Physical and Infrastructure Security

News

- https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Exec%20Summary_2024%20Microsoft%20Digital%20Defense%20Report.pdf
- https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/

Physical and Infrastructure Security

Logical security

- Protects computer-based data from software-based and communication-based threats

Physical security

- Also called infrastructure security
- Protects the information systems that contain data and the people who use, operate, and maintain the systems
- Must prevent any type of physical access or intrusion that can compromise logical security

Premises security

- Also known as corporate or facilities security
- Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations
- Provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards

Physical Security Threats

Physical Security Threat Categories

- Environmental threats
- Technical threats
- Human-caused threats
  - Physical access can overcome logical controls

Environmental Threats and Mitigations

Natural Disasters

	Warning	Evacuation	Duration
Tornado	Advance warning of potential; not site specific	Remain at site	Brief but intense
Hurricane	Significant advance warning	May require evacuation	Hours to a few days
Earthquake	No warning	May be unable to evacuate	Brief duration; threat of continued aftershocks
Ice storm/ blizzard	Several days warning generally expected	May be unable to evacuate	May last several days
Lightning	Sensors may provide minutes of warning	May require evacuation	Brief but may recur
Flood	Several days warning generally expected	May be unable to evacuate	Site may be isolated for extended period

Source: ComputerSite Engineering, Inc.

Examples

- https://mha-it.com/blog/business-emergencies

Natural Disaster Mitigation

- Location of data center – avoid flood zones
- If possible, avoid tornado and hurricane zones

Fire and Smoke

- Fire threats can be wildfire, building fire or electrical fire
- Fire suppression around equipment is a key concern
  - Sprinklers can make equipment unusable and pose electrocution threat to people
  - Clean gas systems can reduce oxygen, but are one-shot and may not extinguish fire
  - Some combination is ideal
- Smoke damage related to fires can also be extensive as smoke is an abrasive.
  - Collected particles can prevent heat dissipation or cause electrical shorts
  - It collects on the heads of unsealed magnetic disks, optical disks, and tape drives

Fire Extinguishers (For Security+)

Table 8.1	Types of Fire and Suppression Methods		
Class of Fire	**Type of Fire**	**Examples of Combustible Materials**	**Example Suppression Method**
A	Common combustibles	Wood, paper, cloth, plastics	Water or dry chemical
B	Combustible liquids	Petroleum products, organic solvents	CO_2 or dry chemical
C	Electrical	Electrical wiring and equipment, power tools	CO_2 or dry chemical
D	Flammable metals	Magnesium, titanium	Copper metal or sodium chloride

Water Damage

- Primary danger is an electrical short
- A pipe may burst from a fault in the line or from freezing
- Sprinkler systems set off accidentally
- Floodwater leaving a muddy residue and suspended material in the water
- **Mitigation**
  - Equipment location: due diligence should be performed to ensure that water from as far as two floors above will not create a hazard
  - Cutoff sensors to turn off power in case of water release

Humidity and Condensation

- Long-term exposure to high humidity can result in corrosion nab also cause a galvanic effect that results in electroplating, in which metal from one connector slowly migrates to the mating connector, bonding the two together.
- Condensation can threaten magnetic and optical storage media and cause a short circuit, which in turn can damage circuit boards
- Low humidity - Static electricity discharges as low as 10 volts can damage particularly sensitive electronic circuits, and discharges in the hundreds of volts can create significant damage to a variety of electronic circuits.
  - Discharges from humans can reach into the thousands of volts
- In general, relative humidity should be maintained between 40% and 60% to avoid the threats from both low and high humidity.

Dust and Infestation

Dust

- Rotating storage media and computer fans are the most vulnerable to damage
- Can also block ventilation
- Influxes can result from a number of things:
  - Controlled explosion of a nearby building
  - Windstorm carrying debris
  - Construction or maintenance work in the building
- Mitigation is filtered air system

Infestation

- Covers a broad range of living organisms:
  - High-humidity conditions can cause mold and mildew
  - Insects, particularly those that attack wood and paper
  - Rodents that chew wire insulation

Mitigation for Environmental Threats

- Environmental control equipment for temperature, humidity and dust

Chemical, Radiological, and Biological Hazards

- Pose a threat from intentional attack and from accidental discharge
- Discharges can be introduced through the ventilation system or open windows, and in the case of radiation, through perimeter walls
- Flooding can also introduce biological or chemical contaminants

Technical Threats

Electricity Issues

- Under-voltage - dips/brownouts/outages, interrupts service
- Over-voltage - surges/faults/lightening, can destroy chips
- Noise - on power lines, may interfere with device operation

Electromagnetic interference (EMI)

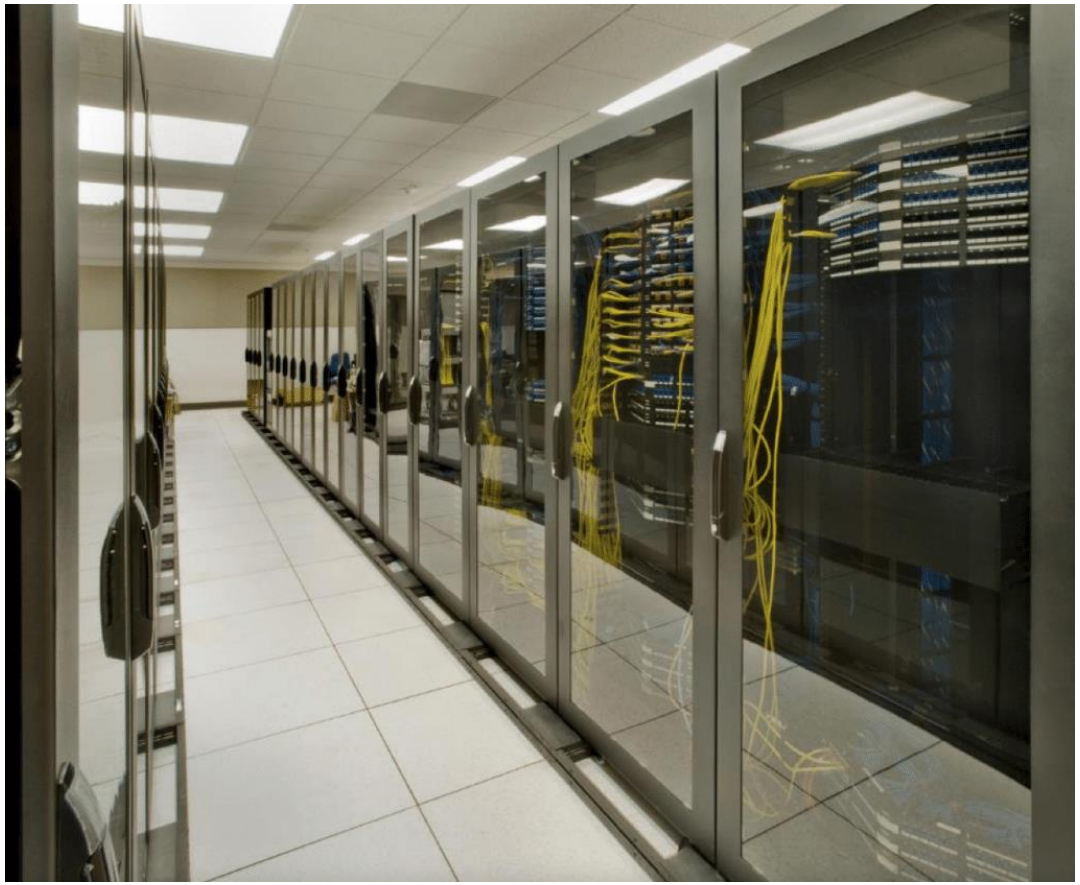
- Noise along a power supply line, motors, fans, heavy equipment, other computers, cell phones, microwave relay antennas, nearby radio stations
- Noise can be transmitted through space as well as through power lines
- Can cause intermittent problems with computers

Mitigation Measures For Technical Threats

- Uninterruptible power supply (UPS) for each piece of critical equipment
- Critical equipment should be connected to an emergency power source (like a generator)
- To deal with electromagnetic interference (EMI) and evesdropping a combination of filters and shielding can be used

TEMPEST Standard
https://en.wikipedia.org/wiki/Tempest_(codename)

Faraday Cage



Faraday Cage

Human Caused Threats

The Physical Security Problem

- Physical access negates all other security measures
  - No matter how impenetrable the firewall and intrusion detection system (IDS), if an attacker can find a way to walk up to and touch a server, he can break into it
- Physically securing information assets does not mean just the servers
  - It means protecting physical access to all the organization's computers and its entire network infrastructure

Physical Security – Data Theft

- Physical access is the most common way of imaging a drive
  - Biggest benefit for the attacker is that drive imaging leaves absolutely no trace of the crime

Physical Security – DoS

- A denial-of-service (DoS) attack can also be performed with physical access
  - Physical access to the computers can be much more effective than a network-based DoS attack

Physical Security – Boot Media

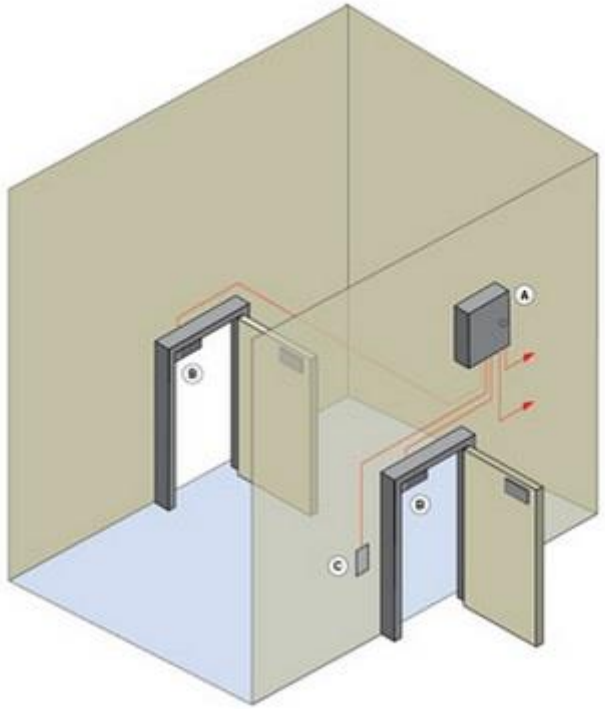
- Any media used to boot a computer into an operating system that is not the native OS on its hard drive can be classified as a bootdisk
- A LiveCD or bootable flash drive contains a bootable version of an entire operating system, typically a variant of Linux, complete with drivers for most devices
  - LiveCDs give an attacker more permissions and a greater array of attack tools
- With a LiveCD, an attacker would likely have access to the hard disk and also to an operational network interface that would allow him to send the drive data over the Internet if properly connected

Kali Boot to Root Demo

Mitigation Measures
Human-Caused Physical Threats

- Physical access control
  - Restrict building access -perimeter security
  - Controlled areas patrolled or guarded
  - Locks or screening measures at entry points
  - Equip movable resources with a tracking device
  - Power switch controlled by a security device
  - Surveillance systems that provide recording and real-time remote viewing
  - Intruder sensors and alarms
  - **Restrict access to critical rooms**

Mantrap Entrance



Overall Physical Security Mitigation

- Use of cloud computing
  - This just shifts who is responsible

Physical Security Standards

- https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PE
- ISO 27002

Open Nice Challenge Workspace

Physical Security Summary

Prevent damage to physical infrastructure	Prevent physical infrastructure misuse that leads to the misuse or damage of protected information
• Concerns include system hardware, physical facility, support facilities, and personnel	• Includes vandalism, theft of equipment, theft by copying, theft of services, and unauthorized entry

Recovery from Physical Equipment Damage

- **Most essential element of recovery is redundancy**
  - Provides for recovery from loss of data
  - Ideally all important data should be available off-site and updated as often as feasible
  - Can use batch encrypted remote backup
  - For critical situations a remote hot-site that is ready to take over operation instantly can be created
    - Can also have warm sites and cold sites

Data Center Security

Includes Redundancy and Resilience

Data Center

- An enterprise facility that houses a large number of servers, storage devices, and network switches and equipment
- Generally includes redundant or backup power supplies, redundant network connections, environmental controls, and various security devices
- Can occupy one room of a building, one or more floors, or an entire building
- Examples of uses include:
  - UNR Pronghorn
  - Cloud service providers
  - Large scientific research facilities
  - IT facilities for large enterprises

TIA-942 Data Center Tiers

- **Rated-1: Basic Site Infrastructure**
  A data center which has single capacity components and a single, non-redundant distribution path serving the computer equipment. It has limited protection against physical events.

- **Rated-2: Redundant Capacity Component Site Infrastructure**
  A data center which has redundant capacity components and a single, non-redundant distribution path serving the computer equipment. It has improved protection against physical events.

- **Rated-3: Concurrently Maintainable Site Infrastructure**
  A data center which has redundant capacity components and multiple independent distribution paths serving the computer equipment. Typically, only one distribution path serves the computer equipment at any time. The site is concurrently maintainable which means that every capacity component, including elements which are part of the distribution path, can be removed/replaced/serviced on a planned basis without disrupting the ICT capabilities to the end user. It has protection against most physical events.

- **Rated-4: Fault Tolerant Site Infrastructure**
  A data center which has redundant capacity components and multiple independent distribution paths serving the computer equipment which all are active. The data center allows concurrent maintainability and one (1) fault anywhere in the installation without causing downtime. It has protection against almost all physical events.

(Table is on page 177 in textbook)

Google Data Center

- https://goo.gl/w03sJ

- Security:
- https://www.google.com/about/datacenters/data-security/

Data Center Security Standards

- https://www.iso.org/standard/75106.html
- Legal Requirements:
  - https://cloud.google.com/security/compliance/#/

NICE Challenge OS Hardening

- STIGs

Midterm Exam

- Review Chapter Outlines and past quizzes
- 50 Questions 70 Minutes
- Take any time before due date/time

Prep for Cloud Computing

- **For Assignment:**
  - Check your UNR email from Qwiklabs or Cloud Skills Boost for training credits for assignment
    - Sign up with **UNR email**
- **For in-class work:**
- Watch for email from me to claim your $50 cloud credits for in-class work next week.
  - Enter UNR email at link to receive the credit voucher
  - Use Google account to redeem the voucher
    - If you have a Google account tied to a credit card, it might be safer to create a new account