

N|DE
Network Defense Essentials

Module 04

Network Security Controls - Physical Controls

Module Objectives



1. Understanding the Importance of Physical Security
2. Understanding the Physical Security Attack Vectors
3. Understanding the Various Types of Physical Security Controls
4. Understanding the Importance of Workplace Security
5. Overview of Physical Security Policy
6. Understanding the Various Environmental Controls

Module Flow

1 **Understand the Importance of Physical Security**

2 **Discuss Various Physical Security Controls**



3 **Describe Workplace Security**

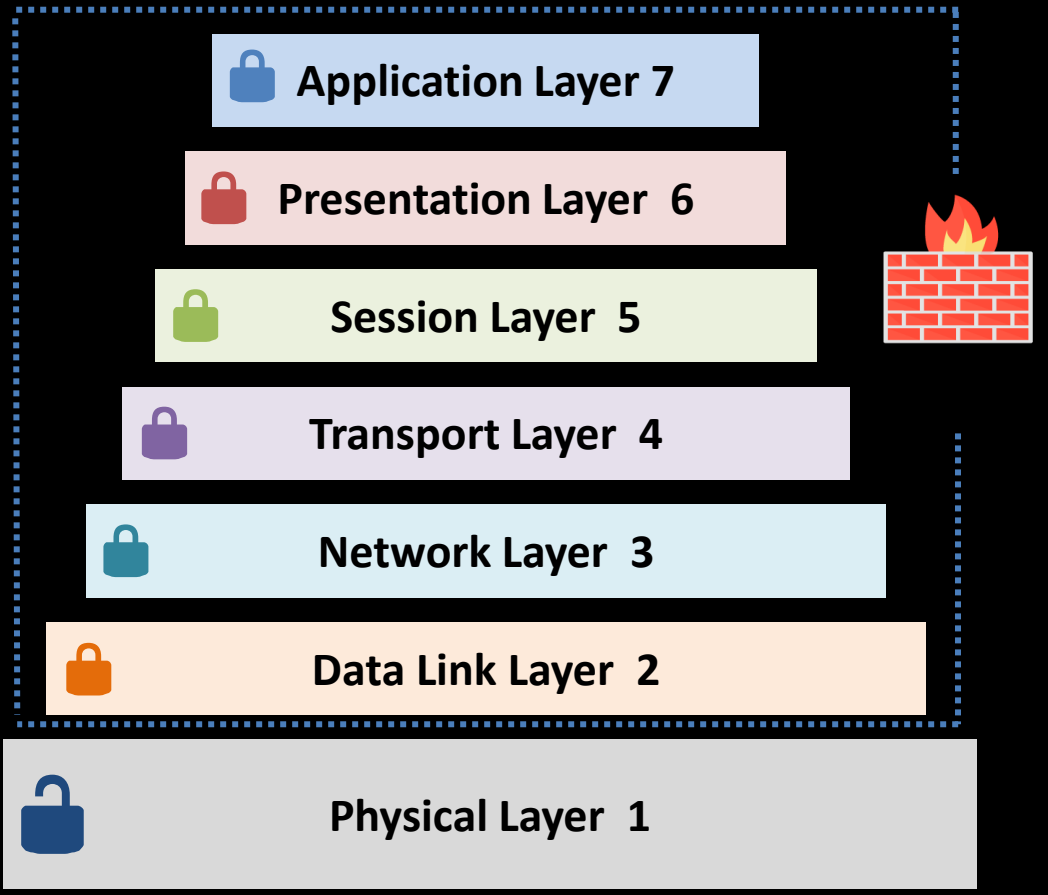
4 **Describe Various Environmental Controls**

Need for Physical Security

A successful unauthorized physical access may lead to **theft**, **damage,** or **modification** of the information systems

A physical security breach can **directly impact confidentiality**, integrity, and availability of information and systems

Physical security is the basis of any **information security program** in an organization. It deals with **restricting unauthorized physical access** to the infrastructure, office premises, workstations, and employees of the organization



The 7 Layers of OSI

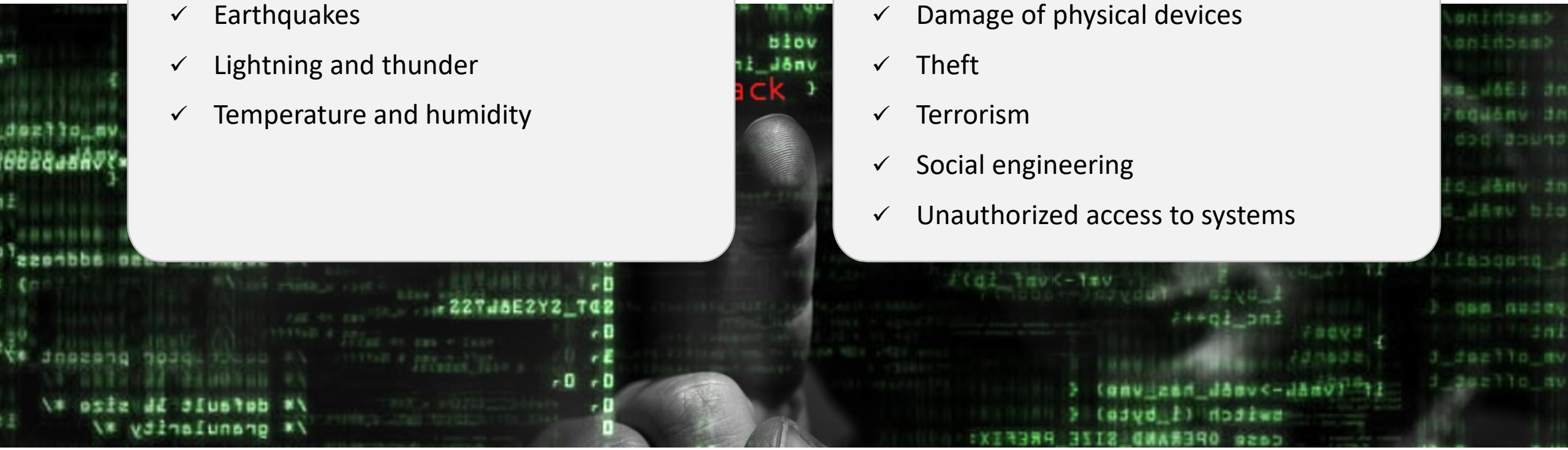
Physical Security Attack Vectors

Natural/Environmental Threats

- ✓ Floods
- ✓ Fires
- ✓ Earthquakes
- ✓ Lightning and thunder
- ✓ Temperature and humidity

Man-made Threats

- ✓ Vandalism
- ✓ Device loss
- ✓ Damage of physical devices
- ✓ Theft
- ✓ Terrorism
- ✓ Social engineering
- ✓ Unauthorized access to systems



Module Flow

1 Understand the Importance of Physical Security

2 Discuss Various Physical Security Controls



3 Describe Workplace Security

4 Describe Various Environmental Controls

Types of Physical Security Controls

Preventive Controls	❑ Prevent **security violations** and enforce various access control mechanisms ❑ Examples include door lock, security guard, and other measures
Detective Controls	❑ Detect security violations and **record any intrusion attempts** ❑ Examples include motion detectors, alarm systems and sensors, video surveillance, and other methods
Deterrent Controls	❑ Used to discourage attackers and **send warning messages** to the attackers to discourage intrusion attempts ❑ Examples include various types of warning signs
Recovery Controls	❑ Used to recover from security violation and **restore information and systems** to a persistent state ❑ Examples include disaster recovery, business continuity plans, backup systems, and other processes
Compensating Controls	❑ Used as an alternative control when the **intended controls failed** or cannot be used ❑ Examples include hot sites, backup power systems, and other means

Location Considerations

1. Visibility of assets
2. Neighboring buildings
3. Local considerations
4. Impact of catastrophic events
5. Joint tenancy risks

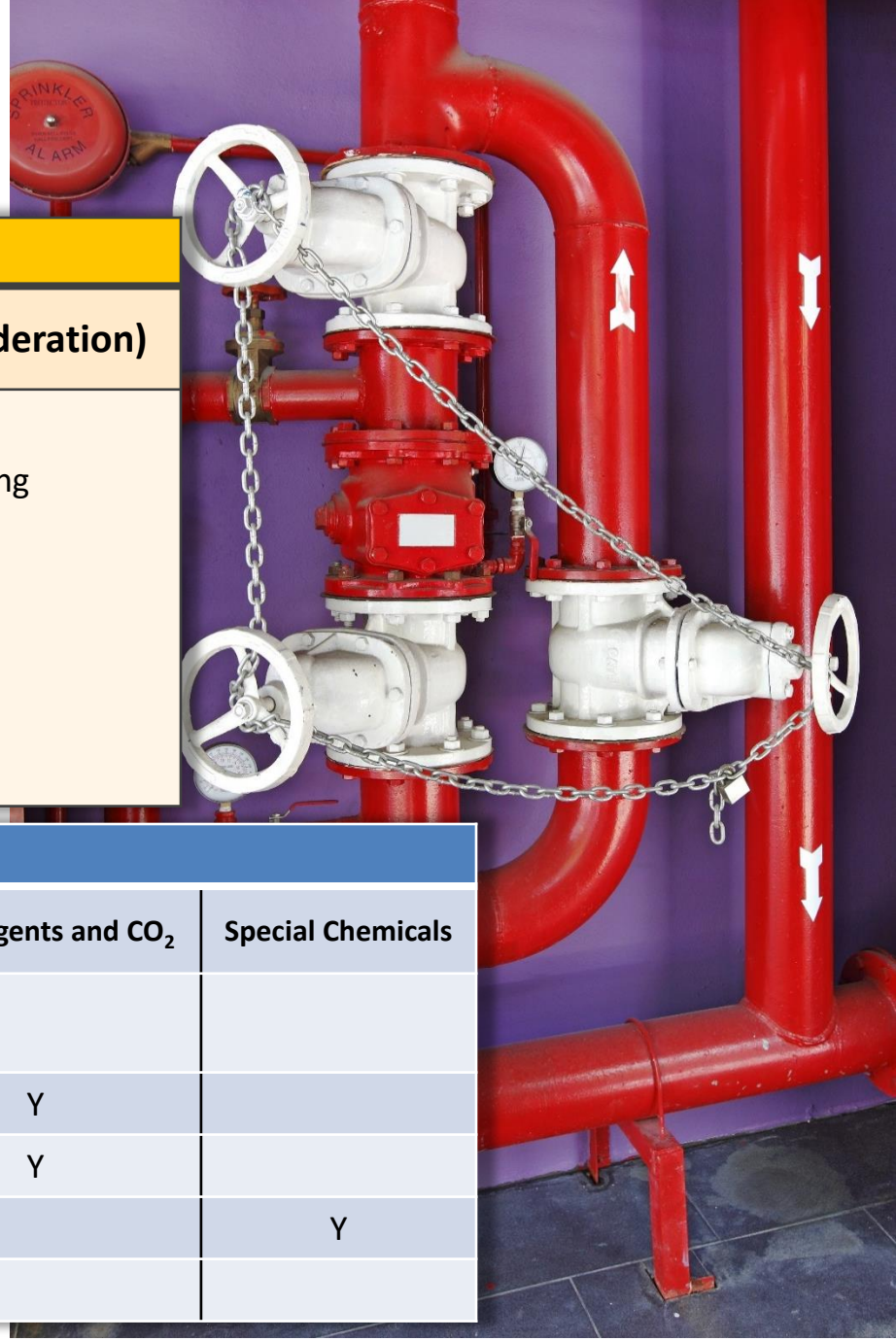


Site Architecture Considerations

- Identify what are the **critical infrastructures**
- Have a separate location for the server and storage room
- Identify what safety measures are required for these systems
- Have **emergency exits**
- Make plans to manage environment hazards
- Define who will be responsible for managing these systems
- Establish procedures explaining how they should be protected
- Use a proper **sanitation system** such as manholes, sewers etc.
- Keep parking away from the main building



Fire Fighting Systems



Types of Fire Fighting Systems	
Active fire protection (manual or automatic)	**Passive fire protection (structural consideration)**
❑ Fire detection • Smoke, flame and heat detectors ❑ Fire suppression • Fire extinguisher • Standpipe system • Sprinkler systems	❑ Use of fire-resistant construction materials ❑ Compartmentalization of the overall building ❑ Emergency exits ❑ Minimizing inflammable sources ❑ Maintenance of fire fighting systems ❑ Emergency procedures ❑ Educating the occupants

Fire Class	Fire Source	Suppressant					
		Water	Foam	Dry Chemical	Wet Chemical	Clean Agents and CO_2	Special Chemicals
A	Ordinary solid combustibles	Y	Y	Y	Y		
B	Flammable liquids & gases		Y	Y		Y	
C	Electrical equipment			Y		Y	
D	Combustible metals		Y				Y
K	Oils and fats		Y		Y		

Physical Barriers

- Physical barriers **restrict unauthorized people from entering the building**; always use a combination of barriers to deter unauthorized entry



Fences/Electric fences/Metal Rails

- First line of defense to stop trespassers



Bollards

- It is used to control vehicular and pedestrian traffic



Turnstiles

- It facilitates entry and access controls



Other Physical barriers

- Include doors, windows, grills, glass, curtains, etc.

Security Personnel

01

- Efficient and well trained **security personnel are critical to** implement, monitor, and maintain the physical security of organization

02

- People involved in physical security include guards, safety officer, plant's security officer/supervisor, etc.

Security personnel should be aware of:		
Physical security policies and procedures	Handling emergency situations	Patrolling procedures
First aid and medical assistance	Fire prevention	Trespassers and crowd management



Physical Locks

Types of Locks

Mechanical locks:
Uses a combination of springs, tumblers, levers, and latches, and operates by means of physical keys





Digital locks:
Requires a fingerprint, smart card or PIN authentication to unlock

Combination locks:
Requires a sequence of numbers or symbols to unlock





Electronic /Electric /Electromagnetic locks:
Uses magnets, solenoids and motors to operate by supplying or removing power

Concealed Weapon/Contraband Detection Devices

- Contraband includes materials that are banned from entering the environment such as **explosives**, bombs, weapons, etc.
- Use different tools such as handheld **metal detectors**, walkthrough metal detectors, X-ray inspection systems, etc. to detect contraband materials

Metal detectors



X-ray inspection systems

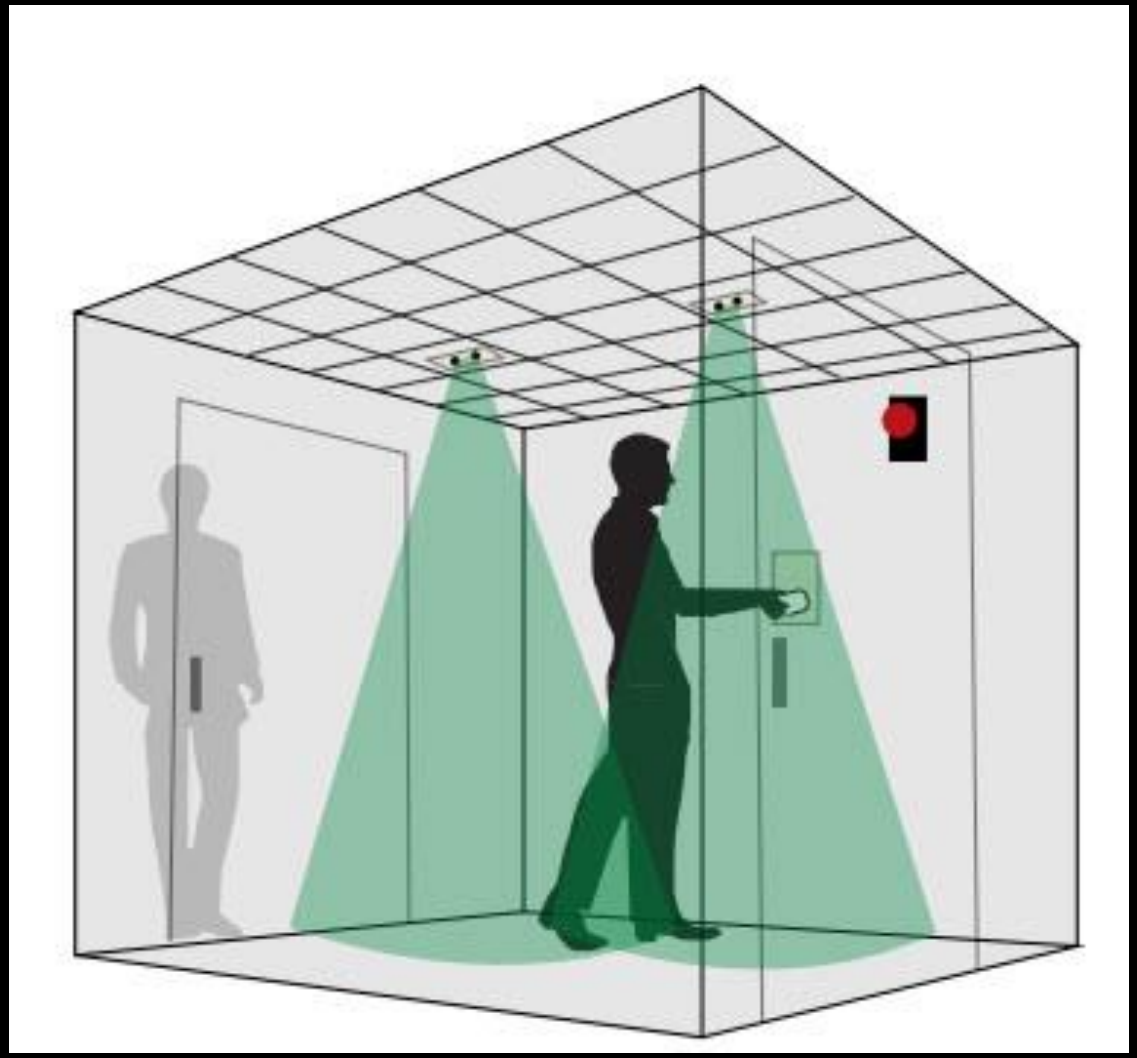


Walkthrough metal detectors



Mantrap

- security system
  separating non-secure area
- security personnel
- access
  control mechanisms



Warning Signs

Warning signs are used to ensure someone does not inadvertently intrude in any **restricted areas**

Appropriate warning signs should be placed at each access control point



Alarm System

Proper alarm systems should be installed inside and at the entrance to **report** intrusions**,** suspicious activity, and emergencies

It can be turned on either **automatically** or **manually** by smoke detectors, heat detectors, security personnel, etc.

It should be **audible** to everyone in the building and set at intervals of 5 minutes such as the first alert, second alert and then the final alert to evacuate



Video Surveillance

1. Video surveillance refers to **monitoring activities in and around the premises** using CCTV (Close Circuit Television) systems

2. CCTV systems can be programmed to **capture motion** and **trigger alarms** if an intrusion or movement is detected

3. Surveillance systems should be installed at strategic locations in and around the premises such as parking lots, reception, lobby, work area, server rooms, and areas having output devices such as printers, scanners, fax machine, etc.



Basic Types of CCTV Camera



Lighting System

Adequate lighting should be provided inside, outside, and at the entrance of the building which helps in seeing long distances during security patrols

Adequate lighting will **discourage intruders** from entering the premises and concealing behind stones, bushes, trees, etc.

Types of lighting systems:

- ✓ Continuous
- ✓ Standby
- ✓ Movable
- ✓ Emergency



Power Supply

- Use UPS (Uninterruptible Power Supply) systems to manage **unexpected power disruptions** or **fluctuations** in primary electric supply that may lead to equipment failure, business disruption or data loss

Different types of UPS systems (UPS Topologies):



Standby

- Most commonly used for personal computers



Line Interactive

- Most commonly used for small business, web, and departmental servers



Standby on-line hybrid

- Most commonly used for server rooms



Standby-Ferro

- No longer commonly used because it becomes unstable when operating a modern computer power supply load



Double Conversion On-Line

- Generally used in environments where electrical isolation is necessary



Delta Conversion On-Line

- Can be useful where complete isolation and/or direct connectivity is required

Module Flow

1 Understand the Importance of Physical Security

2 Discuss Various Physical Security Controls

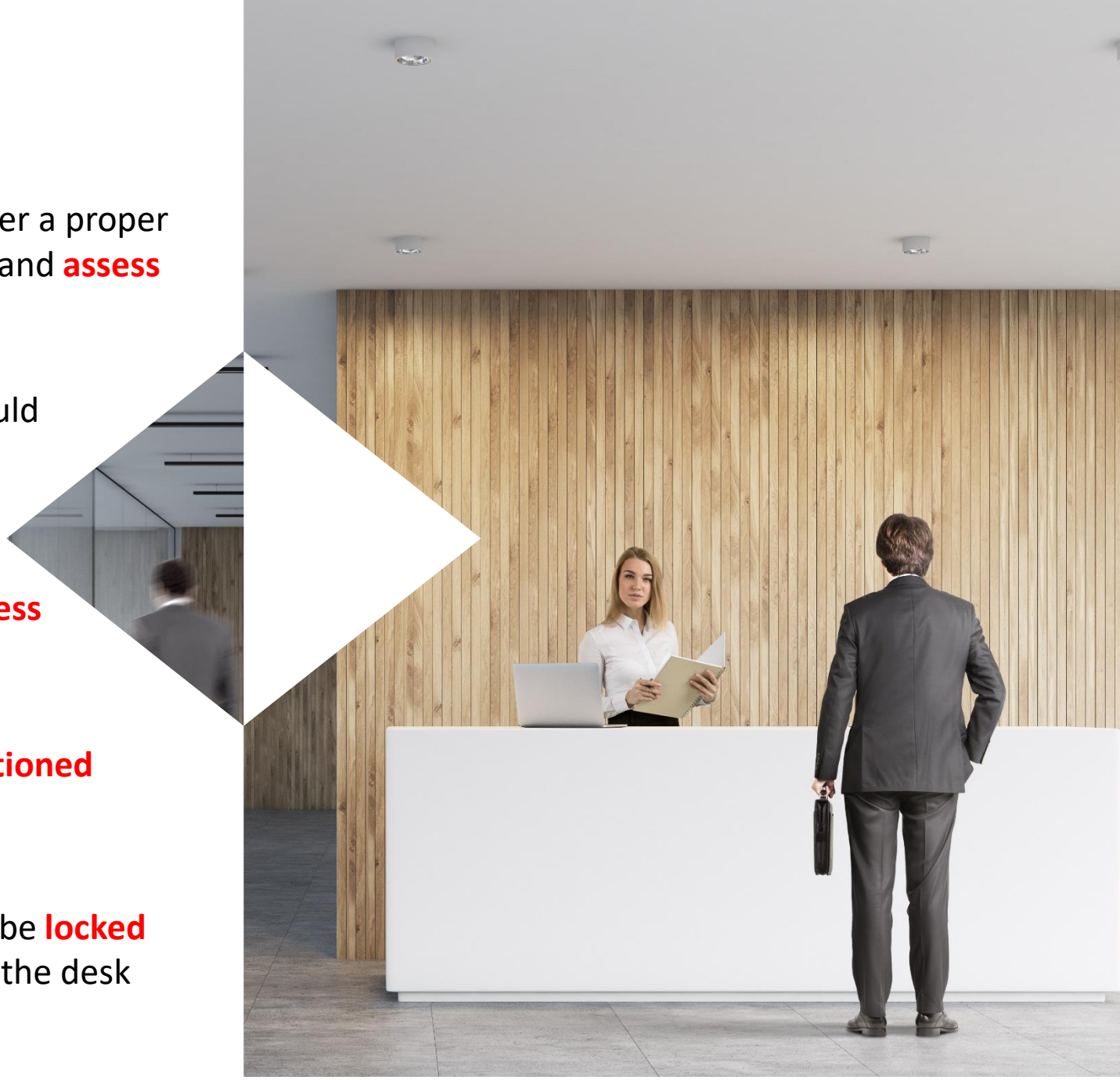


3 Describe Workplace Security

4 Describe Various Environmental Controls

Reception Area

- The reception area should be **spacious** and offer a proper scope to control building access, visitor traffic and **assess visitor's behavior**
- Important files and documents or devices should not be kept on the reception desk
- The design and placement of reception desks should help in **discouraging inappropriate access** to the administrative area
- Computers at a reception desk should be **positioned** so the screens are not visible to visitors
- Computers at the reception desk must always be **locked** when the receptionist personnel is away from the desk



Server/Backup Device Security

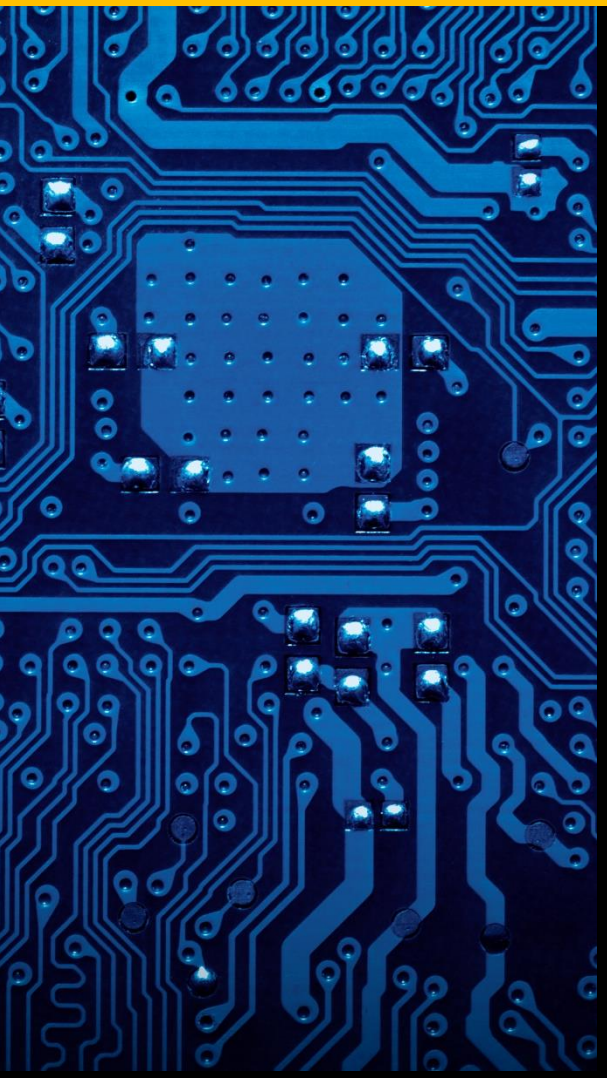


01 Keep critical network assets, such as servers and backup devices, in a **separate room**

02 Protect the server room and backup devices with an **appropriate access control**

03 Keep the server room and backup devices under **video surveillance**

Critical Assets and Removable Devices



locked cabinets

biometric locks

climate control features





acceptable-use policies

inventory

corporate-controlled

Securing Network Cables

01

electronic interference

02

03

transparent conduits

04

05

06

07

cable infrastructure







Securing Portable Mobile Devices

safeguard

impossible access

anti-theft software

device tracking

install erase

third parties

unattended

sticker

Physical Security Policy

- Physical security policy **defines guidelines** to ensure that adequate physical security measures are in place



Design Considerations

1. Is the **building protection deficiency** reviewed regularly?
2. Is there a process to **identify outsiders** such as visitors, contractors, and vendors before giving them access to the premises?
3. Are there adequate **lighting systems** in place?
4. Are each of the **entry points** properly blocked?
5. Are the badges, locks, keys, and authentication controls audited regularly?
6. Is **video surveillance** footage monitored regularly?
7. Is a proper **inventory** of an organization's assets maintained regularly?

Module Flow

1 Understand the Importance of Physical Security

2 Discuss Various Physical Security Controls



3 Describe Workplace Security

4 Describe Various Environmental Controls

Heating, Ventilation and Air Conditioning

- Continuous power consumption/supply makes data centers, hardware, and equipment become hot very quickly
- Improper equipment placement can increase the risk of fire
- **HVAC (Heating, Ventilation, and Air Conditioning)** systems control the surrounding environment in a room or building especially humidity, temperature, and air flow



- HVAC ensures the information system components are less prone to damage due to environmental changes
- Consider various factors and components such as **hardware**, **cabling**, **fire protection**, and **power supply**, etc. before installing the HVAC equipment
- Maintain baseline **temperature** and **humidity** levels to keep equipment working reliably

Electromagnetic Interference (EMI) Shielding

- EMI occurs when electronic device's performance is interrupted or degraded due to **electromagnetic radiation** or conduction

- High levels of disturbance can cause severe damage such as **shaky monitors**, system failures, unexplained shutdowns, etc.

- EMI shielding is a coating on electronic equipment kept in metal boxes which **block** emissions and radiation



Hot and Cold Aisles



- A hot and cold aisle is an arrangement of **server racks** and networking equipment to manage cold and hot air flow
- This arrangement isolates the cold and hot aisles from each other, by placing them in opposite directions

- Cold aisles typically face **air conditioner output ducts** and hot aisles should face **air conditioner input ducts**
- It saves the hardware from humidity and heat, increases hardware performance and maintains **consistent room temperature**

Physical Security Checklists

1. Ensure that proper access control methods are implemented to prevent unauthorized access
2. Ensure that sensitive areas are monitored with proper lighting
3.
4.
5.
6.



Module Summary

1. This module has discussed the importance of physical security, and its role in the organization's information security program
2. This module introduced you to the various physical security controls and security measures that organizations should consider while implementing physical security
3. This module also explained in detail on the importance of workplace security
4. Finally, this module ended with an overview on various environmental controls
5. In the next module, we will discuss on technical network security controls in detail

