InfoSec Tutorial: Physical Security Issues

Tony Kenyon, CEO.

Revision 1.01.
Updated: Jan 5th 2006

Ref: CNXT0002

Physical Security

- Fairly clear and concise domain
  - To protect enterprise resources and information from threats vulnerabilitie and countermeasures
  - Some physical control are duplicated in other domains such as the logical and operations domains
- Physical threats (e.g natural disasters)
- Facility controls
- Industrial security (CCTV, Guards, fencing, Lighting etc)
- Risks to C.I.A
  - Service interruption
  - Physical damage
  - Unauthorised disclose of info
  - Loss of system control/integrity
  - Physical theft

Physical Security

- Threats
  - Emergencies
    - Fire & smoke contaminants
    - Building collapse/explosion
    - Utility loss
    - Water damage
    - Toxic materials
  - Natural disasters
    - Earth movement
    - Storms
  - Human intervention
    - Sabotage
    - Vandalism
    - War
    - Strikes
- Major sources of physical loss
  - Temperature
  - Gases
  - Liquids
  - Organisms
  - Projectiles
  - Movement
  - Energy anomolies

Physical Security - Controls

- Administrative Controls
- Environmental & Life Safety Controls
- Physical and Technical Controls

Administrative Controls

- Facility Requirement Planning
  - Choosing secure sites (visibility, local considerations, natural disasters, transportation, joint tenancy, external services)
  - Designing Secure Sites (walls, ceilings, floors, windows, doors, sprinklers, liquid/gas lines, air conditioning, electrical)
- Facility Service Management
  - Audit Trails
  - Emergency Procedures (system shutdown, evacuation, training. System tests)
- Administrative Personnel Controls
  - HR responsibility (hiring&firing: screening, ongoing check, exit)

Environmental & Life Safety Controls

- Electrical Power
  - Noise
  - Brownouts
  - Humidity
- Fire detection and Supression
- Heating Ventilation and Air Conditioning (HVAC)

Safety Controls - Electrical Power

- Noise (EMI/RFI)
  - EMI
    - **Common-mode** noise (live-ground differential)
    - **Traverse-mode** noise (live-neutral differential)
  - RFI
    - Radiating electrical cables, fluorecent lights, electrical space heaters.
    - Can **permanently damage** electrical sensitive computer components
  - Anti-Noise measures include Power line conditioning, Proper Grounding, Cable Shielding, limiting exposure to magnets, fluoresent light, electric motors, space heaters etc.
- Brownouts
  - Prolonged drop is supplied voltage (unlike a sag). Can cause serious damange to sensitive components. Note that 15% fluctuations common in NYC
  - ANSI permits 8% drop between supply and meter, and 3.5% between meter and the wall socket.
  - Also: Surge is prolonged high voltage, inrush is surge at start.

Safety Controls - Electrical Power

- Humidity
  - Ideal operating humidity range is 40% to 60%
  - >60% causes condensation, corrosion, impeding efficiency.
  - <40% causes static.
    - Poss up to 4,000 volts on wood/vinyl floor in normal conditions
    - Poss up to 20,000 volts in low humidity & non-static free carpet
  - Controls
    - Use HVAC to control humidity
    - Anti-static sprays
    - Anti-static flooring, table and floor mats
    - Proper grounding

- **Static Charge damage**
  - 40V Sensitive circuits
  - 1000V Scramble monitor
  - 1500V Disk drive data loss
  - 2000V system shutdown
  - 4000V Printer Jam
  - 17000V Permanent chip damage

Safety Controls – Fire Detection

- Fire detection and Supression
  - **Water**: supresses temp
  - **Soda Acid**: suppresses fuel supply
  - **CO_2** : suppresses air supply
  - **Halon**: supresses combustion through chemical reaction
- Fire detectors
  - **Heat-sensing** (threshold or delta)
  - **Flame-activated** (expensive (IR sensors), fast acting, used for valuable equipment)
  - **Smoke-activated** (photoelectric sensor used in ventilation system for early warning. Also radioactive detector)
  - **Automatic Dialup Fire Alarm** (automated call to the police etc. Inexpensive but can be subverted)

FIRE CLASSES & COMBUSTABLES

CLASS	DESCRIPTION	SUPPRESS
A	Common Combustables	Water
		Soda acid
B	Liquid	CO_2
		Soda acid
		Halon
C	Electrical	CO_2
		Halon

Safety Controls – Fire Detection

- Fire extinguisher types
  - Water Sprinkers
    - **Wet Pipe**: most common, most reliable. Filed with water. Trigger > 165^{o}F. Issues with flooding and freezing
    - **Dry Pipe**: Water held back by clapper valve (air pressure). Time delay may allow time to shutdown sesnitive computer suystems
    - **Deluge**: dry pipe with much larger volume of water
    - **Preaction**: most recommended for computer rooms. Hybrid wet and dry pipe.
  - Gas discharge
    - Pressurized inert gas
    - Usually installed under the floor
    - Agents typically CO_2 or Halon
    - Halon 1301 requires sophisticated pressurisation system, Halon 1211 does not. FM-200 most common replacement for Halon

Safety Controls – Fire Supression Agents

- CO_2
  - commonly used in gas discharge systems; very effective, removes oxygen
  - Very dangerous for people, so used in unmanned systems or those with suitable delays
  - Note IG-541 contains CO_2
- Halon
  - Once considered perfect, fast, clean, no effects, however, cannot be safely breathed when >10%, and on fires >900^{o}F degrades into highly toxic chemicals (HF, HBr,Bromine)
  - Montreal Protocol 1987 bans Halon due to Ozone depletion (CFCs)
  - Halon 1301 - no new installations allowed due to Montreal Protocol
  - Halon 1211 is being replaced and recovered. Halon 1301 is being banked for the future
- Halon replacements
  - FM-200 (HFC-227ea) most common replacement
  - Also: CEA-410, CEA-308;
  - NAF-S-III (HCFC Blend A);
  - FE-13 (HFC-23);
  - Argon (IG55) or Argonite (IG01 – inert gas);
  - Inergen (IG541)
  - Low pressure water mists

Safety Controls – Fire Detection

- Heat Damage Temperatures
  - 100^{o}F Magnetic storage
  - 175^{o}F Computer Hardware
  - 350^{o}F Paper Products
- Dealing with equipment after a fire or water
  - Initial smoke damage not immediate, so if fire is short lived not necessarily serious. Main problem is subsequent corrossion
  - Turn off power
  - Remove/drain any water in the equipment
  - Move kit to a room with HVAC
  - Clean/spray the kit

Safety Controls –HVAC

- Heating, Ventilation and AC
- HVACR if refrigeration included

Physical and Technical Controls

- Facility Control Requirements
  - Guards, dogs, fencing, lighting, locks, CCTV
- Facility Access Control Devices
  - Security access cards
  - Biometrics
- Intrusion Detection and Alarms
- Computer Inventory Control
- Media Storage Requirements

Fencing

- 3′ to 4′ deters casual trespassers
- 6′ to 7′ Too hard to climb easily
- 8′ with 3 strands of barbed wire – deters intruders

Physical and Technical Controls

- Facility Access Control Devices
  - Security access cards
    - Photo-image (dumb) cards
    - Digitally encoded (smart and smarter)
    - Wireless proximity readers
      - User activated
      - System-sensing (passive, field-powered, transponders)
  - Biometrics

Physical and Technical Controls

- Intrusion Detection and Alarms
  - **Perimeter** Intrusion Detectors
    - **Photoelectric sensors**. Can be seen
    - **Dry Contact Switches**. Most common
  - **Motion** Detectors
    - **Wave pattern detectors**: generates low, ultrosonic or microwave frequency wave and checks for disturbances in reflections, Used in rooms.
    - **Capacitance detectors**: monitor electrical field in very close proximity (inches) to objects
    - **Audio amplification devices**: passive. Trigger on sound in a room. Tends to generate more false alarms than other two.

Physical and Technical Controls

- Alarm Systems
  - **Local**: local alarm, 400ft audio, guards, anti-tamper
  - **Central Station**: private firms, 24x7, leased lines, CCTV, reports, 10 minute response
  - **Proprietary**: as Central Station but monitoring done by customer. Sophisticated
  - **Auxilliary Station**: any of the above may also ring emergency services
  - **Line Supervision** (monitoring or alrm circuit to detect tampering). UL 611-1968
  - **Power Supplies**: separate power supply and 24-hour backup before discharge

Physical and Technical Controls

- Computer Inventory Control
  - PC Physical Control (40% losses estimated through theft of parts)
    - Cable locks, Port controls, switch controls, peripheral switch controls, electronic security boards
  - Laptop control
    - Potentially Serious failure in C.I.A
- Media Storage Requirements
  - On, Offsite. Data, CD, Hard Drive, paper printouts
  - Data destruction
    - De-Gaussing magnetic media
    - Overwriting/formatting 7 times (Orange book)
      - Note that damaged sectors may not be overwritten with formatting
    - Paper Shredding, Burning (DoD)
  - Object Re-use and Data Remanence
  - Data erasure stages
    - Clearing: overwriting
    - Purging: de-gaussing
    - Destruction: destrying physically

Questions?