Ch.7 summary By @MHazazi

Understanding the Secure Facility Layered Defense Model

- If an intruder bypasses one layer of controls, the next layer should provide additional defense and detection capabilities
- Both physical and psychological
- The appearance of security is deterrent

How to Secure the Site

- All implemented controls to physically protect information are dictated by:
  - analysis of the company's risks and vulnerabilities
  - the value of the information that requires protection

- From what are we protecting information assets?
  - Theft
  - Malicious destruction
  - Accidental damage
  - Damage that results from natural disasters

- The design of a secure site starts with the **location**
  - **Location-based threats:**
    1. Political stability
    2. Terrorism
    3. Crime rate
    4. Roadways and flight paths
    5. Utility stability
    6. Vulnerability to natural disasters
  - Critical information processing facilities should be inconspicuous and unremarkable

- The physical perimeter can be protected using:
  - Berms
  - Fences
  - Gates
  - Bollards
  - Man traps
  - Illuminated entrances, exits, pathways, and parking areas
  - Manned reception desk
  - Cameras, closed-circuit TV, alarms, motion sensors
  - Security guards

How Is Physical Access Controlled?

- Physical entry controls:
  - **Access control rules should be designed for:**
    - Employees
    - Third-party contractors/partners/vendors
    - Visitors
  - Visitors required to **wear identification** and clear to see from a distance, such as a badge
  - Identification start **as soon as a person attempts to gain entry**
  - Authorized users should be authorized **prior** gaining access to protected area
  - Visitors be identified, labeled, and authorized **prior** to gaining access to protected area
  - **Audit trail** should be created

Securing Offices, Rooms, and Facilities

- Workspaces should be classified based on the level of protection required
- Some internal rooms and offices must be protected differently
- Individual rooms may also require different levels of protection, such as cabinets closets

Working in Secure Areas

- Define behavioral and physical controls for the most sensitive workspaces
- Policy controls not enough alone , you need physical controls, unless Policy controls is stronger
- Policy should include devices not allowed on premises
- Sensitive documents should be secured from viewing by unauthorized personnel while not in use
- Copiers, scanners, and fax machines should be located in nonpublic areas and require use codes

Protecting Equipment

- Both company and employee-owned equipment should be protected
- Hardware assets must be protected from:

  Theft , Power spikes ,Power loss
- One way to reduce power consumption is to purchase Energy Star certified devices
- Potential power problems include:
  - **Brownout**: Period of low voltage
  - **Power surge**: Increase in voltage
  - **Blackout:** Interruption or loss of power

- Power equipment that can be used:
  - Uninterruptible Power Supply
  - Back-up power supplies
  - Power conditioners
  - Voltage regulators
  - Isolation transformers
  - Line filters
  - Surge protection equipment

How Dangerous Is Fire

- Three elements to fire protection

1) **Fire prevention controls** (Active & Passive)

   Ex: hazard assessments and inspections / adhering to building and construction codes/ using flame-retardant materials/ proper handling & storage procedures for flammable materials

2) **Fire detection** (Recognizing that there is a fire)

   Ex: Fire detection devices can be smoke activated, heat activated, or flame activated

3) **Fire containment and suppression** (responding to the fire)

   - Specific to file classification
     - Class A combustible materials as fuel source (wood, cloth, paper, rubber, plastics)
     - Class B flammable liquids (oils, greases, tars, oil paints, lacquers, flammable gases)
     - Class C electrical equipment
     - Class D combustible materials as metal
   - Test fire-extinguishing methods annually to validate full functionality.
   - Data centers & critical locations protected by an automatic fire-fighting system

What About Disposal

- Formatting a hard drive or deleting files does not mean that the data cannot be retrieved
- All computers that are discarded must be sanitized prior to being disposed of

- Data file type:
  - **Apparent data files**: files that authorized users can view and access.
  - **Hidden files:** files operating system does not display.
  - **Temporary files:** created to hold information temporarily while a file is being created.
  - **web cache:** temporary storage of web documents, such as HTML pages, images,downloads.
  - **Data cache:** temporary storage of data that has recently been read and used.
  - **Metadata**: is details about a file that describes or identifies it.
  - **Browser-based data**:
    - Browsing history, which is the list of sites visted
    - Download history, which is the list of files downloaded
    - Form history, which includes the items entered into web page forms
    - Search bar history, which includes items entered into the search engines
    - Cookies, store information about websites visited(site preferences ,login status)

- Removing Data from Drives
  - **Formatting** a disk erases the operating system address tables. The files still inside the hard drive, and system recovery software can restore them.
  - **Data destruction** "Actions taken to ensure media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive

- Methods of permanently removing data from a drive

1) **Disk wiping (scrubbing)**

- Overwrite the master boot record (MBR), partition table, and every sector of the hard drive with the numerals 0 and 1 several times. Then the drive is formatted.
- The more times the disk is overwritten and formatted, the more secure the disk wipe is.
- Disk wiping does not work reliability on SSD; USB drives, compact flash, MMC/SD cards.

Ex. The government medium security standard (DoD 5220.22-M) specifies

- three iterations to completely overwrite a hard drive six times.
- Each iteration makes two write-passes over the entire drive; the first pass inscribes ones (1) over the drive surface and the second inscribes zeros (0) onto the surface.
- After the third iteration, a government-designated code of 246 is written across the drive, then it is verified by a final pass that uses a read-verify process.
- There are several commercially available applications that follow this standard.

2) **Disk Degaussing**

- magnetic object, is exposed to a great magnetic field which lead to the movement of magnetic media through the degaussing field realigns the particles, resetting the magnetic field of the media to a near-zero state,
- This process will erase all of the data previously written to the tape or hard drive.
- Degaussing resets the media to a like-new state so that it can be reused and recycled

3) **Disk physical destruction**

- Make the disk unreadable and unusable.
- disk can be crushed, shredded, drilled