With the increased threat to overall information security for laptops, handhelds, and PDAs, mobile computing requires even more security than the average in-house system.

• Many of these mobile computing systems not only have corporate information stored within them, many are configured to facilitate the user’s access into the organization’s secure computing facilities.
Stopping Laptop Losses

- Controls support the security and retrieval of lost or stolen laptops
  - CompuTrace is stored on a laptop’s hardware and reports to a central monitoring center
  - Burglar alarms made up of a PC card that contains a motion detector
    - If the laptop alarm is armed, and the laptop is moved beyond a configured distance, the alarm triggers an audible alarm
    - The system also shuts down the computer and includes an encryption option to completely render the information unusable
  - BitLocker (Windows Vista+), FileVault (OS X), home directory encryption (Linux)
**Figure 9-6** Laptop Theft Deterrence

1. Laptop loaded with trace software
2. Laptop periodically reports connection and electronic serial number
3. Central monitoring station verifies ownership
4. Stolen computer information passed to law enforcement
Remote Computing Security

- Remote site computing – distant from the 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 a secure extension of the 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 physical security includes gaining the experience and knowledge of these agencies
  – Downside includes high expense, *loss of control* over the individual components, and the *level of trust* that must be placed in another company

• Social engineering is the use of people skills to obtain information from employees
  – For more info see Kevin Mitnick’s *The Art of Deception*
Inventory Management

• Computing equipment should be inventoried and inspected on a regular basis

• Classified information should also be inventoried and managed
  – Whenever a classified document is reproduced, a stamp should be placed on the original before it is copied
  – This stamp states the document’s classification level and document number for tracking
  – Each classified copy is issued to its receiver, who signs for the document
Summary

• Physical security complements information security – it’s just as important!
  – Controls include locks & keys, ID badges, biometrics, etc.
  – Monitoring, intrusion detection via alarms, electronic systems
  – Utilities management (electrical, AC, etc.) and structural integrity concerns
  – Fire detection/suppression are crucial
  – Data loss prevention & secure remote computing
  – Laptop/mobile device inventory, management, and security