PART A
LECTURE 4
ENVIRONMENTAL SECURITY

Physical & Environmental Security

- Physical security is extremely important. There is no point in technical and administrative security controls if someone can simply bypass them from physically accessing systems.

  - Physical security is harder today as systems are more distributed (not just mainframes) and complex.
  - Not just about protecting data, but more importantly PEOPLE! (remember safety is always issues #1*)
  - Often physical security is an afterthought when building new facilities. ☹
  - Lawsuits against companies CAN be filed if a company does not take adequate physical security measures.

Threats to Physical Security

- Natural hazards (floods, tornadoes, fires, temperatures)
- Supply system threats (power outage, water, gas, WAN connection etc)
- Manmade threats (unauthorized access, explosives, damage by disgruntled people, accidents, theft)
- Politically motivated threats (strikes, riots, civil disobedience)

Physical Security Fundamentals

- Life safety goals* should always be #1 priority
- Defense should be layered which means that different physical controls should work together to accomplish the goal of security. (examples)
- Physical security can address all of the CIA fundamental principals.

Physical Security Fundamentals

- Life safety goals* should always be #1 priority
- Defense should be layered which means that different physical controls should work together to accomplish the goal of security. (examples)
- Physical security can address all of the CIA fundamental principals.

Planning Process

- Threats should be classified as internal or external.
- Risk analysis should be taken on a physical aspect. Assets should be identified, threats should be identified (probabilities calculated) and countermeasures put in place that are COST EFFECTIVE and appropriate to the level of security needed.
- Physical security will ultimately be a combination of people, processes, procedures and equipment to protect resources.

Planning Process

The planning and security program should include the following goals:

- Deterrence – fences, guards, signs
- Reducing/Avoiding damage by Delaying attackers – slow down the attackers (locks, guards, barriers)
- Detection – motion sensors, smoke detectors
- Incident assessment – response of guards, and determination of damage level
- Response procedures – fire suppression, law enforcement notification etc

Planning Process

- Idea is to avoid problems if at all possible, otherwise mitigate problems.
- This can be best accomplished by layering (which we already talked about).
- If a crime happens you must be able to detect it, and response should be implemented.
- Remember this is the same process that we cover in Rink Analysis! All the same processes and concepts apply.

Designing Physical Security (examples)

COMPUTER ROOM

Computer rooms are where important servers and network equipment is stored. Thus:

- Equipment should be placed in locked racks.
- Computer rooms should be near the center of the building, and should be above ground, but not too high that it would be difficult to access by emergency crews.
- Strict access control should be enabled.
- They should only have 1 access door, though they might have to have multiple fire doors.

Designing Physical Security (examples)

PROTECTING ASSETS

Companies must protect from theft. Theft of laptops is a big deal especially if private information is on the laptop. You should understand best practices in regards to physically protecting things from being stolen.

- Inventory all laptops including serial number
- Harden the OS
- Password protect the BIOS
- Use disk encyrption on laptops
- Do not check luggage when flying
- Never leave a laptop unattended
- Install tracking software on laptops (lowjack type software)

Perimeter Security

Perimeter security is concerned with protecting the outside of your facility, that is ensuring that nobody unauthorized gets inside to cause any security violations. Perimeter security can implement multiple controls to keep the facility secure such as:

- Locks
- Personnel access controls
- Fencing
- Lighting
- Bollards
- Surveillance devices
- Intrusion detection systems
- Guard dogs

Personnel Access Control

- There are different technologies to grant access to a building.
  - User activated – a user does something (swipe cards, biometrics)
  - Proximity devices/transponders – a system recognizes the presence of an object. (Electronic access control tokens) is a generic term for proximity authentication systems)

Surveillance

- Surveillance systems are a detective control. Generally these are CCTV systems.

- CCTV systems consist of
  - Cameras
  - Transmitters
  - Receivers
  - Recording systems

Performing A Physical Security Audit

- Surveillance systems are a detective control. Generally these are CCTV systems.

- CCTV systems consist of
  - Cameras
  - Transmitters
  - Receivers
  - Recording systems

PART B
LECTURE 4
CYBER SECURITY – PHYSICAL SECURITY

Physical Security

- ➢ Metal theft (copper, aluminium)
- ➢ Sabotage or the destruction of critical equipment
- ➢ Insider theft of assets, information, or availability
- ➢ Theft of power
- ➢ Natural Disaster
- ➢ Aging Assets
- ➢ Personal Safety

Physical Security Standard

- Purpose:
  - To identify and protect transmission stations and transmission substations, their associated primary control centres, that if rendered inoperable or damaged as a result of physical attack could result in widespread instability, uncontrolled separation, or cascading within an interconnection.
- Applicability:
  - Transmission Owners (TO)
  - Transmission Operators (TOP)

Physical Security Standard

- R1 Assessment
- R2 Verification
- R3 Notify Control Centre
- R4 Threat Evaluation
- R5 Security Plan
- R6 3rd Party Review

Site Specific Layered Approach

- Deter potential adversaries from considering the facilities in their pre-operational planning
- Detect adversaries in their planning, surveillance, or approach stages
- Delay adversaries from gaining access to critical facilities and equipment
- Minimize the impact of any intrusions or attacks on BPS reliability
- Rapidly respond to any attacks or intrusions
- Preserve and assist law enforcement in evidence recovery for potential apprehension

Roadmap/Mind Map