Introduction to Cybersecurity

Chapter 8

Physical Security

Chapter Objectives

- Physical Security Controls
- Secure Data Destruction
- Equipment protection

Physical Security Controls

- Physical security protects tangible assets, like buildings and equipment
  - theft, vandalism, burglary, terrorism, natural disasters, and fire
- Physical access controls (PACs) are security systems that prevent unauthorized access to certain areas

- PACs can be used to:
  - Secure buildings
  - Monitor and enforce physical security
  - Identify users and employees
  - Authenticate who users are
  - Authorize access to items or areas
  - Limit and track which users have access to a physical space

Why Physical Security Is Essential

- Cybersecurity depends on physical safeguards
- Prevents data loss, service disruption, and insider threats
- Required by standards (HIPAA, PCI-DSS, NIST)
- Social engineering often begins with a physical breach

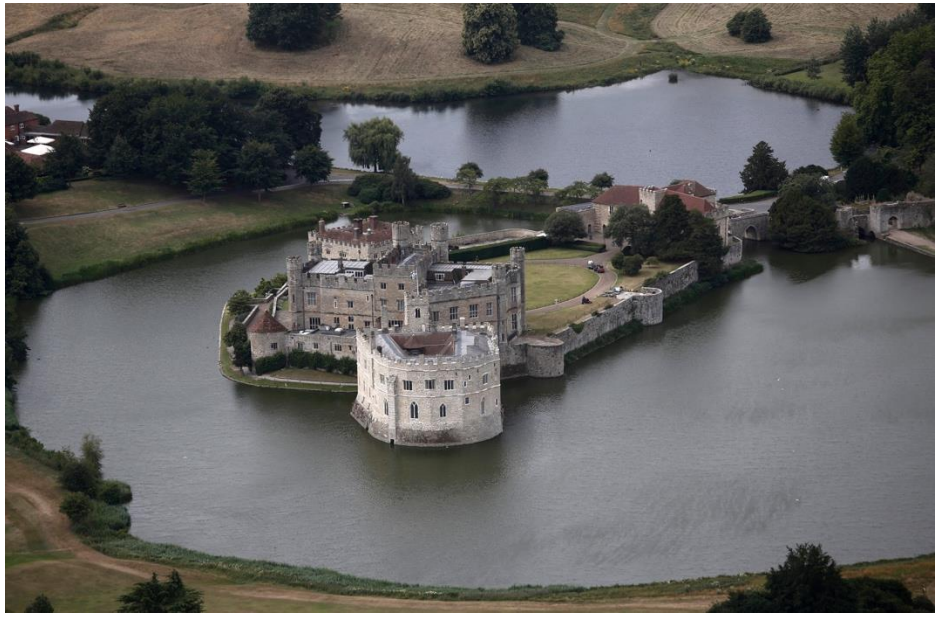
If someone can walk in and steal your server, no encryption will save you.

Fence/Bollards/Barricades

- **Fence**: A fence is a wood/wire /concrete barrier that encloses an area
- **Bollards/Barricades**: A bollard is a short post that prevents vehicle access to an area

- Channel people through a specific access point
  - Allow people, prevent cars and trucks
  - Prevent people from driving into or through the walls of a data center
  - Protect equipment from tampering, vandalism
  - Protect a building from accidental or intentional structural damage

- Use a moat to surround an area
  - ➢No one outside the network is able to access data on the inside



The cube: Sat outside the city of Covilha, at the foot of Portugal's highest mountain range, is what will be one of Europe's largest datacentres

Tailgating/ Piggybacking

- Tailgating happens when someone secretly follows another person into a restricted area without the first person knowing
- Piggybacking involves some degree of permission from the person with access. It can occur if the person holding the door assumes the follower should also be allowed in, often by mistake or out of politeness
  - ➢Bypasses physical access controls
  - ➢Exploits human trust and courtesy
  - ➢Can lead to data theft, sabotage, or surveillance

- Safeguard
  - ➢Use mantraps/vestibules to restrict entry
  - ➢Implement badge-in and badge-out systems
  - ➢Educate staff to challenge unknown individuals

Tailgating Vs Piggybacking

keepnet

Tailgating

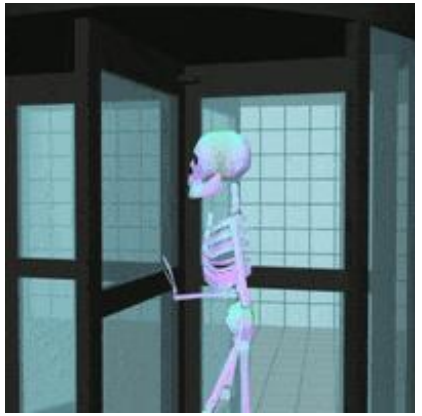
The attacker **follows somebody** with authorized access into a secure location **without their knowledge.**

Piggybacking

The attacker is **purposely let into a restricted area** with the help of someone with authorized access.

Access control vestibules

- All doors normally unlocked
  - ➢ Opening one door causes others to lock
- All doors normally locked
  - ➢Unlocking one door prevents others from being unlocked
- One door open/others locked
  - ➢When one is open, the other cannot be unlocked
- One at a time, controlled groups
  - ➢managed control though an area

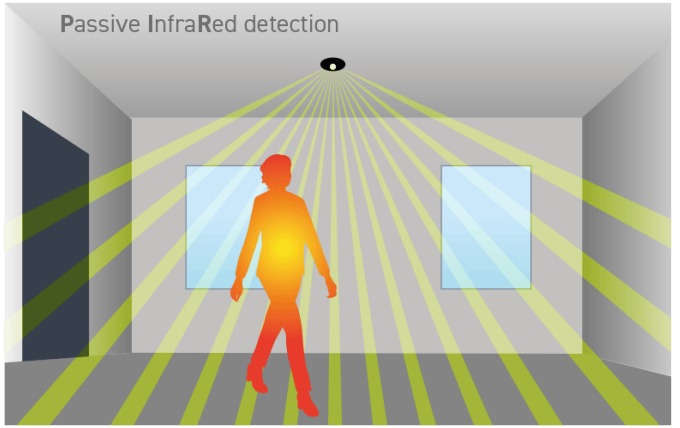


Alarms

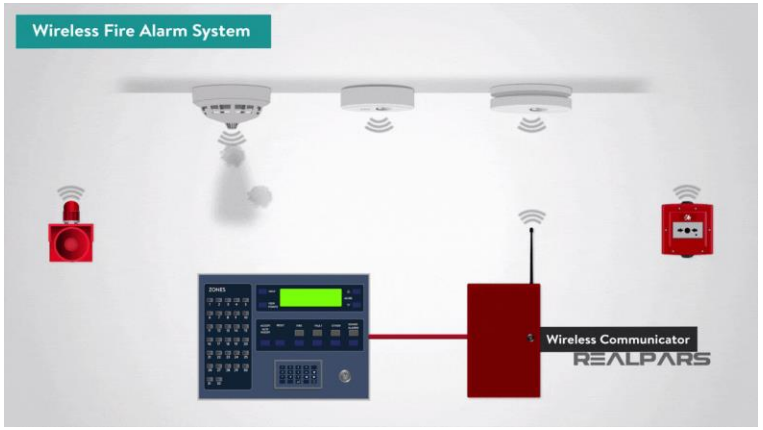
- Alarms provide early warnings to deter threats and prevent unauthorized access

- Circuit based
  - ➢Circuit is open or closed (usually a sensor connected to door or window)
  - ➢Door, window, fence
  - ➢Useful on the perimeter

- Motion detection
  - ➢Passive infrared
  - ➢Useful in areas not often in use



- Panic Button/Duress
  - ➢Triggered by a person



Signs

- Clear and Specific Instructions
  - ➢Keep people away from restricted areas
  - ➢Consider visitors
- Consider personal safety
  - ➢Fire exits
  - ➢Warning signs
    - Chemicals
    - Constructions
  - ➢Medical resources
- Informational
  - ➢Emergency contact number

Video Surveillance

- CCTV (Closed circuit television)
  -can replace physical guards

- Camera features are important
  - ➢Motion recognition can alarm and alert when something moves
  - ➢Object detection can identify a license plate or person's face

- Drones may be used for surveillance
  - ➢Covers large areas
  - ➢Site surveys, damage assessment

Industrial Camouflage

- Industrial camouflage is the act of obscuring a building's purpose
  - ➢Blends in the local environment
  - ➢Often used to protect critical facilities like data centers from being targeted

- Protect data center
  - ➢No business sings
  - ➢No visual clues
  - ➢Install a guard gate
  - ➢Planters out front are bollards

Guards and access list

- Security guards
  - ➢Physical protection at the reception area or gate
  - ➢Validate identification of employees
  - ➢Provides guest access
- ID badge
  - ➢Picture, name, other details
  - ➢Must be worn at all times
- Access list
  - ➢Physical list of names
  - ➢Enforced by security guard
- Maintains visitor log

Guards

- Two-person integrity/control
  - ➢Minimize exposure to an attack
  - ➢No single person has access to a physical asset

- Robot surveillance
  - ➢Monitoring
  - ➢Rounds/periodic check

Biometric

- Biometric Authentication
  - Fingerprint, retina, voice, palm
- Difficult to change
  - You can change your password
  - You can’t change your fingerprint

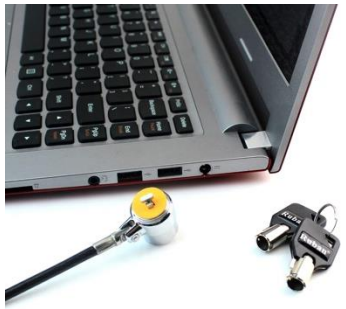
- Unique data and specific characteristics of the fingerprint are filtered
- Then saved as a mathematical representation (algorithm) or as an encrypted biometric key

- Not foolproof

Conventional: Cable/Locks

- Locks
  - Lock and key
  - Physical cipher locks
  - PIN based
  - Cable locks
  - RFID badge, magnetic swipe card, key fob
  - Biometric
  - Multifactor locks
  - Smart card and pin

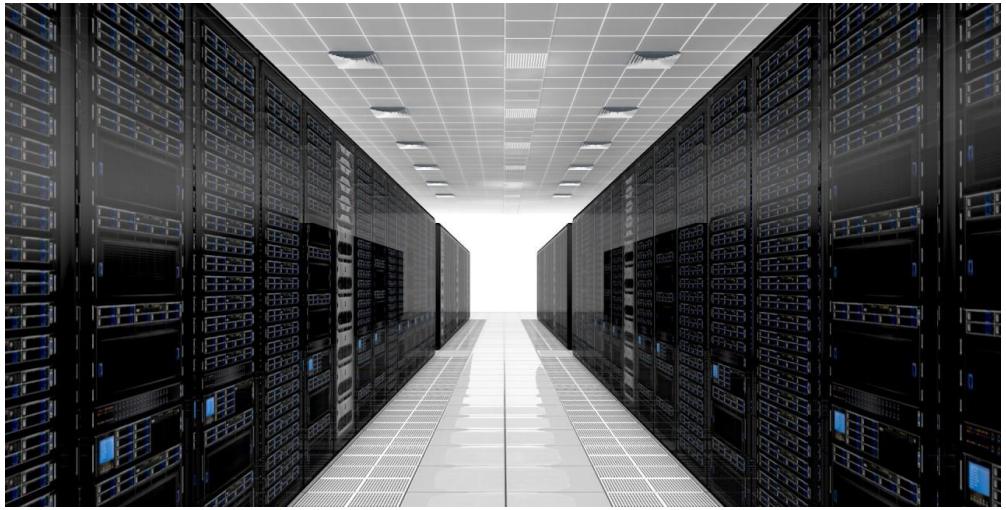
- Laptop Security Locks
  - Thin cable, not for long term protection
  - Cut without alerting owner



Proper lighting

- Proper lighting is a fundamental aspect of physical security, enhancing both visibility and the effectiveness of surveillance systems while deterring potential threats

- More lighting means more security
  - Attacks avoid the light
  - Easier to see when lit
  - Non IR camera can see better



- Lighting angles are important
  - Facial recognition
  - Avoid shadow and glare

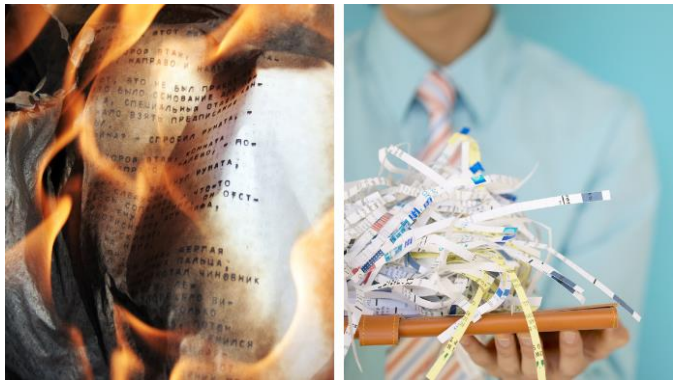
Fire Suppression

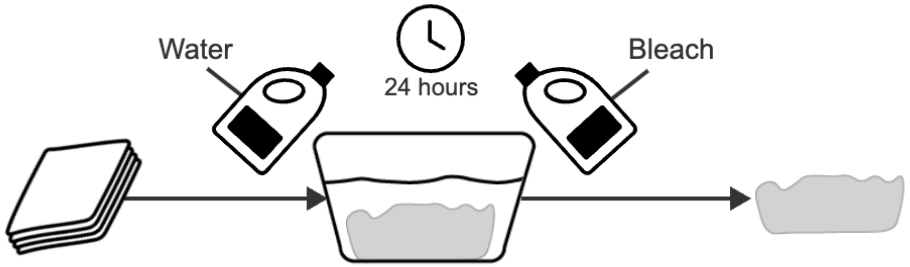
- Fire suppression systems are a critical, especially in facilities housing sensitive electronics and data, such as data centers or server rooms
- Electronics require unique response to fire
  - Water is generally not good
  - Data loss should be prevented
  - Use water where appropriate
- Detection
  - Smoke detector, flame detector, heat detector
- Suppress with chemicals
  - Halon- no longer used (destroys ozone)
  - Replaced with dupont FM-200
    - (Heptafluoropropane) is a compound of carbon, fluorine and hydrogen (CF3CHFCF3)

Secure Data Destruction

Paper documents:

- Burning
  - Burning turns paper to ash in a high-temperature incinerator
- Shredding
  - Shredding turns paper into small confetti-like shreds using rotating blades
- Pulping
  - Pulping turns paper into a soft mush, called pulp, by soaking the paper in water and bleach

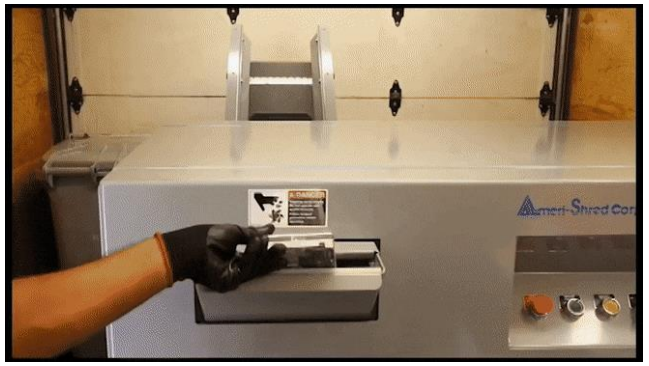




Secure Data Destruction

Digital documents:

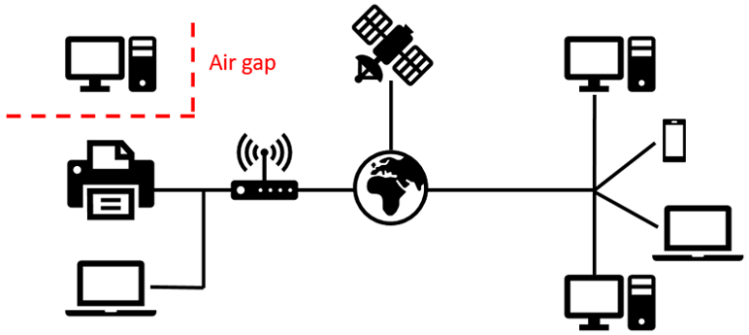
- **Hardware shredding**: turns hardware into small metal pieces using specialized blades
- **Pulverizing**: turns hardware into powder by crushing
- **Degaussing**: wipes data from magnetic media using strong magnetic fields
- **Puncturing**: punches multiple pins into the hard drive, and the chips contained within them



Equipment protection

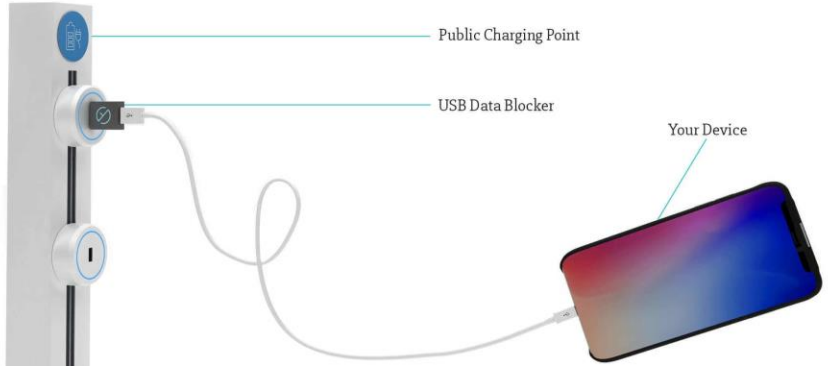
Air gap: deliberate lack of connection between a device and a network

- Ex: A backup server is air-gapped to protect against data breach

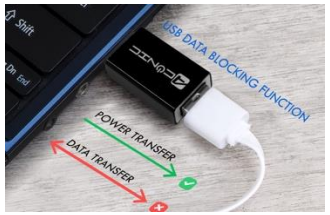


USB data blocker: a device placed between a USB connector and a power source that prevents data from traveling through the USB connection

- allows the voltage, rejects the data



- Don’t connect to unknown USB interfaces
- Prevent “juice jacking”



Equipment Protection

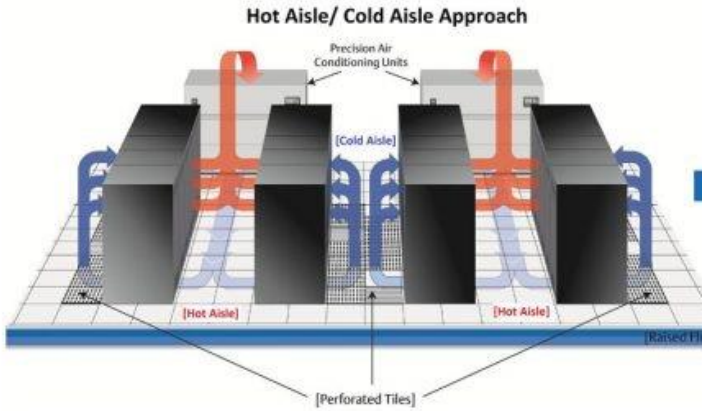
- **Protected cable distribution**: a strategy that secures network cables against unauthorized access or harm
  - ➢Ex: network cable is mounted inside a metal enclosure to prevent tampering

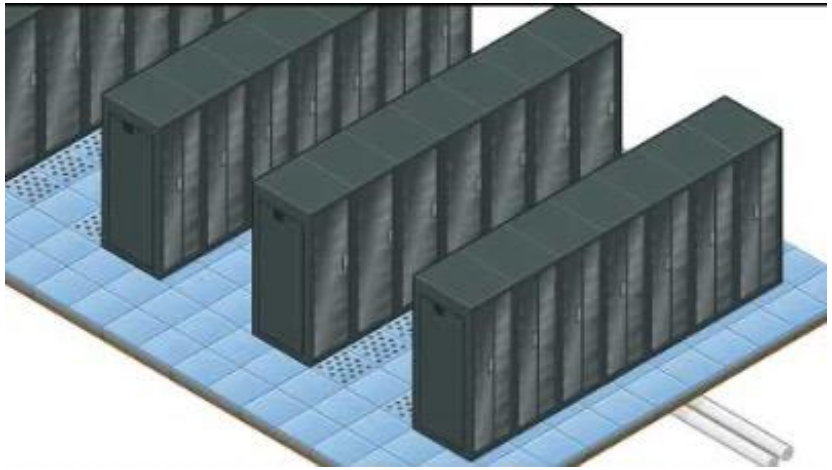
- **Faraday cage**: mesh enclosure that blocks electromagnetic fields like Wi-Fi signals
  - ➢Ex: Faraday cage is built into a server rack to protect the servers from outside eavesdropping

Equipment Protection

- Several servers are housed in a server rack can heat excessively to damage the servers
- A hot aisle/cold aisle system uses alternating hot and cold aisles in a server room to manage the heat and cool the servers
  - ➢Manage airflow in a way that conserves energy
  - ➢Lower cooling costs
  - ➢Prevent “overcooling” or “overheating” of areas

    - Server racks are lined up in alternating rows
    - Cold air intakes face one direction, Hot air exhausts face the opposite direction
    - Rows with rack fronts are known as cold aisles
    - Hot air is exhausted out the back of the servers and directed into a plenum space above the racks





https://www.youtube.com/watch?v=xv-i4RQLswo&ab_channel=MEPAcademy

Credit: Cool Shield

Example: Google Data Center Security: 6 Layers Deep

Data Centers (Data & Security) → https://goo.gle/2LmkzF3
Google Cloud (Trust & Security)→ http://goo.gle/38bAn8F