Physical Security

Ed Crowley CISSP
‘05

Topics

- Facility Requirements Planning
- Faculty Security Management
- Environmental and Life Safety Controls
- Fire Detection and Suppression
- Heating, Ventilation, and Air Conditioning (HVAC)
- Physical and Technical Controls
- Facility Access Control Devices
- Intrusion Detection
- Media

Physical Security Domain

- Concerns aspects of surrounding physical environment and supporting infrastructure that may affect systems security.
- Includes:
  - Choosing a secure site
    - Secure design and configuration.
  - Physical Access Methodologies.
  - Equipment, or information, theft countermeasures.
  - Environmental and safety measures.

Physical Security Issues

- Threats, vulnerabilities, and countermeasures that apply to physically protecting enterprise resources.
- Resources include:
  - Personnel
  - Facility
  - Data
  - Equipment
  - Support systems
  - Media

Threats

- Emergencies
  - Fire
  - Building collapse
  - Utility Failure
- Natural Disasters
  - Earthquake
  - Storms
  - Flood
- Human
  - Sabotage
  - Vandalism
  - War
  - Strikes

Sources of Physical Loss

1. Temperature
2. Gases
3. Liquids
4. Organisms
5. Projectiles
6. Movement
7. Energy anomalies

Physical Security Controls

- Administrative
  - Facility Requirements Planning
  - Facility Security Management
  - Administrative Personnel Controls
- Physical and Technical Controls

Facility Requirements Planning

- Physical security controls need to be planned early.
  - Secure Site Considerations
    - Visibility
    - Local considerations
    - Natural disasters
    - Transportation
    - Joint Tenancy
    - External Services
  - Secure site design issues
    - Walls
    - Ceilings
    - Floors
    - Liquid or Gas Lines
    - Electrical Requirements
    - Windows
    - Doors
    - Sprinkler System
    - Air Conditioning

Facility Security Management

- Audit Trails
  - Record access attempts
    - Where
    - By whom
  - Detective
- Emergency procedures
  - Shutdown
  - Evacuation
  - Employee awareness training
- Administrative Personnel Controls
  - Pre-, post-, and ongoing, employee screening

Environmental and Life Safety Controls

- Physical security controls required to sustain:
  1. Computer's operating environment or
  2. Personnel's operating environment.
- Includes
  - Electrical power
  - Fire Detection and suppression
  - Heating, Ventilation and Air Condition (HVAC)

Electrical Noise

- EMI
  - Common mode noise (hot to ground)
  - Traverse mode noise (hot and neutral)
- RFI generated by the components of an electrical system, such as fluorescent lighting.
- Countermeasures
  - Power line conditioning
  - Proper grounding
  - Cable shielding
  - Limiting exposure to noise generators like magnets, fluorescent lights, and electric motors.

Electrical Power Terms

- Power Loss
  - Momentary power loss – Fault
  - Complete power loss – Blackout
- Voltage
  - Momentary low voltage -- Sag
  - Prolonged low voltage -- Brownout
  - Momentary high voltage–Spike
  - Prolonged high voltage – Surge
- Inrush – Initial power surge
- Noise – Steady interference
- Transient -- Short duration line noise

Humidity

- 40 to 60 % -- Ideal humidity operating range
  - Less than 40 percent increases potential for static electricity damage
  - More than 60 percent increases potential of condensation
- Hygrometer -- tool that measures humidity

Fire Classes

- A -- Common Combustibles
- B – Liquid
- C – Electrical
- D – Combustible Metals

Fire Suppression Chemicals

- Water – suppresses temperature required to sustain the fire
- Soda Acid – Suppresses fire fuel supply
- CO2 – Suppresses oxygen
- Halon – Suppresses combustion through a chemical reaction that kills the fire

Fire Detector Methodology

- Heat sensing
- Flame actuated
- Smoke actuated
- Automatic Dial up Fire Alarm

Fire Extinguishing Systems

- Wet Pipe – Water in pipes always.
- Dry Pipe – Water in pipes only when activated.
- Deluge – Type of dry pipe with large volume of water
- Preaction – Combination of Wet and Dry Pipe

Halon

- Not harmful to computer equipment
- Greater concentrations than 10 percent cannot be breathed safely
- At high temps, can degrade toxically.
- EPA regulations forbid new Halon 1301 installations.

Halon

- Halon 1211 -- Liquid
- Halon 1301 -- Gaseous
- Common EPA acceptable Halon replacements
  - FM-200
  - CEA –410
  - NAF-S-III
  - Argon
  - Inergen
  - Low pressure water mists

Heating, Ventilation, and Air Conditioning

- Physical and Technical Controls
- Facility Control Requirements
- Facility Access Control Devices
- Intrusion Detection and Alarms
- Computer Inventory Control
- Media Storage Requirements
- In event of fire, turn power off.

Facility Control Requirements

- Guns, guards, and gates
- Guards are the best resource during periods of personnel safety risks
  - Reliability, Training, and Cost of guards are significant issues
- Dogs – Loyal and reliable
- Fencing –Perimeter access control means.
  - Mantrap – Physical access control method where the entrance is routed through a set of double doors that may be monitored

Physical Security

- Lighting – Common form of perimeter protection.
- Fencing Height Requirements
  - 3 to 4 feet – Deters casual trespassers
  - 6 to 7 feet – Too hard to climb easily
  - 8 feet with three strands of barbed wire – Better Deterrence

Physical Security

- Locks
  - Preset
  - Programmable
- Closed Circuit TV
  - Monitor in real time – Preventative
  - Record – Detective

Facility Access Control

- Security Access Cards
  - Photo image (dumb)
  - Digitally encoded (smart)
- Wireless Proximity Reader – user activated and system sensing
  - Passive devices
  - Field powered devices
  - Transponders

Intrusion Detection and Alarms

- Identifies attempts to gain accesses.
- Perimeter Intrusion Detectors
  - Photoelectric sensor – light beam
  - Dry contact switches – metallic foil
- Motion Detectors
  - Wave pattern
  - Capacitance
  - Audio Detectors

Alarm Systems

- Local Alarm Systems
- Central Station Systems
- Proprietary Systems
- Auxiliary Station Systems
- Line Supervision –Process where an alarm signaling transmission medium is monitored to detect any line tampering to subvert its effectiveness.
- Power supplies – separate circuits with back up

Computer Inventory Control

- Physical Control
  - Cable control
  - Port control
  - Switch controls
  - Peripheral switch control
  - Electronic security boards
- Laptop Control

Media Storage Requirements

- Any sensitive data on a laptop requires encryption.
- Media types that require storage, destruction, or reuse
  - Backup tapes
  - CDs
  - Diskettes
  - Hard drives
  - Paper printouts and reports

Data Destruction and Reuse

- Magnetic media is typically destroyed by degaussing or overwriting.
- Sensitive reports should never be disposed of without shredding.

Object Reuse

- Concept of reusing data storage media after its initial use
- Remanence -- residual information remaining on the media after erasure.
  - May be subject to restoration by another user.
  - Orange book recommends magnetic media be formatted seven times before discard or reuse.

Data Deletion Notes

- For most operating systems, deleting doesn't actually remove data
- Damaged sectors may not be overwritten by format utility
- Paging doesn't necessarily delete temporary data.

Data Erasure Terms

- Clearing – Overwriting of data media (primarily magnetic) intended to be reused in the same organization or monitored environment.
- Purging –Degaussing or overwriting media intended to be removed from a monitored environment.
- Destruction – Completely destroying media

Questions?