Protecting Information Assets
- Week 7 -

Physical and Environmental Security

MIS5206 Week 7

- In the News
- Readings
- Review Mid-Term Exam
- Physical and Environmental Security
- Test Taking Tip
- Quiz

In the News

- I will lead a discussion of one of your “in the news” article

Reading

- Vacca - Homeland Security
  2009 Chapter 38
  2012 Chapter 38
- SANS Assignment 3

Team Presentation

Team presentation: PCI DSS

Business focus: DONGXUE XU

Technical focus: ANDREA BLANCO

Risk Assessment focus: WEN CHUNG,

Risk Mitigation focus: WENHANG LU

Physical and Environmental Security

Physical security addresses the physical protection of the resources of an organization, which include people, data, facilities, equipment, systems, etc. It concerns with people safety, how people can physically enter an environment and how the environmental issues affect equipment and systems. People safety always takes precedence over the other security factors.

Physical Control Types

Administrative Controls	Facility selection, facility construction and management, personnel control, evacuation procedure, system shutdown procedure, fire suppression procedure, handling procedures for other exceptions such as hardware failure, bomb threats
Physical Controls	Facility construction material, key and lock, access card and reader, fences, lighting
Technical Controls	Physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup

Sources of Physical Threats

- ***Weather*** *- temperature, humidity, water, flood, wind, snow, lightening*
- ***Fire and Chemical*** *- explosion, smoke, toxic material, industrial pollution*
- ***Earth Movement*** *- earthquake, volcano, mud slide*
- ***Object Movement*** *- building collapse, falling object, car, truck, plane*
- ***Energy*** *- electricity, magnetism, radio wave anomalies*
- ***Equipment*** *- mechanical or electronic component failure*
- ***Organism*** *- virus, bacteria, animal, insect*
- ***Human*** *- strike, war, sabotage*

Facilities – Site Selection

- **Visibility** - surrounding terrain, markings and signs
- **Local Considerations** - crime rate, adjacent neighbors, proximity to police and fire station
- **Transportation** - road access and traffic condition, proximity to airport and train station
- **Natural Threats** - likelihood of flood, earthquake, or other natural threats.

Facilities – Data Center

- Should not be located on the top floor because of risk of fire
- Should not be in the basement - flooding risk
- Ideally in the core of a building - provides protection from natural disasters and intrusion
- Should not be close to a public area – to ease security

Design Considerations

Walls - fire rating (level of fire protection and combustibility), load (the maximum weight it can hold), floor to ceiling barrier, reinforcement for secured area.

Partitions – considerations similar to those of wall, plus the requirement of extension above drop ceiling (if there is no extension, an intruder can lift the ceiling panels and climb above the partition).

Doors – fire rating (should be equal to that of the surrounding walls), emergency marking, directional opening, resistance from being forced open, intrusion detection alarm, fail-soft vs fail-safe lock (i.e. lock that is unlocked or locked in a power outage), placement of doors.

Windows – characteristics of windows material (opaque, translucent, transparent,shatterproof, bulletproof), intrusion detection alarm, placement of windows.

Ceilings – fire rating, load, waterproof (preventing water leakage from the upper floor), drop ceiling.

Floor – fire rating, load, raised floor, electrical grounding (for raised floor), non-conducting material.

Heating, ventilation, and air conditioning (HVAC) – independent power source, positive air pressure to avoid contamination of the room, protected intake vents to prevent tampering, monitoring of environmental condition, emergency power off, placement of HVAC

Power supplies – backup power supply, clean power supply, circuit breaker, access to power distribution panels, placement of power sockets.

Liquid and gas lines – shutoff valve, positive flow, leakage sensor, placement of liquid and gas lines.

Fire detection and suppression – fire or smoke detector and alarm, sprinkler, gas discharge system, placement of detectors and sprinkler heads.

Emergency lighting – essential power supply and battery for emergency lighting

Perimeter Security

- Perimeter security controls are used to prevent unauthorized access to a facility. They deal with access control, auditing and monitoring, intrusion detection and response

- The perimeter security requirements when a facility is in operation should be different from those when the facility is closed

Access Control and Auditing

Physical access control mechanisms include:

- Lock and key
- Access card and reader
- Fence
- Lighting
- Doorway and Man-trap

Perimeter Control

Fencing is another physical access control mechanism. Fences of different heights can serve different purposes:

- 3 – 4 feet – deter casual trespassers
- 6 – 7 feet – deter general intruders
- 8 feet with strands of barbed wire (slant at a 45 angle) to deter more determined intruders

PIDAS - Perimeter intrusion and detection assessment system is a fencing system with mesh wire and passive cable vibration sensors that can detect if an intruder is approaching and damaging the fence. However, it may generate many false alarms.

Bollards are small and round concrete pillars that are constructed and placed around a building to protect it from being damaged by someone running a vehicle into the side of the building.

Lighting - streetlight, floodlight or searchlight is a good deterrent for unauthorized access. It can also provide safety for personnel. The National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power.

Physical Access Monitoring

- **Patrol force / security guard**
  - Good deterrent to intrusion
  - Can provide flexible security and safety response
  - Can be expensive.
  - Reliability of security guards is an issue.
  - Re-employment screening and other background checking are required.
  - Training against social engineering is

- **Dogs**
  - Very effective in detecting intruders
  - They are loyal, intelligent
  - Can be trained to recognize specific smells like smoke, for instance

Technical Access Monitoring Controls

Dry contact switch - uses metallic foil tape as a contact detector to detect whether a door or window is opened.

Electro-mechanical detection system - detects a change or break in a circuit. It can be used as a contact detector to detect whether a door or window is opened.

Vibration detection system - detects movement on walls, ceiling, floors by vibration.

Pressure mat - detects whether there is someone stepping on the mat.

Visual recording device - Camera and Closed Circuit TV (CCTV), records the activities taking place in a particular area. It should be used together with security guards to detect for anomalies.

Technical Access Monitoring Controls

Photoelectric or photometric detection system - emits a beam of light and monitors the beam to detect for motion and break-in.

Wave pattern motion detector - generates microwave or ultrasonic wave, and monitors the emitted wave to detect for motion.

Passive infrared detection system - detects for changes of heat wave generated by an intruder.

Audio or Acoustical-seismic detection system - listens for changes in noise level.

Proximity detector or capacitance detector - emits magnetic field and monitors the field to detect for any interruption. It is especially useful for protecting specific objects.

Fire Protection

Combustion elements which can sustain a fire are:

Fuel - wood, paper, wiring, etc. - can be suppressed by CO2 or Soda acid

Oxygen - can be suppressed by CO2 or Soda acid

Temperature - can be reduced by water

Chemical - can be suppressed by Halon, which interferes with the chemical reaction

Fire Protection

The 4 classes of fire are:

Class	Description	Element of fire	Suppression method
A	Common combustibles	Miscellaneous, e.g. wood, paper, etc.	Water, Soda acid
B	Liquid	Petroleum products, coolants, etc.	Halon, CO_2, Soda acid
C	Electrical	Electrical equipment, wires, etc.	Halon, CO_2
D	Combustible metal	Magnesium, sodium, etc.	Dry powder

Power Protection

Uninterrupted Power Supply (UPS) to protect against a short duration power failure.

There are two types of UPS:

- Online UPS – It is in continual use because the primary power source goes through it to the equipment. It uses AC line voltage to charge a bank of batteries. When the primary power source fails, an inverter in the UPS will change DC of the batteries into AC.
- Standby UPS – It has sensors to detect for power failures. If there is a power failure, the load will be switched to the UPS. It stays inactive before a power failure, and takes more time than online UPS to provide power when the primary source fails.

Power Protection

Backup power source to protect against a long duration power failure, e.g. motor generator, another electrical substation, etc.

Voltage regulator and line conditioner to protect against unstable power supply.

Proper grounding for all electrical devices to protect against short circuit and static electricity, e.g. by using 3-prong outlets.

Cable shielding to avoid interference.

Power line monitor to detect for changes in frequency and voltage amplitude.

Emergency power off (EPO) switch to shut down the power quickly when required.

Electrical cables should be:

- placed away from powerful electrical motors and lighting to avoid electromagnetic interference.
- placed away from powerful electrical cables and fluorescent lighting to avoid radio frequency interference.

Test Taking Tip

Keep track of your guesses

- OK to guess and move on if you don't know answer
- Often in a standardized test, later questions on the same topic appear
- Remembering where you saw that topic earlier and if you guessed at the answer can make that information valuable

Quiz