EC-Council

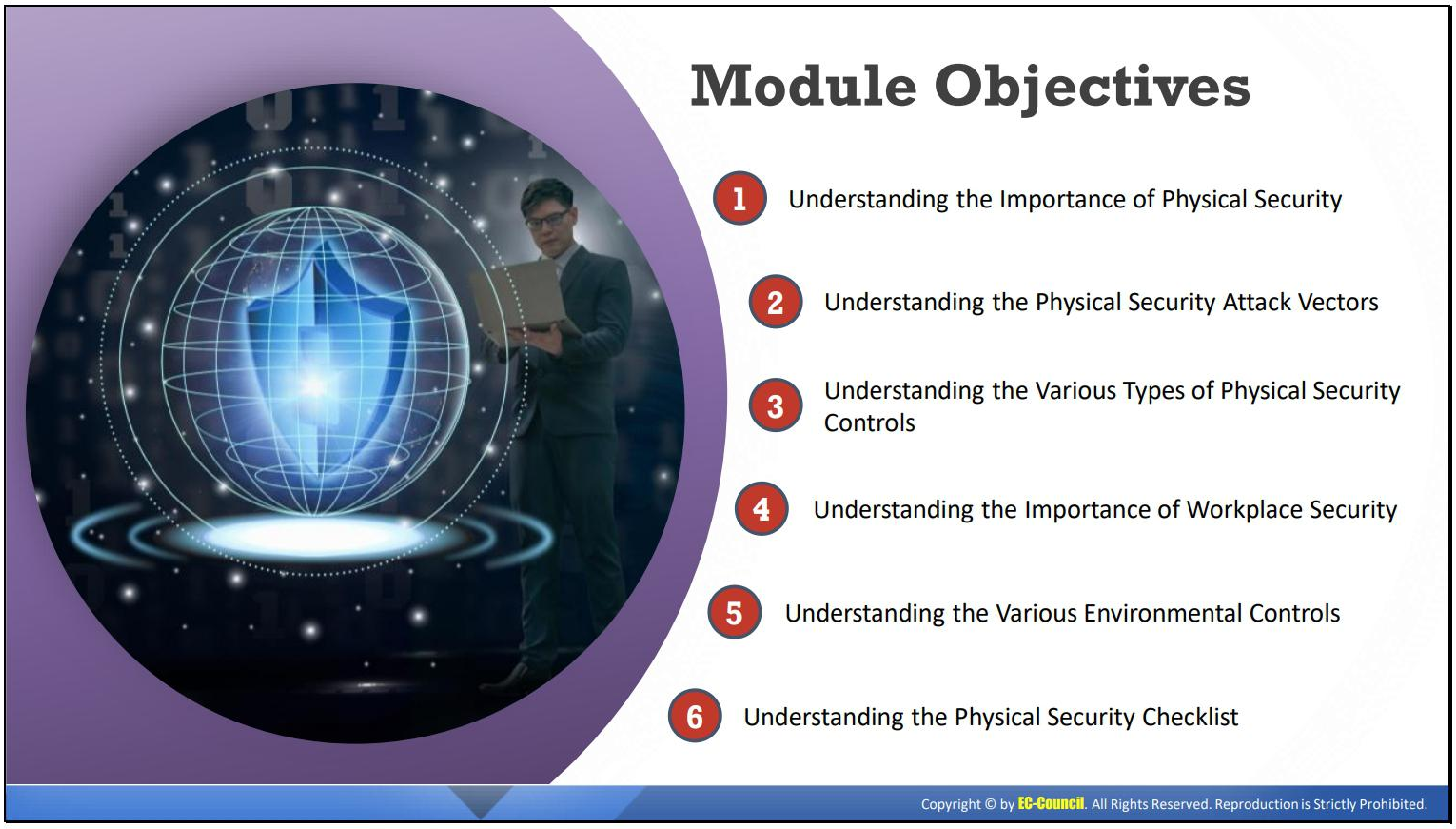
C|CT

Certified Cybersecurity Technician

Module - 06

Network Security Controls - Physical Controls

This page is intentionally left blank.



Module Objectives

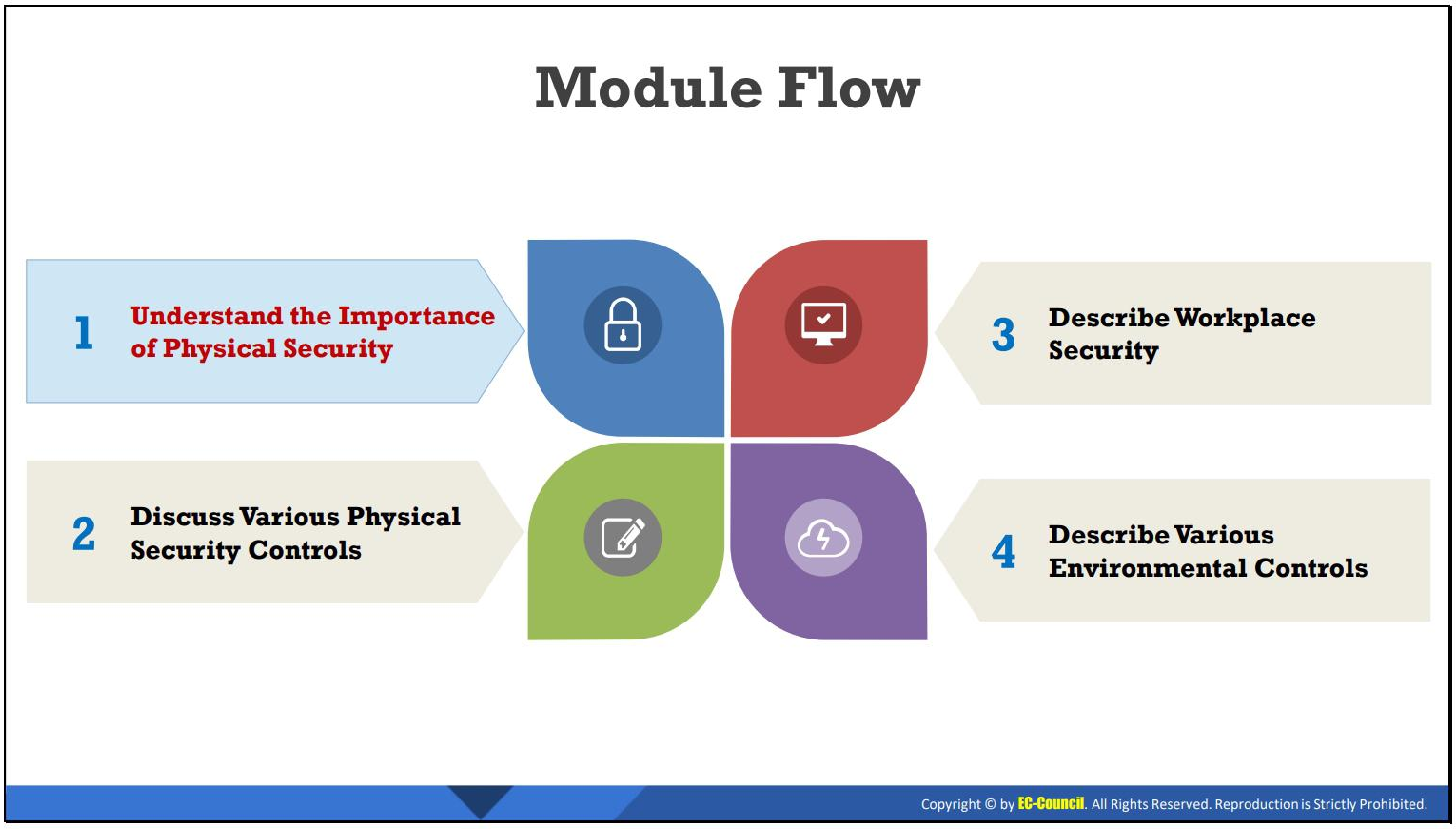
1. Understanding the Importance of Physical Security
2. Understanding the Physical Security Attack Vectors
3. Understanding the Various Types of Physical Security Controls
4. Understanding the Importance of Workplace Security
5. Understanding the Various Environmental Controls
6. Understanding the Physical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

Module Objectives

Physical security plays a major role in every organization. It entails the protection of critical information, network infrastructure, physical equipment and devices, facilities, personnel, etc. from environmental disasters, terrorism, vandalism, and theft. Physical security is becoming a challenging task with the increased usage of devices such as USB drives, laptops, smartphones, and tablets because malicious actors can easily gain physical access to such devices and steal sensitive data. This module explains the importance of physical security, various physical security controls, importance of workplace security, and various environmental controls.

At the end of this module, you will be able to:

- Understand the importance of physical security
- Understand the physical security attack vectors
- Describe the various types of physical security controls
- Explain the importance of workplace security
- Understand the various environmental controls
- Understand the physical security checklist



Module Flow

1 Understand the Importance of Physical Security

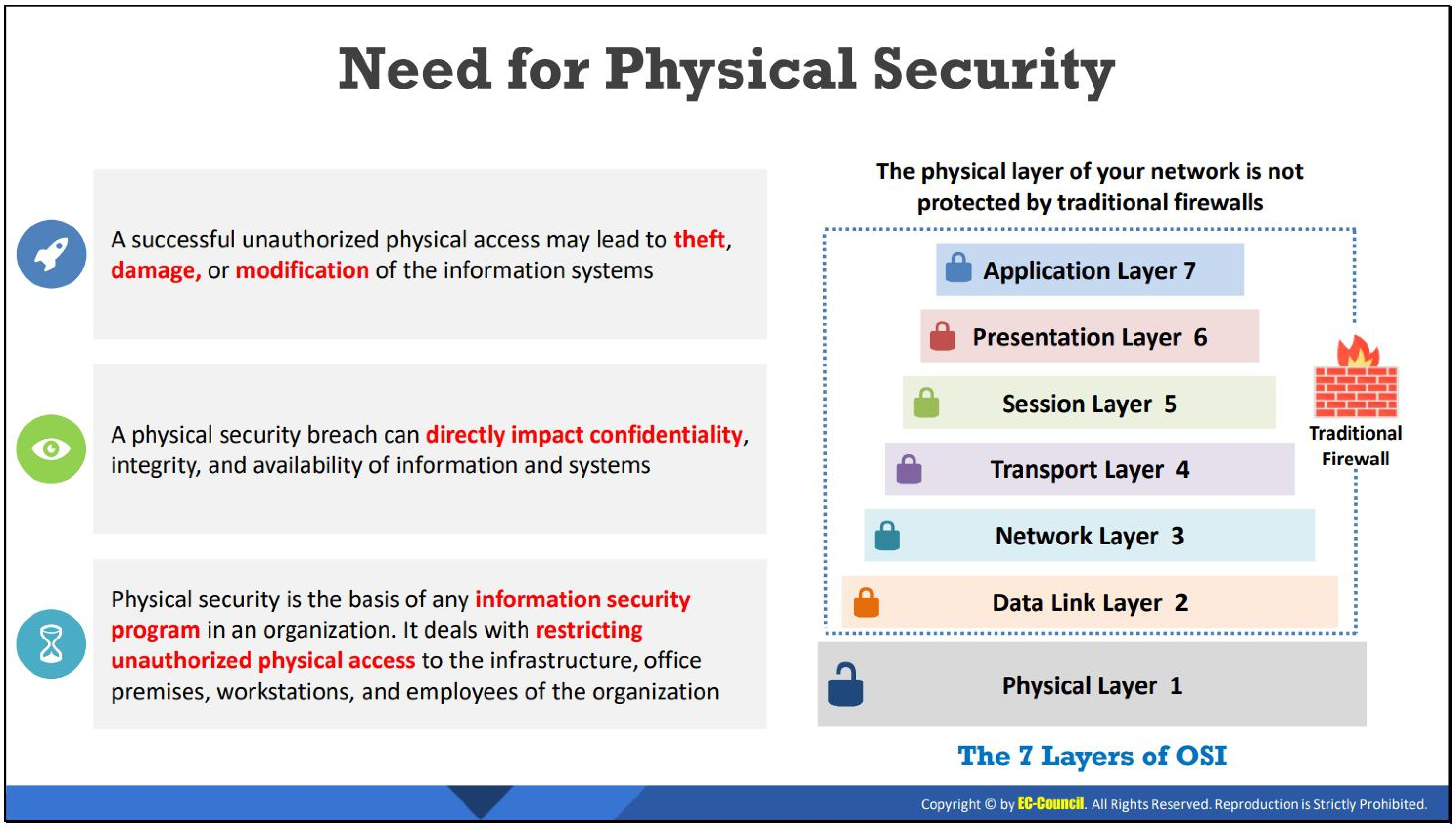
2 Discuss Various Physical Security Controls

3 Describe Workplace Security

4 Describe Various Environmental Controls

Understand the Importance of Physical Security

Physically safeguarding systems and networks is the top priority of network security. This section explains the importance of physical security in organizations.



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 physical layer of your network is not protected by traditional firewalls

The 7 Layers of OSI

Need for Physical Security

Although cyber-attacks are becoming increasingly complex, attackers continue to use various techniques to compromise the physical security of an organization. However, organizations are increasingly focusing on strengthening their IT security, which overshadows physical security. Physical security is the most overlooked aspect of security, and this fact has been brought to the notice of many organizations over the last five years. Knowing this fact, attackers are taking advantage of loopholes to compromise the physical security of organizations. According to data collected by the US Department of Health and Human Services Breach Portal, physical security breaches are among the most frequently occurring security incidents in organizations.

According to the findings of the fifth annual Horizon Business Continuity Institute (BCI) Scan Report, physical security is now perceived as a growing concern for business continuity professionals. According to this report, a degree of concern has been expressed with regard to the possibility of both an act of terrorism and a security incident such as vandalism, theft, or fraud disrupting the organization at some point.

Physical security breaches are vastly different from other security breaches. They can be performed with little to no technical knowledge. Physical security concerns arise because conventional security measures such as firewalls and IDSes do not ensure physical security. Deploying a firewall at various levels ensures security from different types of attacks but does not ensure the physical security of the organization. A conventional firewall is entirely unrelated to physical security as it works above the physical layer of the OSI model. Thus, conventional firewalls do not protect the physical layer of a network.

A successful attempt at unauthorized physical access may lead to the theft, damage, or modification of information systems. A physical security breach can directly impact the confidentiality, integrity, and availability of information and systems. Therefore, physical security forms the basis of any information security program in an organization. It entails restricting unauthorized physical access to the infrastructure, office premises, workstations, and employees of the organization.

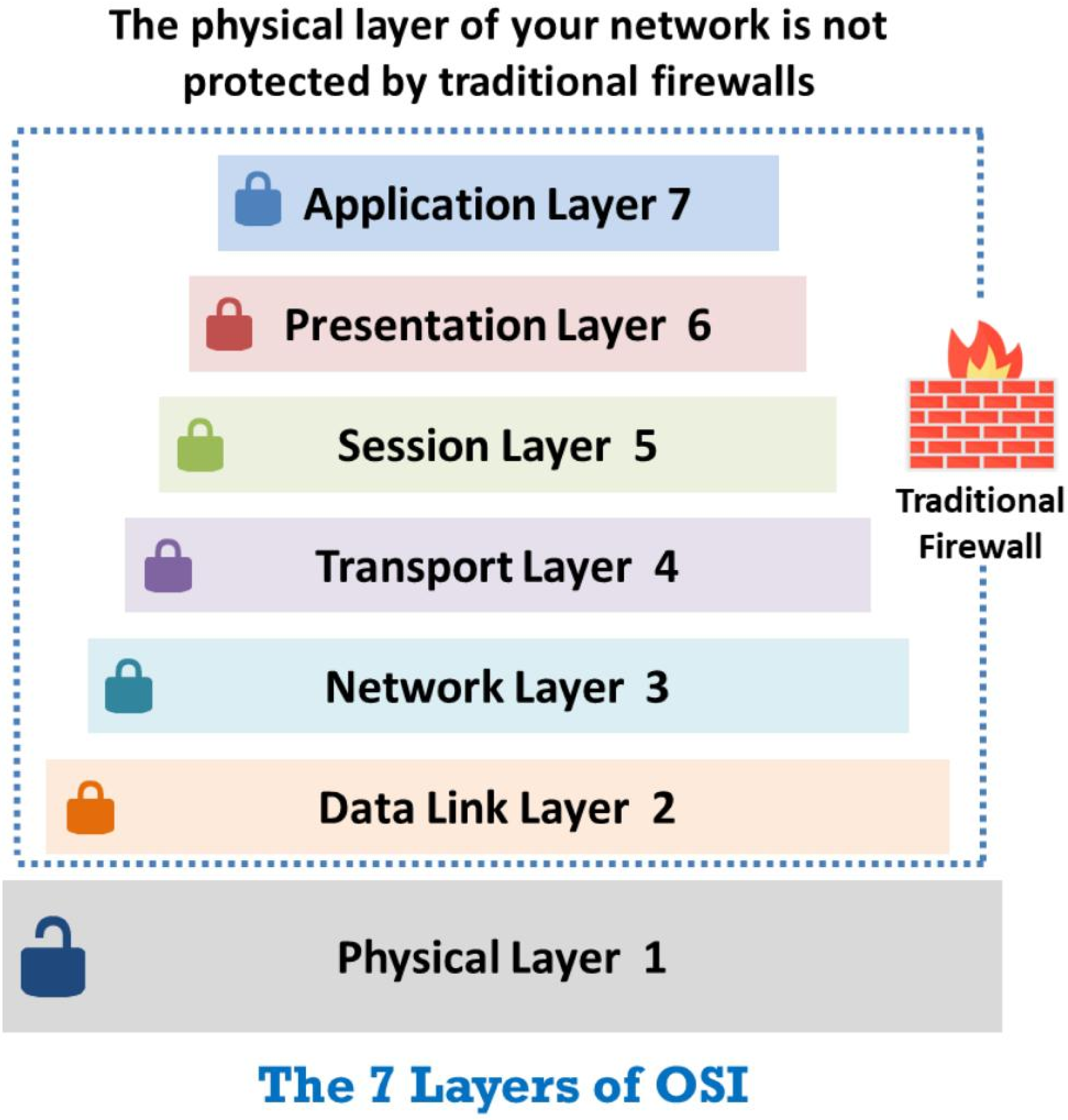
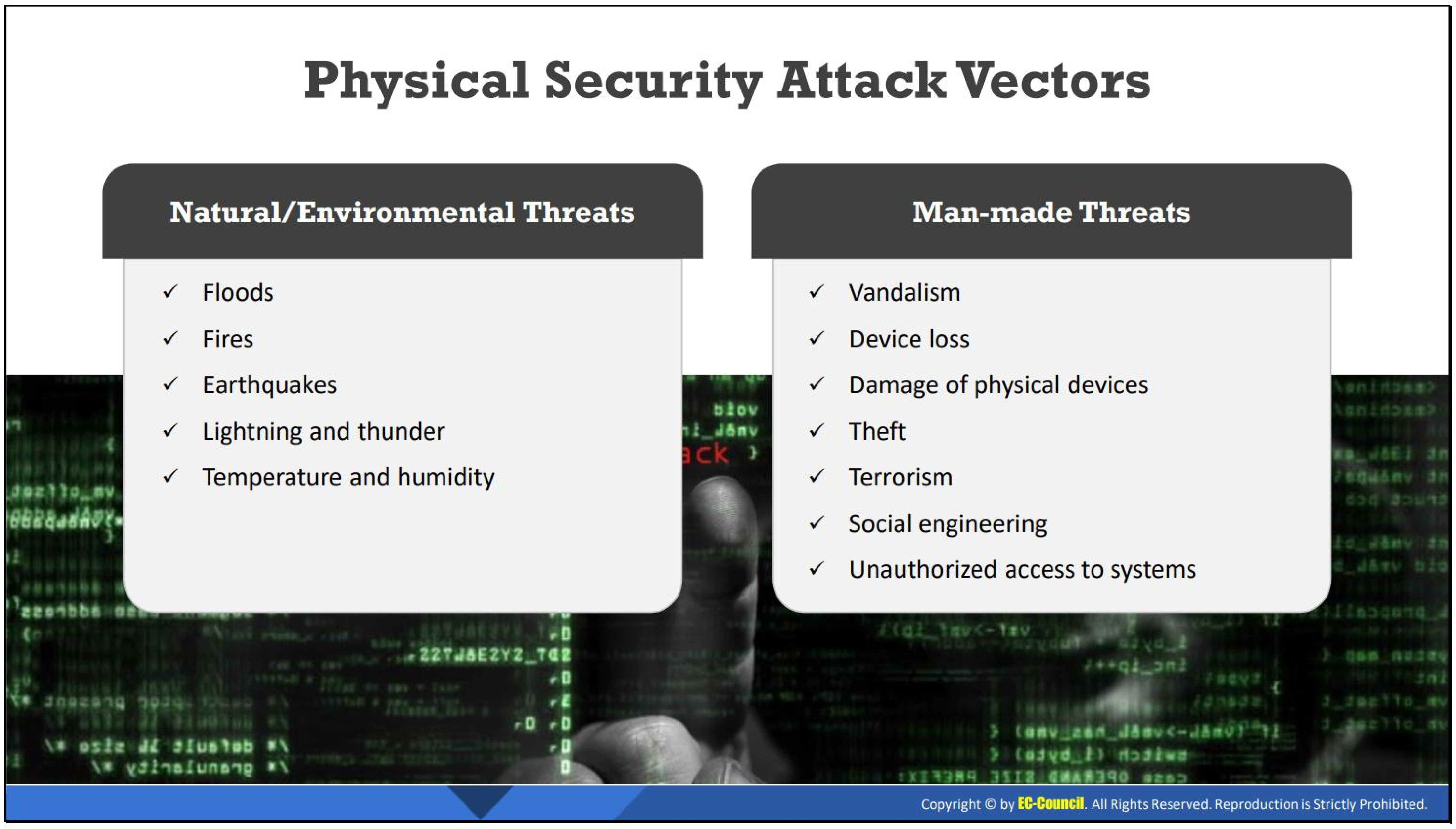


Figure 6.1: OSI layers and physical security

Physical security cannot be ensured in the same manner as network, application, or database security, and separate security measures are required for physical security. Physical security should be implemented at the physical layer of the OSI model.

A physical layer includes the following:

- All cabling and network systems
- Physical access to cables and systems
- Power support for cables and systems
- Environment supporting the systems



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

Physical Security Attack Vectors

Organizations are at a risk of the following types of physical security threats.

Natural/Environmental Threats

- **Floods:** Floods commonly occur because of heavy rains or the melting of ice. Floods may affect electrical systems and server rooms in an organization. Server rooms located in the basement have a greater chance of being affected by floods.

- **Fires:** Fires mainly occur because of short circuits or poor building materials. They may affect the operational facility and computer rooms in an organization. Fires can damage the hardware, cabling system, and other important components.

- **Earthquakes:** An earthquake is the sudden release of stored energy in the Earth's crust that creates seismic waves. It disrupts the physical infrastructure in an organization. It damages computers and other hardware devices and documents in the sensitive areas inside an organization. Moreover, it can affect the safety or security of the organization. Earthquakes mainly affect the cabling, the wiring system, and the physical building itself. Any damage to the cabling system affects the working of the computer systems.

- **Lightning and thunder**: Lighting and thunder occur because of environmental changes. It necessitates the shutdown of all outdoor activities. Lightning and thunder lead to power and voltage fluctuations that, in turn, affect the working of systems. In particular, it may affect the memory chips and other hardware components of a system. It may lead to a short circuit in the cabling and other wiring systems if they are not covered properly. The information system may stop working with one lightning strike. Lightning may damage all electrical and electronic appliances and lead to the loss of all sensitive information.

- **Temperature and humidity**: Computer systems operate in a certain range of temperatures; otherwise, they function in an inappropriate manner. Computer systems do not work well in hot areas and may become damaged if the temperature increases or decreases by extreme amounts. Although every computer has cooling systems, the performance of a computer still depends on the exterior temperature conditions. Furthermore, electrical and electronic appliances in an organization may be affected by a change in humidity. A high humidity leads to issues such as corrosion and short-circuits and damages magnetic tapes and optical storage media. A low humidity affects electronic devices mainly through electric discharge.

Man-made Threats

The most significant threat to physical components and the network is from man-made errors, both intentional and unintentional. There is a wide range of such possibilities, including hackers/crackers, theft, fire, and human error. Some examples of human error that may lead to man-made threats are the unintentional pressing of an incorrect button and unplugging of the wrong device. Typical man-made threats include mechanical errors, electrical disturbance, pollution, radio-frequency interference, and explosion.

- **Vandalism**: Disgruntled employees or former employees may attempt to compromise a system by willingly breaking or harming system components. During civil unrest or a disaster, there is a chance of systems being mishandled.

- **Device loss**: Unauthorized access may lead to the loss of important information and devices. Device theft is a concern if devices are not properly secured.

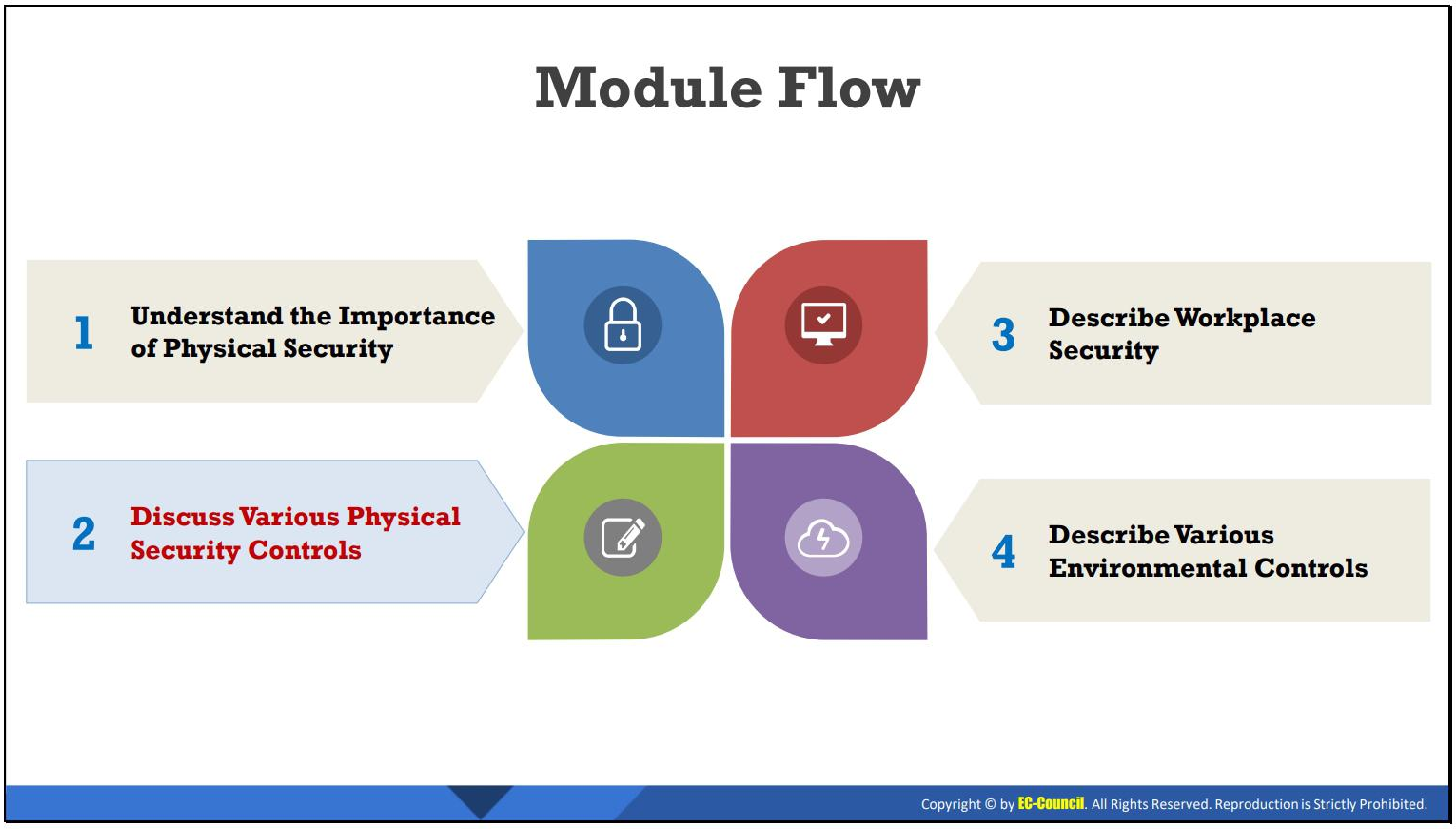
- **Damage to physical devices:** Improper device maintenance activities such as the improper handling of a device or information, failure to replace damaged devices, and poor cabling can damage physical devices to a great extent.

- **Theft:** Lack of proper security and locks may result in equipment theft.

- **Terrorism:** Terrorism activities such as the planting of a vehicle bomb, human bomb, or postal bomb in and around the organization’s premises impact physical security in many ways.

- **Social engineering:** Social engineering is defined as an illegal act of acquiring personal information from people. An attacker can gain unauthorized physical access by performing social engineering on an organization’s employees.

- **Unauthorized access to systems**: Both internal and external users can attempt to gain unauthorized access to a system or information about the organization.



Module Flow

1 Understand the Importance of Physical Security

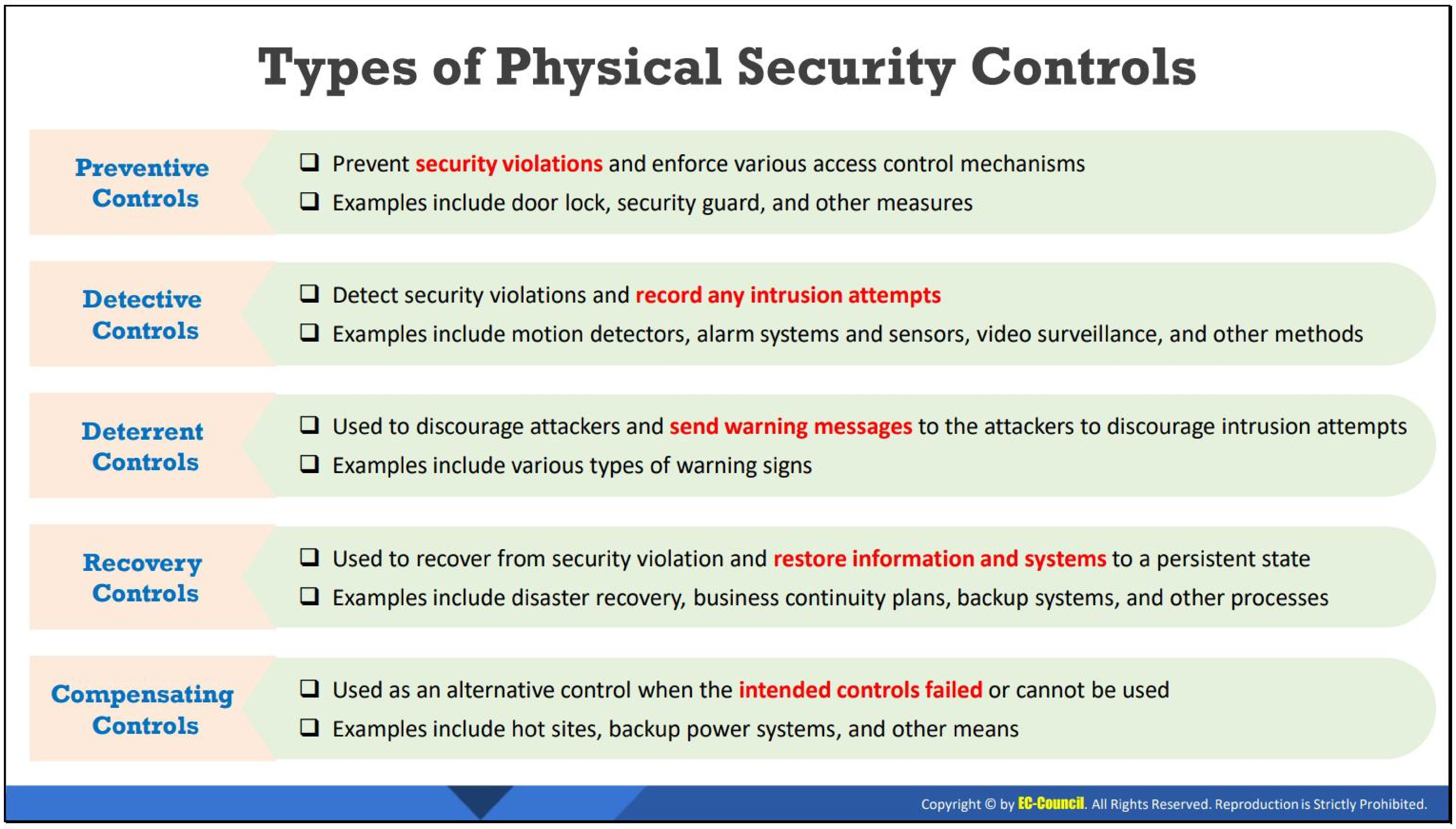
2 Discuss Various Physical Security Controls

3 Describe Workplace Security

4 Describe Various Environmental Controls

Discuss Various Physical Security Controls

This section explains various physical security controls that can be used in organizations.



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

Types of Physical Security Controls

Physical security controls are categorized based on their functionality and the plane of application. Based on their functionality, the types of physical security control include the following.

- **Preventive Controls**

  These controls prevent security violations and enforce various access control mechanisms. Preventive controls may be physical, administrative, or technical. Examples include door locks and security guards.

- **Detective Controls**

  These controls detect security violations and record any intrusion attempts. They act when preventive controls fail. Examples include motion detectors, alarm systems and sensors, and video surveillance.

- **Deterrent Controls**

  These controls may not prevent access directly. They are used to discourage attackers and send warning messages to them to discourage an intrusion attempt. Examples include various types of warning signs.

- **Recovery Controls**

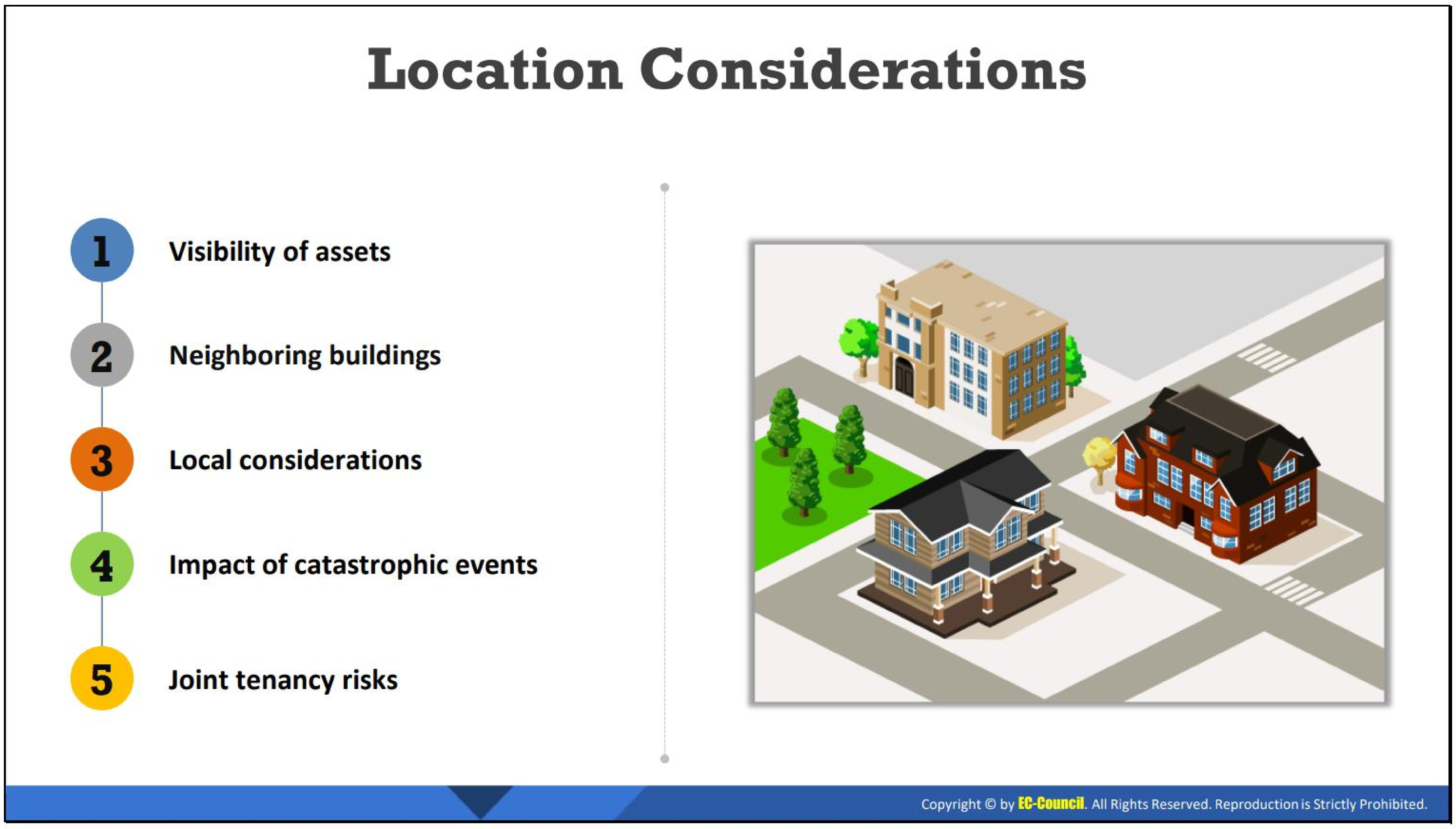
  These controls are used in serious situations to recover from security violations and restore information and systems to a persistent state. Examples include disaster recovery, business continuity plans, and backup systems.

- **Compensating Controls**

  These controls are used as alternatives when the primary controls fail or cannot be used. They do not prevent any attack attempt but attempt restoration using techniques such as restoring from a backup. Examples include hot sites and backup power systems.

Based on the plane of application, the types of security controls include the following.

- Physical security controls such as doors, secure facilities, fire extinguishers, and flood protection
- Administrative security controls such as the organization’s policies, procedures, and guidelines to provide information security
- Technical security controls such as IDSes/IPSes, firewalls, and authentication systems

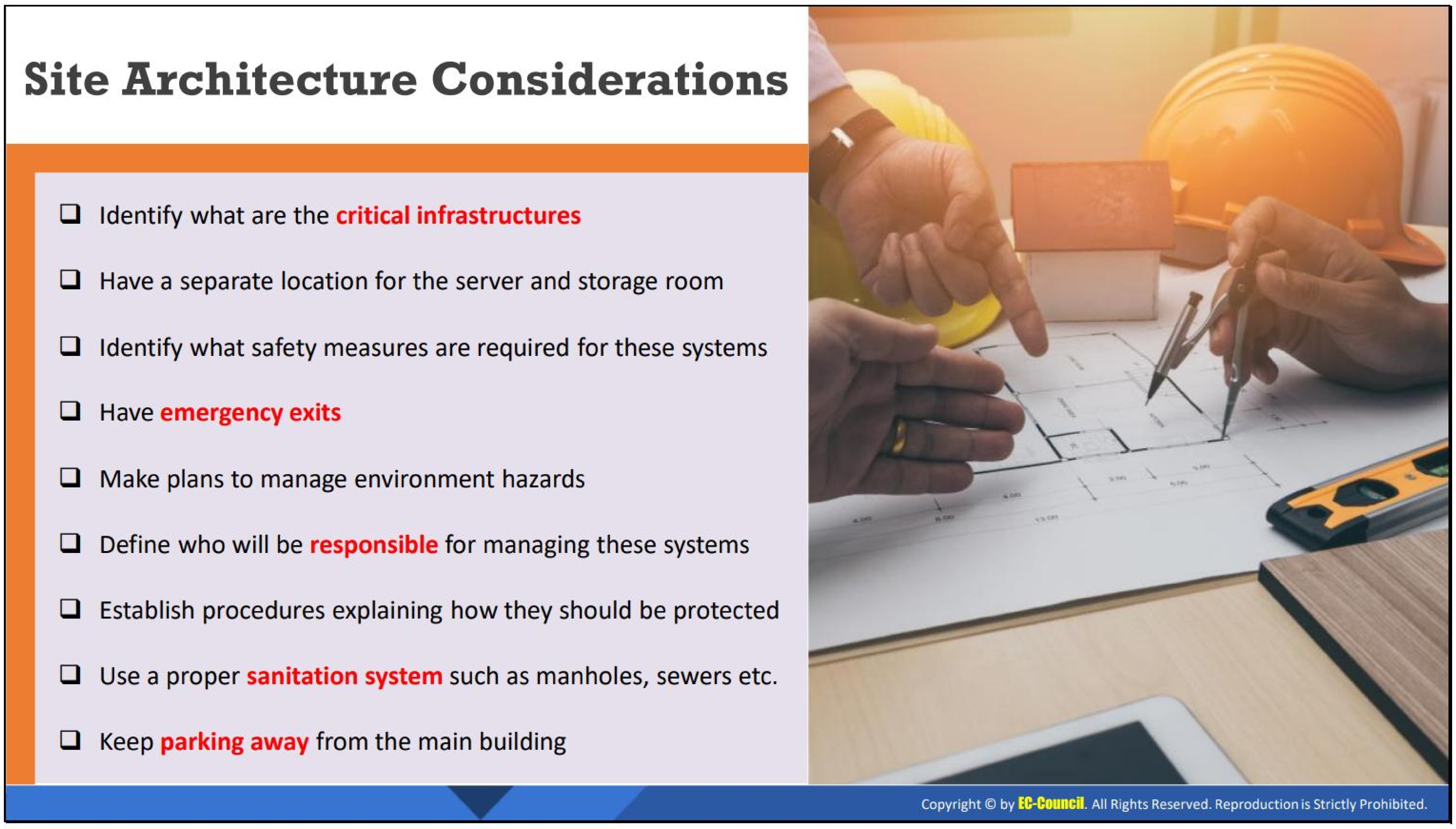


Location Considerations

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

Location Considerations

Organizations should consider various factors that may affect physical security before planning to buy or lease a building. The factors to consider may include the facility location, neighboring buildings, joint tenancy risks, power and water supply, sewage systems, proximity to public and private roads, transportation, emergency support, fire stations, hospitals, airports, local crime or rate of riots, and prior security incidents in the surrounding area. The location should not be prone to natural disasters such as floods, tornadoes, earthquakes, hurricanes, excessive snow or rainfall, mudslides, and fires.



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

Site Architecture Considerations

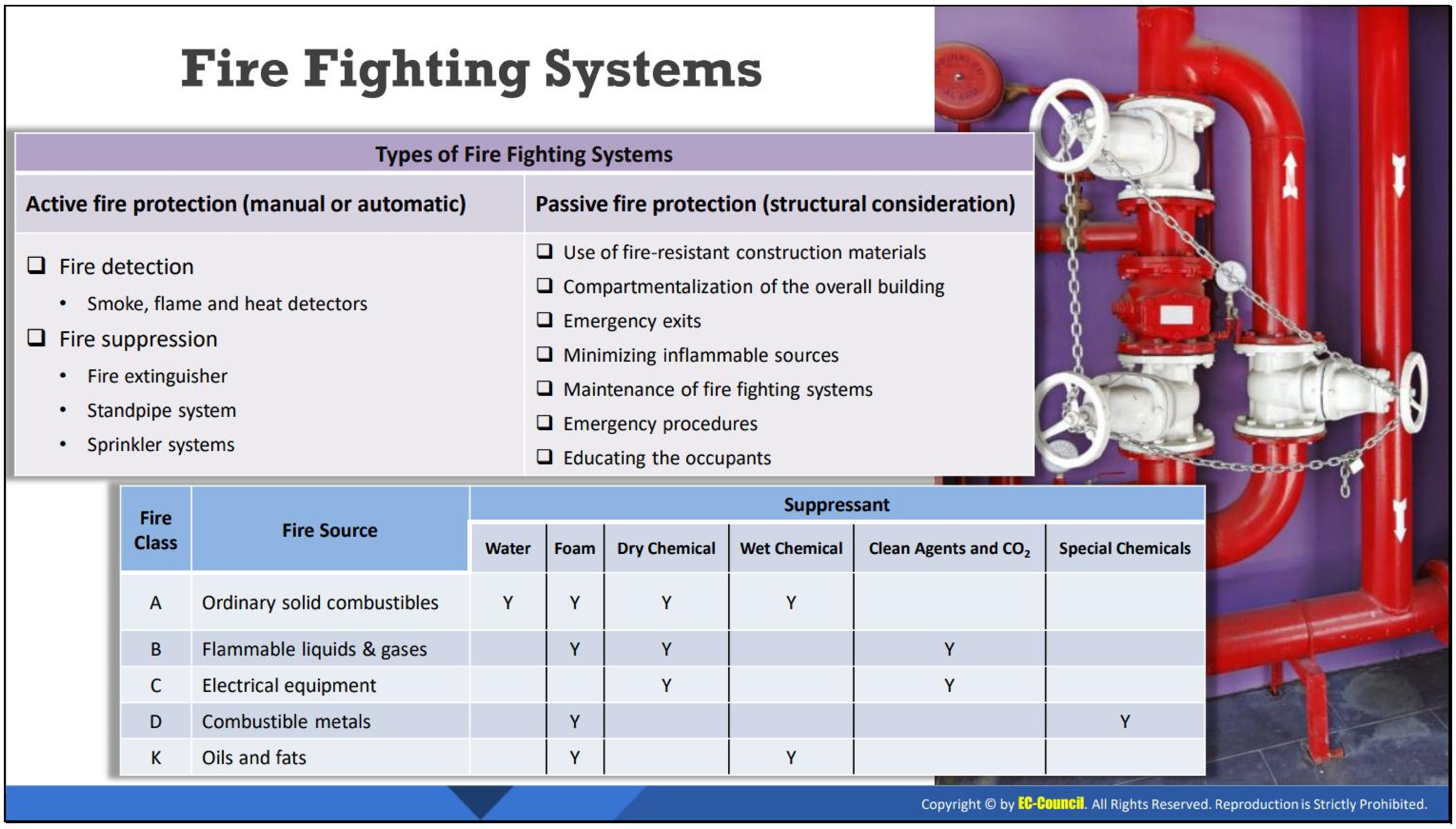
After gaining adequate information about the facility location, the planning and designing of the internal infrastructure and architecture should be performed. While planning and designing the site architecture, an organization should prepare a list of all of its assets in the facility.

The organization should consider the following points while designing the infrastructure and architecture.

- Decide the number of entrances required for the building, including the main entrance, staircase, parking, lift, hallway, and reception area.
- Find the neighboring facilities around the site location and check the internal and external architecture for them. Talk to the supervisors or owners of the buildings to gain additional insights about the surroundings.
- Analyze the assets that can be impacted by catastrophic failures as well as the visibility of assets to outsiders.
- Consider the joint tenancy factor; if the facility is shared with other companies, consider their impact on the organization's sensitive information and critical assets.
- Identify the necessary critical infrastructure that is required for managing the physical security, storing sensitive data, and running business operations effectively.
- Design separate security zones to place critical components and equipment deep inside the premises without any direct contact with entry doors, compound walls, and windows.
- Establish a demilitarized zone (DMZ) between highly secure infrastructure and public-access areas.

- Ensure a separate location for the server and storage room.
- Identify what safety measures are required for these systems.
- Use security labels and warning signs wherever necessary to make visitors understand that tight security is implemented within the premises.
- Ensure that public areas having high accessibility are under complete and simplified surveillance.
- Implement emergency exits.
- Make plans to manage environmental hazards.
- Define who will be responsible for managing these systems.
- Establish procedures explaining how they should be protected.
- Use a proper sanitation system including manholes and sewers.
- Keep parking away from the main building.
- Communicate physical security control procedures and policies with the employees, tenants, stakeholders, and administration to minimize physical security threats such as insider theft, fraudulent activities, and collusion.
- Restrict the movement of people between different zones.

These critical infrastructure systems may not use standard IT for safety, performance, and reliability, but they are critical to business operations. An improper or faulty implementation of certain physical measures such as electricity, backup, storage facilities, lighting, wiring, and cooling systems can be critical to the business operations of the organization.



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		

Fire Fighting Systems

Fire is an incident that can occur with or without warning and is usually attributed to man-made errors, short circuits, and defective or faulty equipment. Fire protection is an important aspect of physical security. Firefighting systems mainly detect fire incidents and alert the occupants to them. Fire incidents may be identified either manually or automatically.

The types of firefighting systems include the following.

Active Fire Protection

Active fire protection alerts the occupants of an organization regarding a fire incident. This type of fire protection system is generally used in commercial places, process industries, and warehouses to protect storage vessels, processing plants, etc. The main aim of implementing an active fire protection system is to control the spread of fire and extinguish it as soon as possible, thereby facilitating the clearance of occupants in an organization. The system requires a certain number of actions to handle fire incidents. These actions may be performed either manually or automatically.

Certain active fire systems include water sprinklers, fire/smoke alarm systems, spray systems, and fire extinguishers. Fire/smoke alarms indicate the presence of any fire or smoke in the building. Water sprinklers reduce the spread of fire, and fire extinguishers help put out fire. Water sprinklers fall under the category of automatic fire protection systems, whereas fire extinguishers and standpipes fall under the category of manual fire protection systems.

Active fire protection systems include the following.

- **Fire detection system:** A fire detection system helps detect a fire incident before allowing the fire to spread.

Automatic fire detection systems include the following components.

- **Smoke detectors:** Smoke detectors generally detect smoke and send alerts about the suspected fire incident in an organization. Upon detection of smoke, the detectors send an alarm to the fire alarm control panel or generate an audio/visual alarm.

- **Flame detectors:** Flame detectors mainly detect flames in a fire incident. Flame detectors normally include sensors that detect flames. The working of a flame detector is as follows:

  - An alarm is generated on fire flame detection.

  - Gas supply is cut through the fuel line.

  - The fire suppression system is activated.

  Flame detectors work more efficiently and faster than smoke detectors and heat detectors.

- **Heat detectors:** Heat detectors are used to detect and respond to the thermal energy generated by fire incidents. Heat detectors are further classified into fixed-temperature heat detectors and rate-of-rise heat detectors.

- **Fire suppression:** A fire suppression system is used to extinguish fire without much human intervention. Fire suppression systems regulate destruction and device loss. They can be classified into manual and automatic. Commonly used fire suppression systems include the following.

  - **Fire extinguisher:** Fire extinguishers aim to extinguish fires at the initial stage. They are not useful in the case of a fire covering a large area. A fire extinguisher normally consists of an agent that is discharged inside a cylindrical vessel. Fire extinguisher systems need to be checked often to ensure that they work properly in case of fire. Fire extinguishers are usually inspected yearly or bi-yearly by trained professionals. They can also be recharged.

    Dry chemicals, water, wet chemicals, water additives, clean agents, and carbon-dioxide are used as agents in fire extinguisher systems. Below table provides details for selecting the proper extinguisher based on various types of fire sources.

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		

Table 6.1: Classification for Fire Extinguishers

- **Standpipe system:** Standpipe systems connect hose lines to the water supply. They provide a pre-piped water system for organizations as well as water supply to hose lines in certain locations. The three types of standpipe systems are Class I – A, Class II – A, and Class III – A. These types differ in terms of the thickness of the hose lines used and the volume of water used for fire suppression.

- **Sprinkler system:** Fire sprinkler systems maintain a water supply system to supply water to a water distribution piping system that controls sprinklers. The sprinklers are used to avoid loss to human lives and assets. These are mainly used in areas that firefighters cannot reach with their hose lines.

Wet-pipe fire sprinklers are not optimal for sub-freezing areas because any damage to sprinklers or piping may lead to water leakage and water damage. As an alternative solution, the following fire sprinklers can be used.

- **Dry-pipe sprinklers**: Dry-pipe sprinklers are generally used in locations where freezing is expected, i.e., where the temperature is below 40 °F. Dry-pipe systems are suitable for sub-freezing environments as nitrogen or air is maintained completely within the pipe. When the sprinkler is activated, the nitrogen or air is released from the activated pipe, minimizing the pressure, and water is released from the sprinkler.

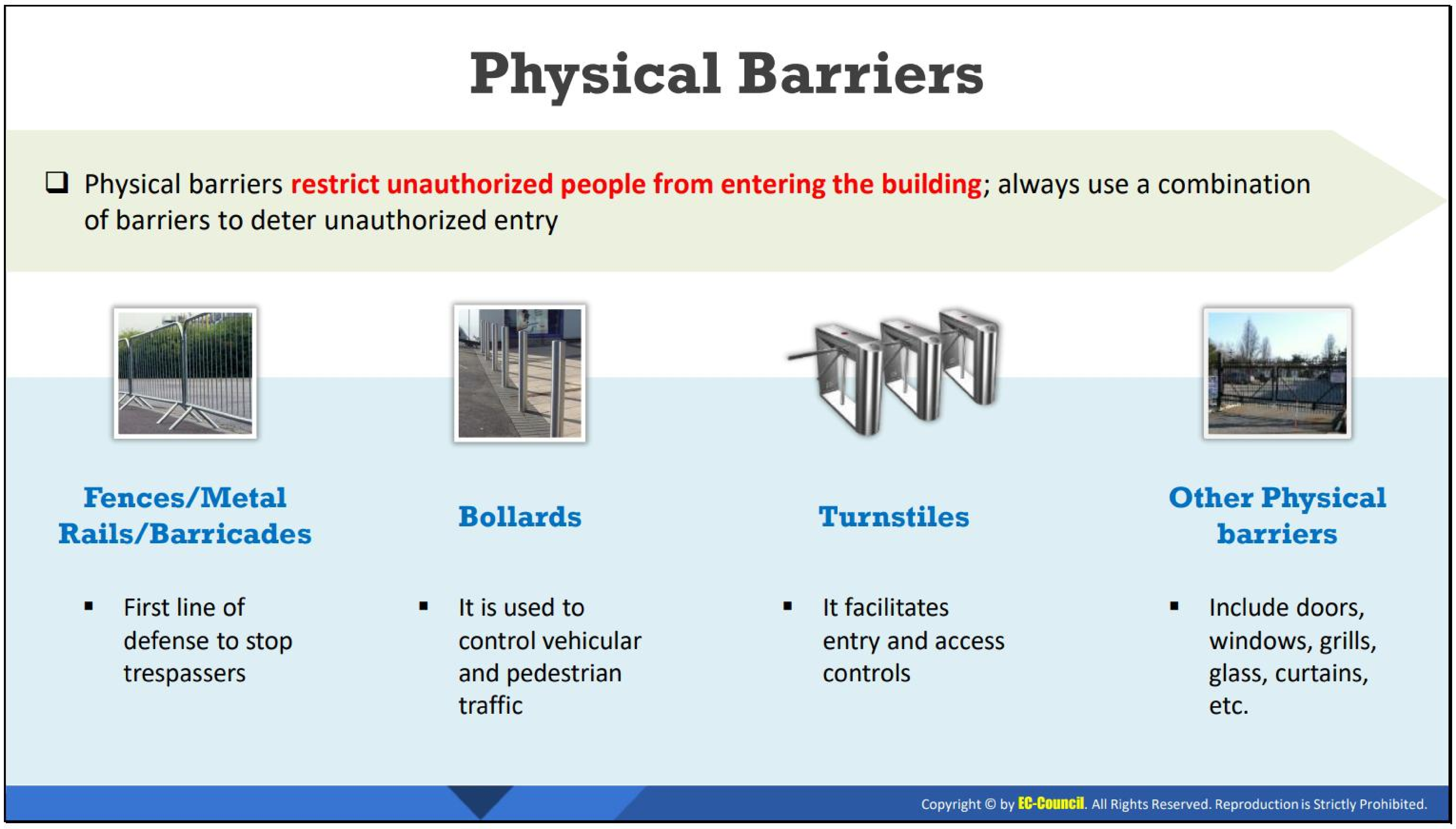
- **Pre-action sprinklers**: Pre-action sprinklers are employed in locations that are susceptible to water damage; they reduce accidental water discharges. Similar to dry-pipe sprinklers, pre-action pipes maintain nitrogen or air within the pipes or sprinklers, but in contrast to dry-pipe sprinklers, pre-action sprinklers hold the water from the sprinkler using electrically operable valves. The valves are operated based on the alerts received from detection systems.

  - **Deluge system**: A deluge system can be used in highly dangerous areas where high volumes of water are required to control fire or heat. In a deluge system, sprinkler heads are always open; hence, pipes are not pressurized. Like pre-action sprinklers, they are also managed by electrically operable valves. Upon activating the system, water fills into the sprinklers and is released immediately and simultaneously over the entire environment.
  - **Foam-water sprinkler system**: It is a special type of sprinkling system that contains "foam-water" sprinklers that release a solution or mixture of foam and water at a specified flow rate when activated. Foam-water sprinkler systems are generally used in environments containing flammable liquids. Such systems are also managed by automatic deluge valves that are activated by a heat detection device, and the solution is distributed across the environment that needs to be protected.
  - **Clean-agent suppression system**: This type of system employs an inert gas or chemicals to control a fire that is in the initial stage of growth or development. A clean-agent suppression system can be used in public places where no costly clean-up is needed after its discharge. The cleaning agents are stored in a liquid or gas form and are released as a cleaning solution to suppress the fire before it causes severe damage.

Passive Fire Protection

Passive fire protection systems are used to prevent fire from spreading further across the organization. Fire-resistant doors, windows, and walls may be used for passive fire protection. It facilitates the protection of the building's occupants and reduces the rate of damage due to the fire. Passive fire protection systems do not need to be activated by other systems, and no operational assistance is required in implementing passive fire protection systems.

- Passive fire protection is implemented in the following ways:
  - Minimal use of flammable materials
  - Building additional floors and rooms in a building to slow down the spread of fire
  - Providing adequate training to the occupants regarding the procedures to follow in case of fire
  - Proper maintenance of fire-related systems
  - Adequate number of emergency exits
- The following are the steps to manage fire incidents:
  - Detect fire.
  - Evacuate occupants in the building to a safe location.
  - Notify the fire department and safety department regarding the fire.
  - Shut down all electrical and electronic systems to prevent the fire from spreading.



Physical Barriers

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

Fences/Metal Rails/Barricades

- 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.

Physical Barriers

Many factors determine the physical security of an organization. These factors are essential considerations and contribute to the successful operation of physical security in an organization. The main goal of physical security is the control and prevention of unauthorized access, while physical barriers restrict unauthorized people from entering the building. Physical barriers define the physical boundary of an area and divide vehicle traffic from pedestrians. The use of a physical barrier deters and delays outsiders from entering the premises. An intruder or outsider can compromise a barrier by spending time and money as well as planning and contemplating on the site architecture. To discourage these intruders, it is a good policy to use a multilayer approach that includes external barriers, middle barriers, and internal barriers. External barriers include fences and walls; although they are built to form a structure, they inadvertently act as an obstruction. Middle barriers are equipment used to obstruct traffic and people. Internal barriers include doors, windows, grills, glass, and curtains.

The following are different types of physical barriers used in a building.

- **Fences/electric fences/metal rails:** These form the first line of defense against a trespasser and are the most commonly used type of physical barriers worldwide. Fences/metal rails/electric fences generally mark restricted and controlled areas and prevent unauthorized access.

  The aim of deploying physical barriers is as follows:

  - Block and deter attackers
  - Mark the boundary of the organization
  - Protect security guards from external attacks

  - Prevent the entry of vehicles
  - Protect against explosive attacks

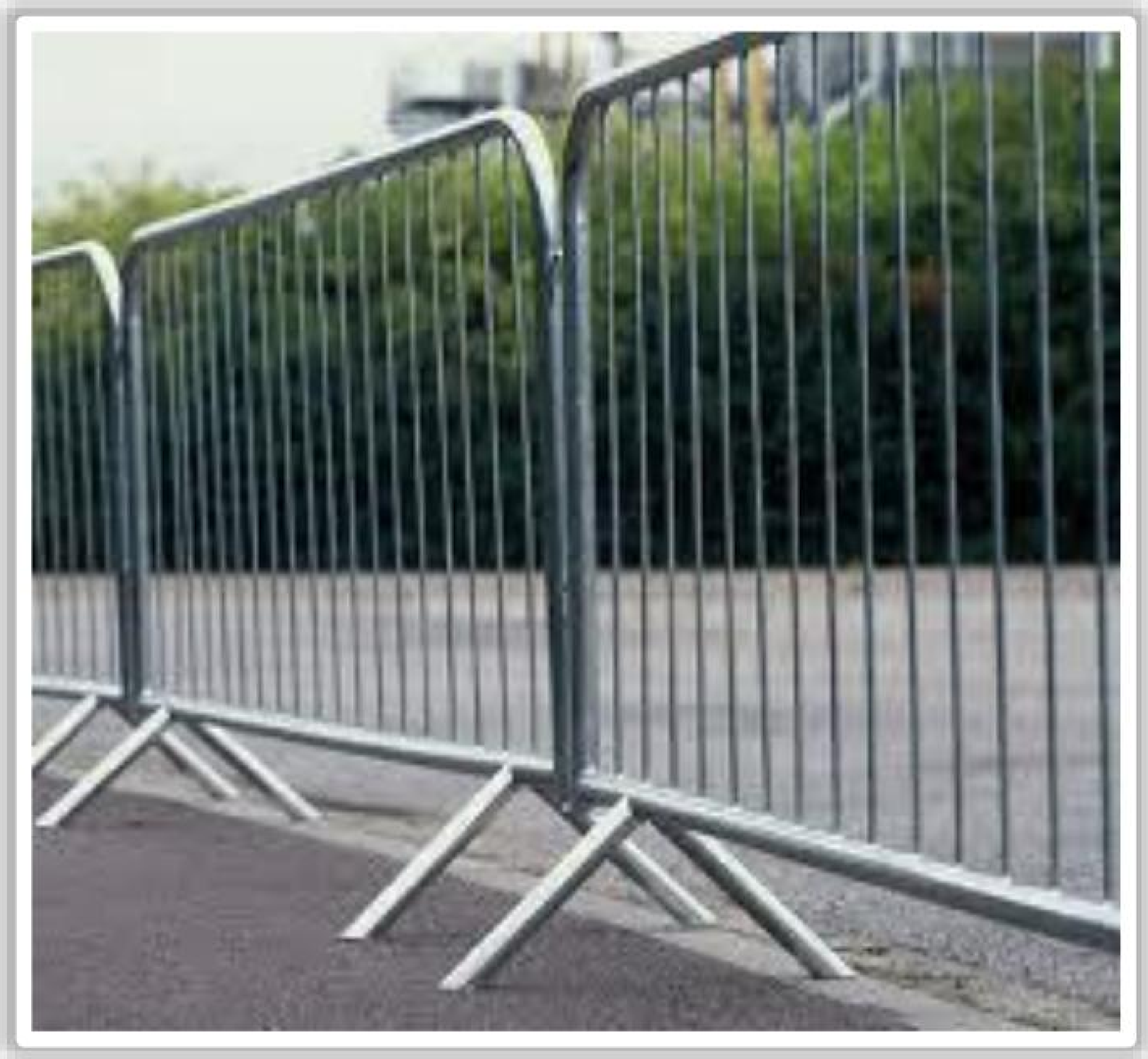


Figure 6.2: Metal Rails

- **Bollards:** A bollard may be defined as a short vertical post that controls and restricts motor vehicles in parking areas, offices, etc. This facilitates the easy movement of people. Bollards are mainly used in building entrances, pedestrian areas, and areas that require safety and security. It is effective in controlling pedestrian and vehicle traffic in sensitive areas.

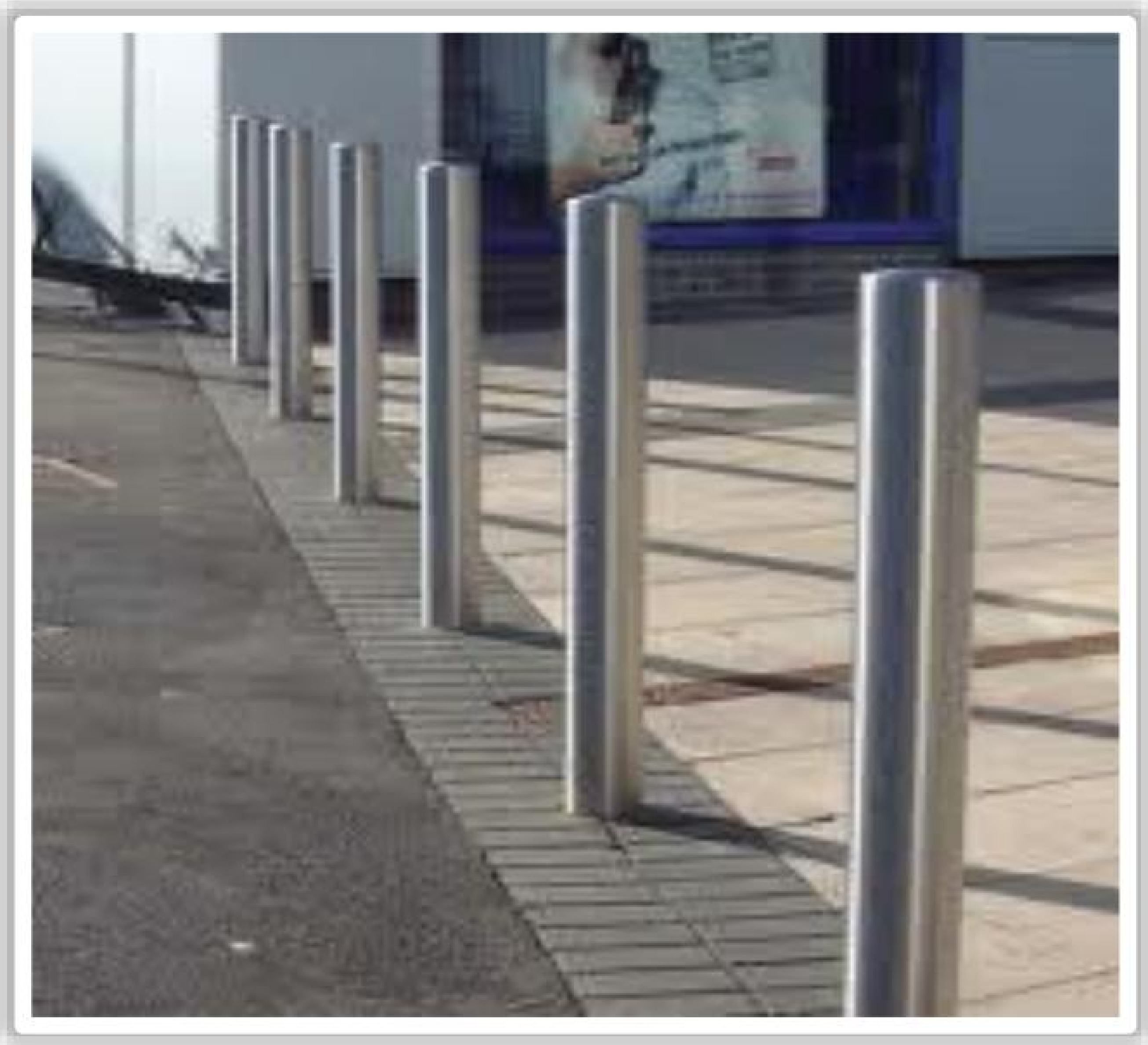


Figure 6.3: Bollards

- **Turnstiles:** This type of physical barrier allows entry to only one person at a time. Entry can be achieved only by the insertion of a coin, ticket, or pass. It allows security personnel to closely watch the people entering the organization and stop any suspicious persons at the gate. However, the use of a turnstile can hamper the fast evacuation of occupants in case of a fire emergency.

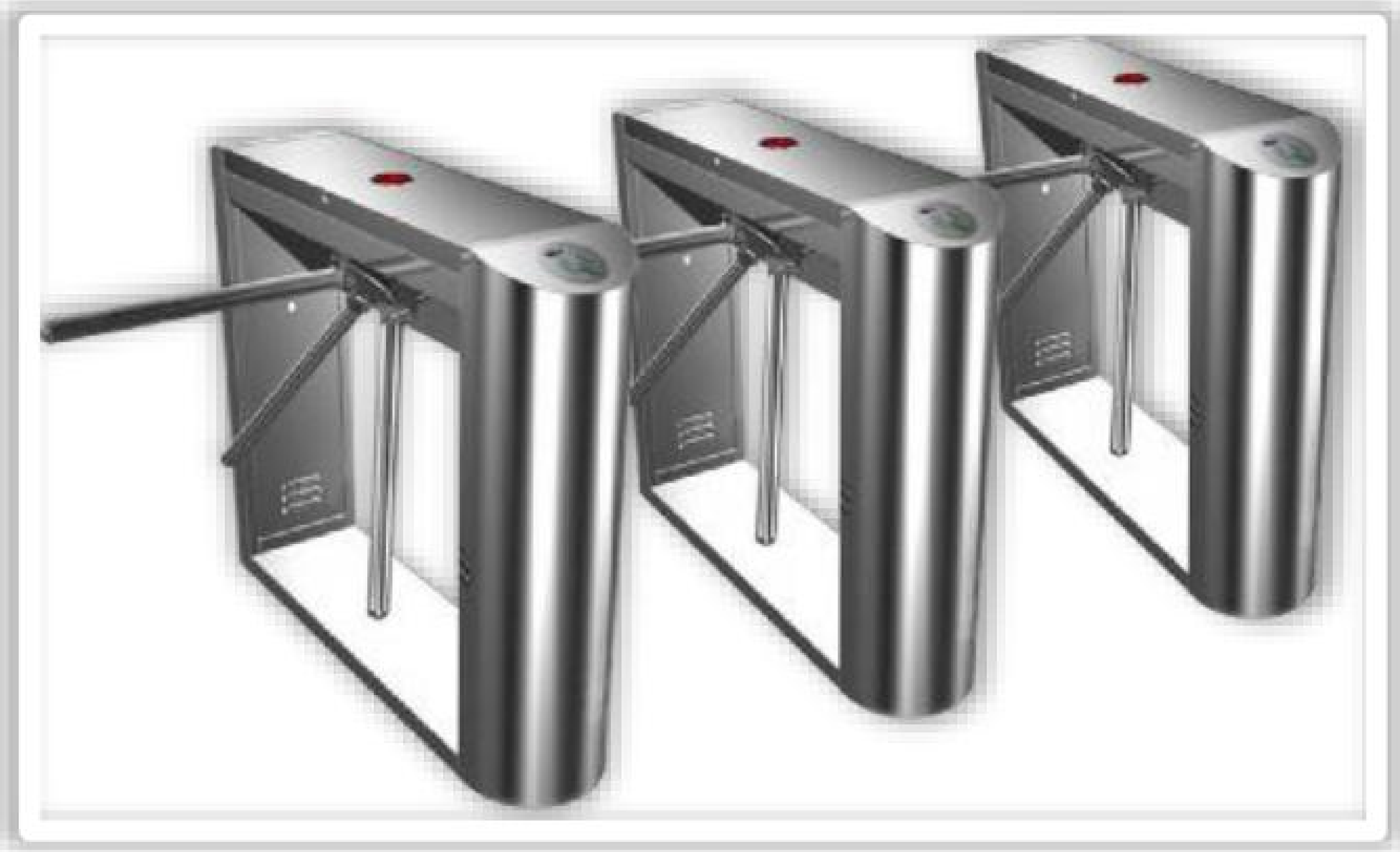
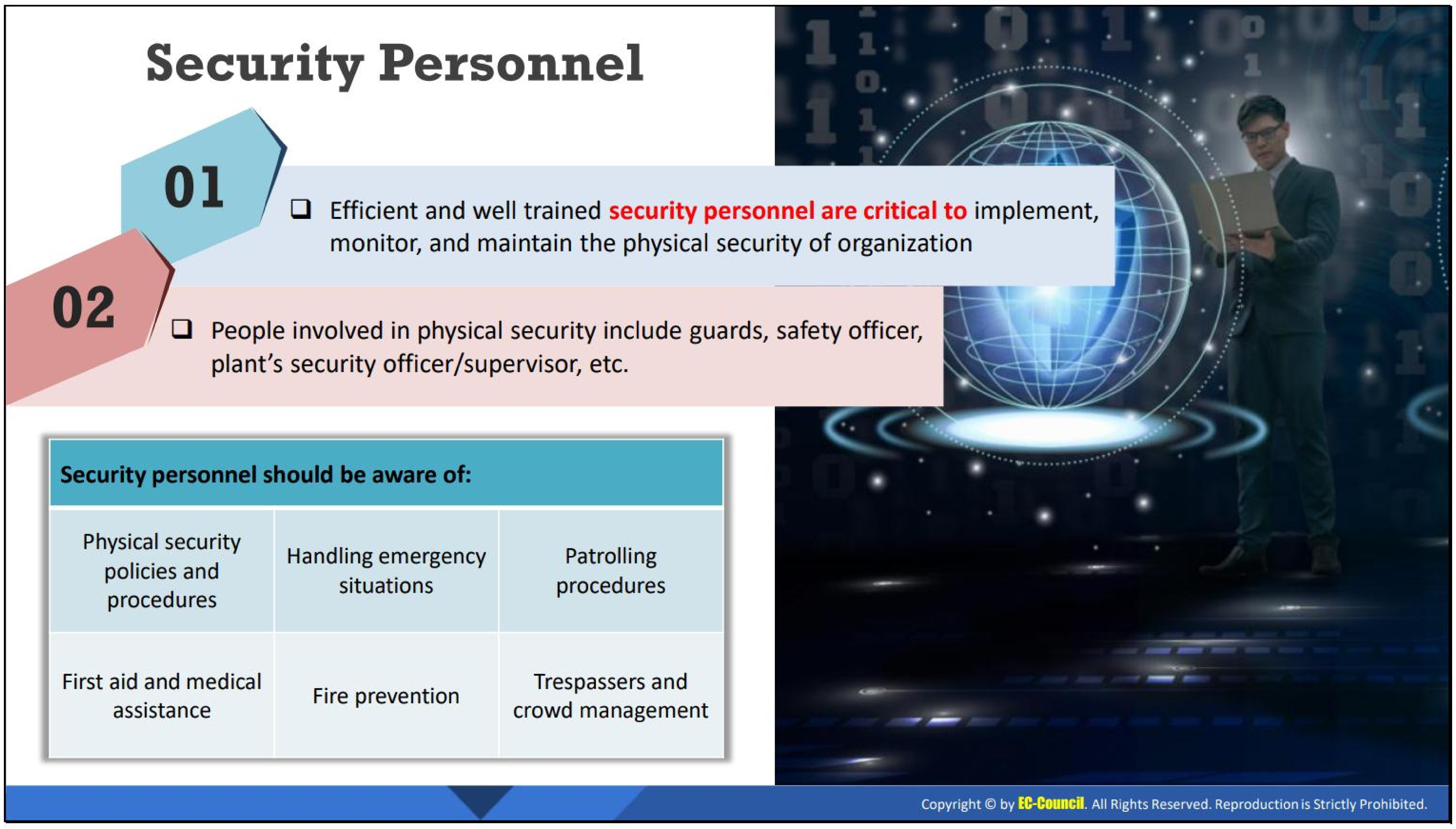


Figure 6.4: Turnstiles

- **Other Barriers:** These include doors, windows, grills, glass, and curtains installed to limit access to certain areas.
  - **Doors:** Doors can be used as a good structure to control the access of users in a restricted area. Door security may be increased with the installation of CCTV cameras, proper lighting systems, locking technology, etc.
  - **Windows**: An intruder can use windows to gain unauthorized access to restricted areas. Proper security measures should be considered while installing windows. Some of these considerations include the following:
    - Method of opening the window
    - Assembling and construction of the window
    - Technique used in locking the window
    - Hinges used for the window
  - **Grills:** Grills should be used with doors and windows to strengthen security. Grills may be used for internal as well as external security.
  - **Glass:** Sliding glass doors and sliding glass windows also strengthen physical security.

Figure 6.5: Other Barriers

- The following are security considerations for physical barriers:
  - Use a combination of barriers to deter unauthorized entry.
  - Use bullet-resistant windows and glass.
  - Install doors both at the main entrance and inside the building.
  - Lock doors and windows.
  - Use electric security fences to detect the climbing and cutting of wires.
  - Use alarms to alert security personnel of any intrusions through fences.



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

Security Personnel

Security personnel/guards are hired to implement, monitor, and maintain the physical security of an organization. They are responsible for developing, evaluating, and implementing security functions such as the installation of security systems to protect sensitive information from loss, theft, sabotage, misuse, and compromise. Hiring skilled and trained security personnel can be an effective security measure for any organization. They play a crucial role in physical security. However, organizations generally do not consider this a core competency to invest in as part of their strategic plan.

Organizations should hire security personnel by themselves and provide adequate training on physical security. Alternatively, they can contact dedicated physical security service firms to handle physical security for them. There are organizations dedicated to training security officers, providing standardized procedures, and managing security on a 24 × 7 × 365 schedule by sharing guards across different organizations.

The following are the people involved in physical security.

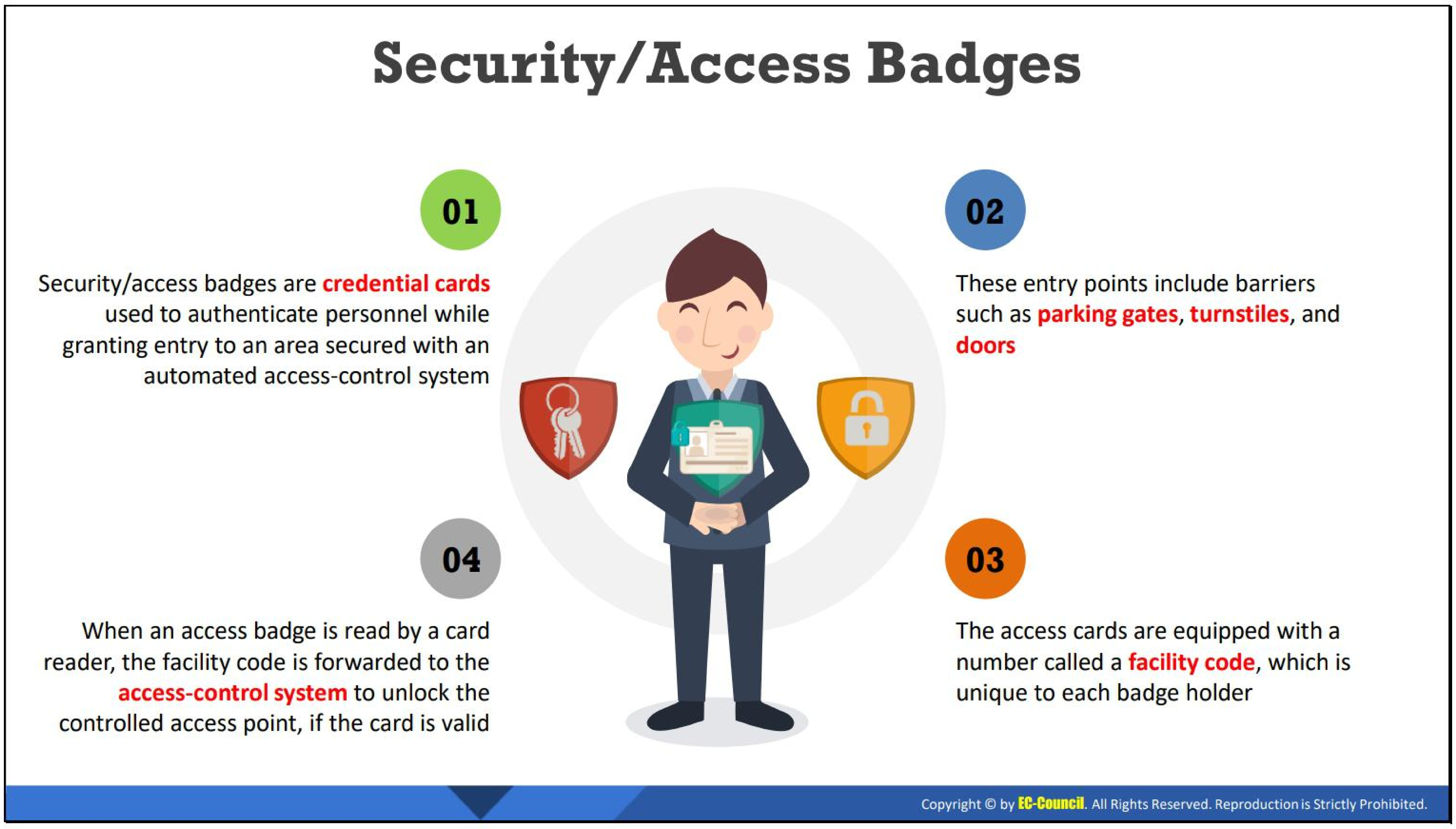
- **Guards**: Their responsibilities include screening visitors and employees at the main gates or entrance; documenting names and other details about visitors; conducting regular patrols on the premises; inspecting packages, luggage, and vehicles; managing vehicle traffic; and guiding visitors to the reception area after noting their details. Guards should maintain visitor logs and record entry and exit information. Guards generally handle the use of CCTV cameras as a deterrent as well as a mechanism to detect and possibly prevent an intrusion.

- **The plant's security officers/supervisors**: Their responsibilities include training and monitoring the activities of the guards; assisting guards during crisis situations; handling crowds; and maintaining the keys, locks, lights, greenery, etc. of the facility.
- **Safety officers**: Their responsibilities include implementing and managing safety-related equipment installed around the facility and ensuring the proper functioning of this equipment.
- **Chief information security officer (CISO)**: In the past, it was common for the CISO of an organization to be an extremely technically competent individual who has held various positions with an enterprise security function or even has a networking or systems background. Today, a CISO is required to be much more than technically competent. The modern CISO must have a diversified set of skills to successfully dispatch their duties and establish the appropriate level of security and security investment for their organization.

Continuous training for security personnel can provide great benefits and an effective team for the organization. Regardless of the position, security-related personnel should be selected based on the experience and qualification required for the job. Executives should thoroughly evaluate the personnel's past experiences and, based on this information, provide adequate training to fill the gap between the ability and skills necessary for the job.

An organization should train newly hired security personnel in the following areas:

- Organizational culture, ethics, and professionalism
- Security policies and procedures
- Policy enforcement
- Trespassers and crowd management
- Handling emergency situations
- Human and public relations
- Patrolling procedures
- Managing workplace violence
- First aid and medical assistance
- Fire prevention
- Vehicle traffic management
- Handling foreign guests, invitees, etc.
- Report writing



Security/Access Badges

01

Security/access badges are **credential cards** used to authenticate personnel while granting entry to an area secured with an automated access-control system

02

These entry points include barriers such as **parking gates**, **turnstiles**, and **doors**

03

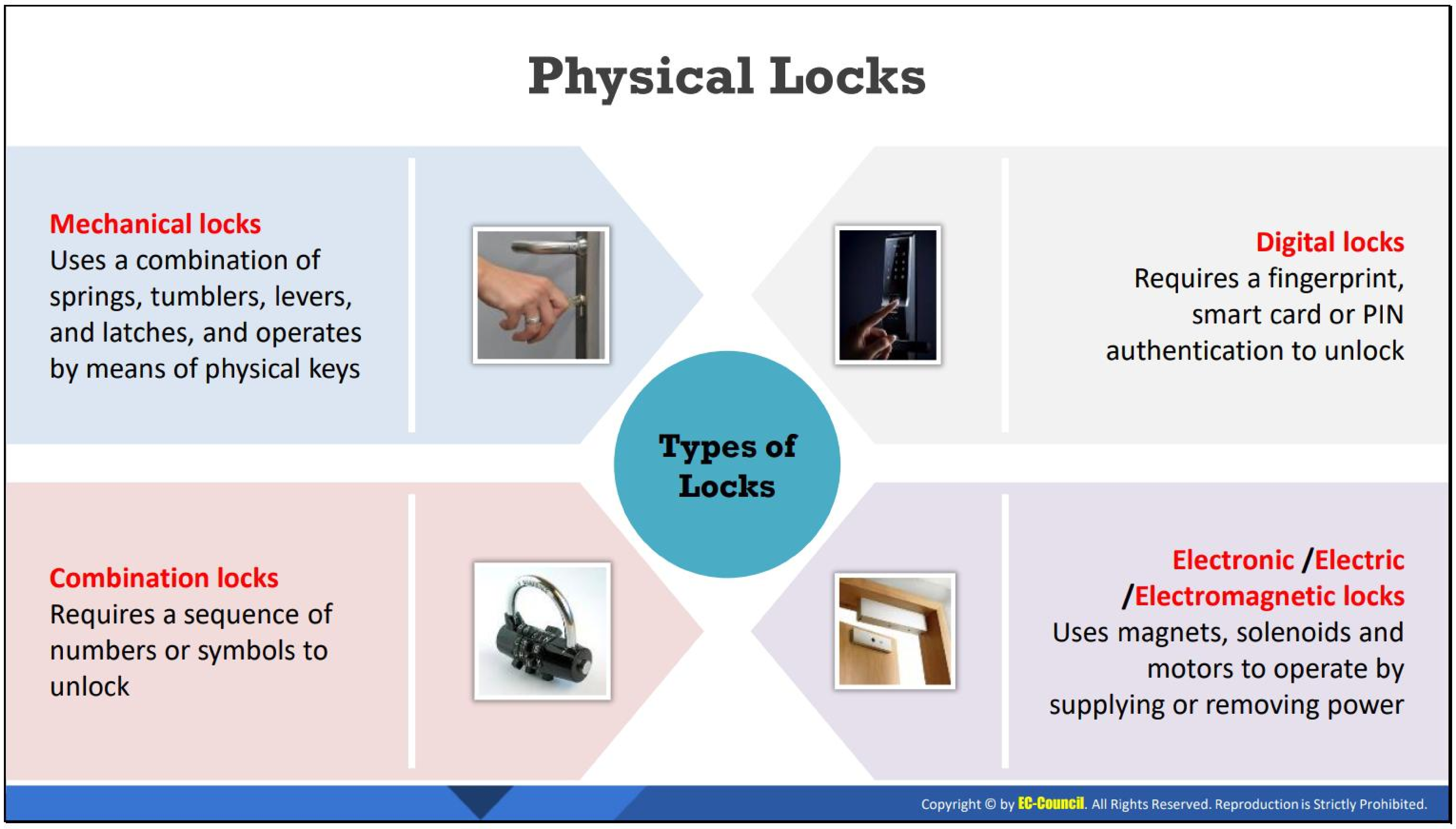
The access cards are equipped with a number called a **facility code**, which is unique to each badge holder

04

When an access badge is read by a card reader, the facility code is forwarded to the **access-control system** to unlock the controlled access point, if the card is valid

Security/Access Badges

Security/access badges are credential cards used to authenticate personnel while gaining entry to an area secured with an automated access-control system. These entry points include barriers such as parking gates, turnstiles, and doors. The cards are assigned a number called the facility code, which is unique to each badge holder. These numbers are identified using various technologies such as smart cards, barcodes, biometrics, and magnetic stripe devices. When an access badge is read by a card reader, the facility code is forwarded to the access-control system (computer system) to unlock the controlled access point, if the card is valid. This system also records the details of access such as card swipe time and date for future reference.



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

Physical Locks

Various types of locking systems are available to improve the restriction of unauthorized physical access. The organization should select an appropriate locking system according to their security requirements.

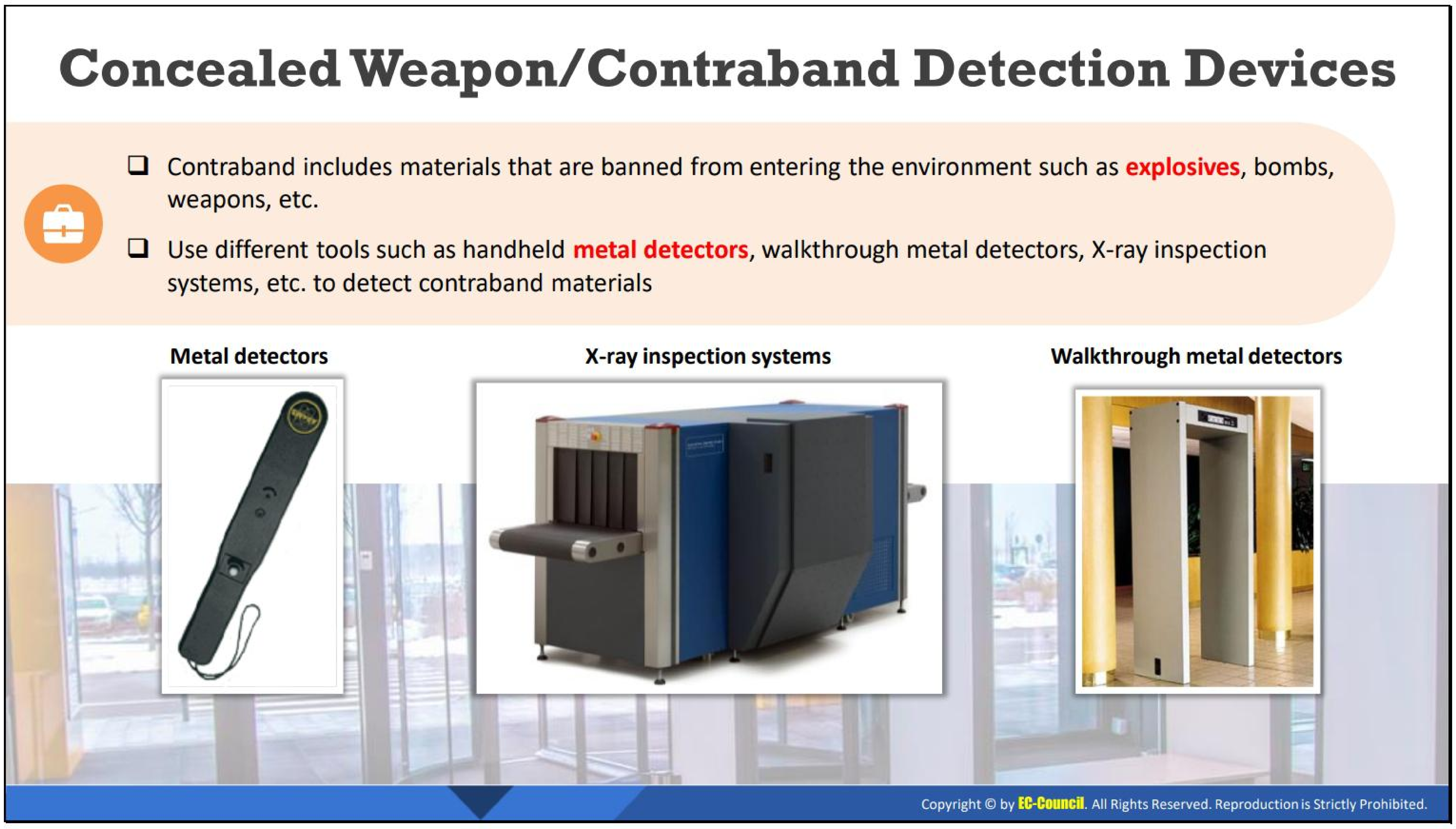
The following are the different types of locks.

- **Mechanical locks**: These provide an easy method to restrict unauthorized access in an organization. Mechanical locks come with or without keys. There are two types of mechanical locks.
  - **Warded lock**: A warded lock contains a spring-loaded bolt attached to a notch. A key inserted into the notch moves the bolt backward and forward. Only the correct key can be inserted into the notch, which blocks incorrect keys.
  - **Tumbler lock**: A tumbler lock consists of metal pieces inside a slot in the bolt. This prevents the bolt from moving. A correct key contains grooves that allow the bolt to move by raising the metal pieces above the bolt. Tumbler locks are further classified into pin tumbler, disk tumbler, and lever tumbler locks.
- **Digital locks:** Digital locks require fingerprints, smart cards, or keypad PINs to unlock. It is easy to handle and does not require keys, eliminating the chance of forgetting or losing keys. It provides automatic locking for doors. The user only has to use their fingerprint impression, swipe their smart card, or enter the PIN to unlock it.
- **Electric/electromagnetic locks**: Electric locks or electronic locking systems operate on electric current. Locking and unlocking are achieved by supplying and eliminating power.

The locks are activated or deactivated mainly using magnets or motors. They do not require keys to be maintained for the locking system.

An electromagnetic lock or magnetic lock consists mainly of an electromagnet and an armature plate. The locking device can be of two types: fail safe and fail secure. Fail secure locks remain locked even during power loss, whereas fail safe locks remain inactive when de-energized. The electromagnetic part may be placed on a door frame, and the armature plate may be placed on the door. The magnetic flux created by the electromagnet creates an attractive force towards the armature plate, which initiates the door closing process.

- **Combination locks:** These require the user to provide a combination of numbers and letters to unlock. Users may enter the combination sequence either through a keypad or by using a rotating dial that intermingles with several other rotating discs. Combination locks do not use keys for functioning.



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

Concealed Weapon/Contraband Detection Devices

Contraband detection devices act as an important physical security control as they restrict undesirable activities and/or a person carrying contraband from entering the premises. Contraband refers to illegal materials such as explosives, bombs, and weapons, which should be banned from the premises. An attempt to enter the premises with contraband can be considered an act of terrorism. Contraband detection devices are able to detect such substances, even when they are covered by other objects.

Different types of devices are used to detect contraband materials; examples are handheld metal detectors, walkthrough metal detectors, and X-ray inspection systems.

- Walkthrough metal detectors are mainly used in airport terminals, schools, sports stadiums, etc. They help check people who have admission to certain areas. Furthermore, walkthrough detectors should be maintained and properly monitored. They should be deployed at each entry point of the organization.

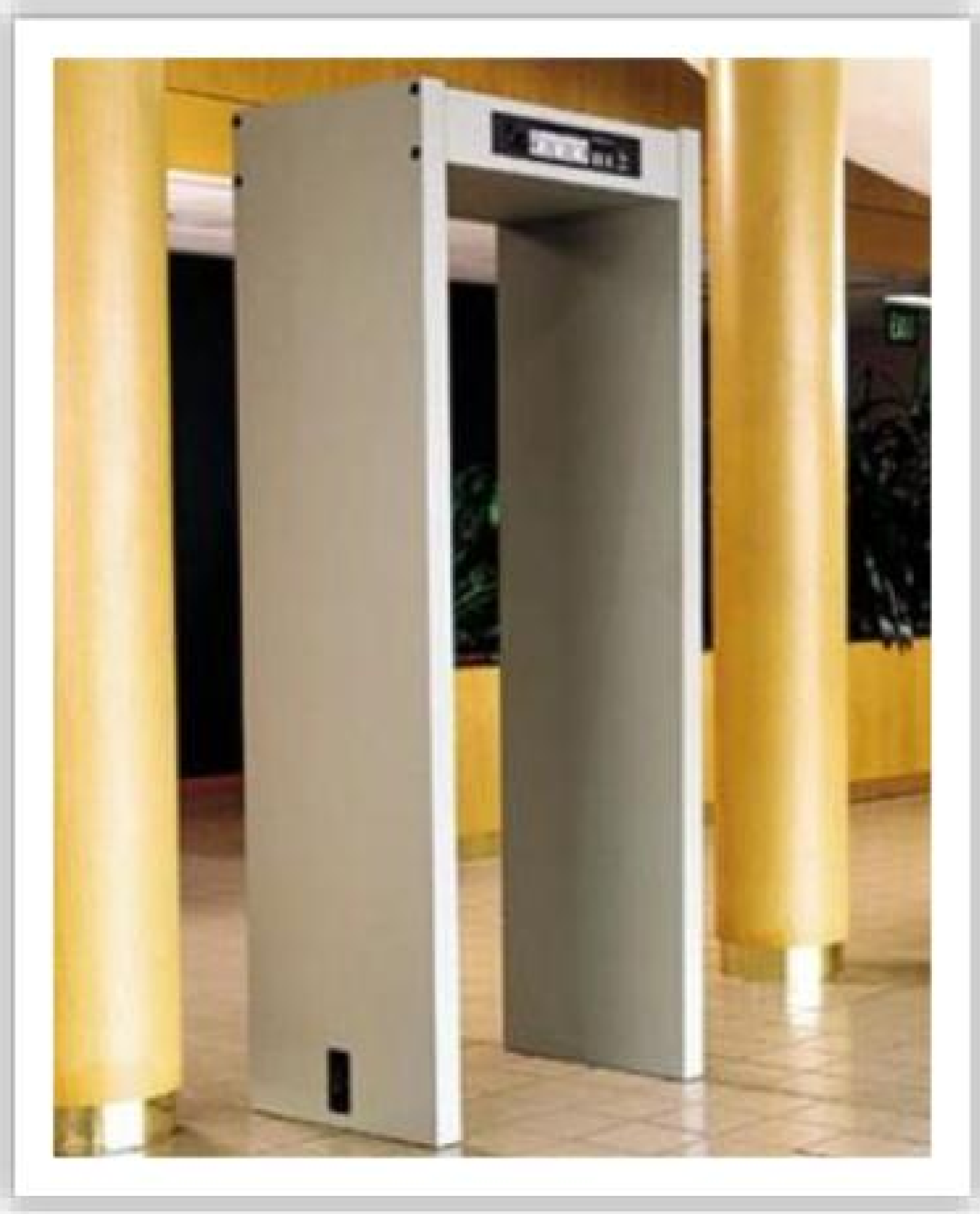


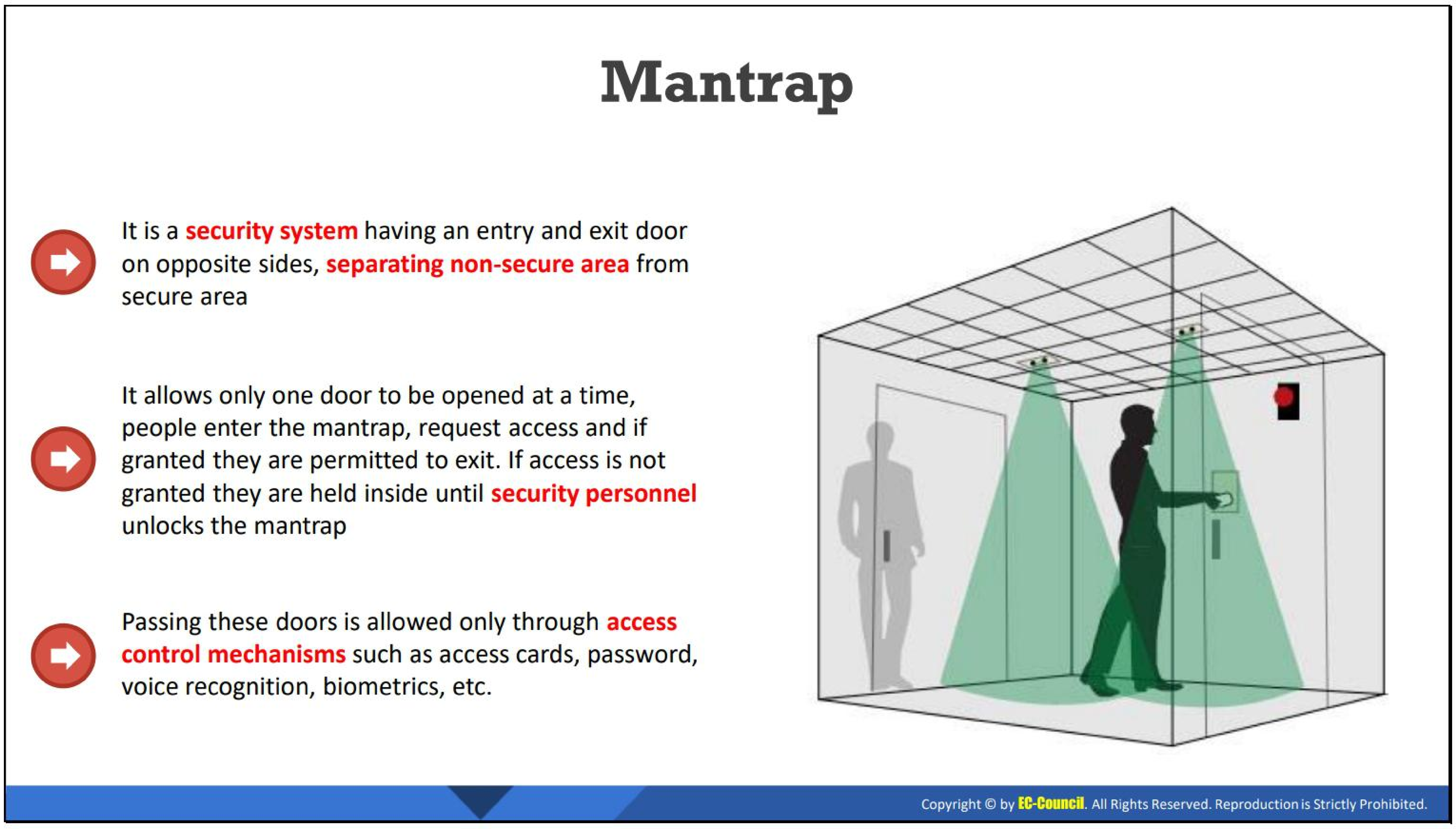
Figure 6.6: Walkthrough metal detectors

- Handheld metal detectors allow people to be screened more closely and detect suspicious objects. Handheld detectors are used in most places where walkthrough detectors are used.

Figure 6.7: Metal Detectors

- X-ray inspection systems are easy to handle and use. They use X-rays instead of visible light to screen objects.

Figure 6.8: X-ray inspection systems



Mantrap

- It is a **security system** having an entry and exit door on opposite sides, **separating non-secure area** from secure area
- It allows only one door to be opened at a time, people enter the mantrap, request access and if granted they are permitted to exit. If access is not granted they are held inside until **security personnel** unlocks the mantrap
- Passing these doors is allowed only through **access control mechanisms** such as access cards, password, voice recognition, biometrics, etc.

Mantrap

A mantrap is another type of physical access security control that is used for catching trespassers. It is most widely used to separate non-secure areas from secure areas and prevents unauthorized access. It is a mechanical locking mechanism consisting of a small space with two sets of interlocking doors. The first set of doors must close before the second set opens. User authentication at mantrap doors is performed using smart cards, keypad PINs, or biometric verification. It operates automatically, is useful in authorizing visitors, reduces the manpower required for security systems, and guarantees the safety of the organization.

Working of Mantraps

- **Step 1:** The mantrap authenticates the person attempting access.
- **Step 2:** The first door opens after authentication. The person walks in.
- **Step 3:** The first door closes soon after the person enters the room. Now, the person is locked inside the room. This signals the unlocking of the second door.
- **Step 4:** The second door opens with the person walking out of the room. The first door is automatically locked soon after the second door opens.
- **Step 5:** The second door enters the locked state soon after the person walks out.

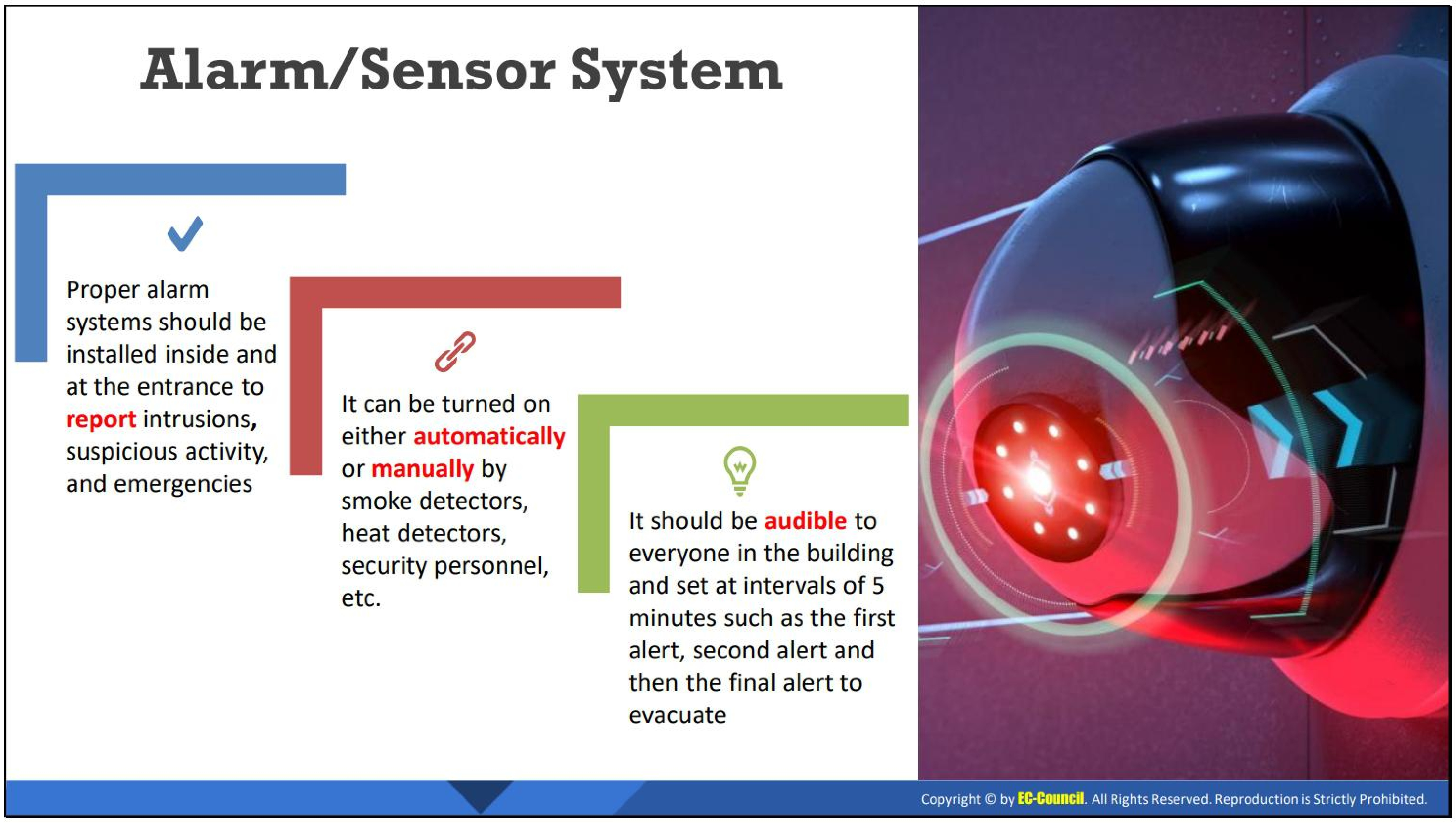
Warning Signs

- 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

RESTRICTED AREA
AUTHORIZED PERSONNEL ONLY

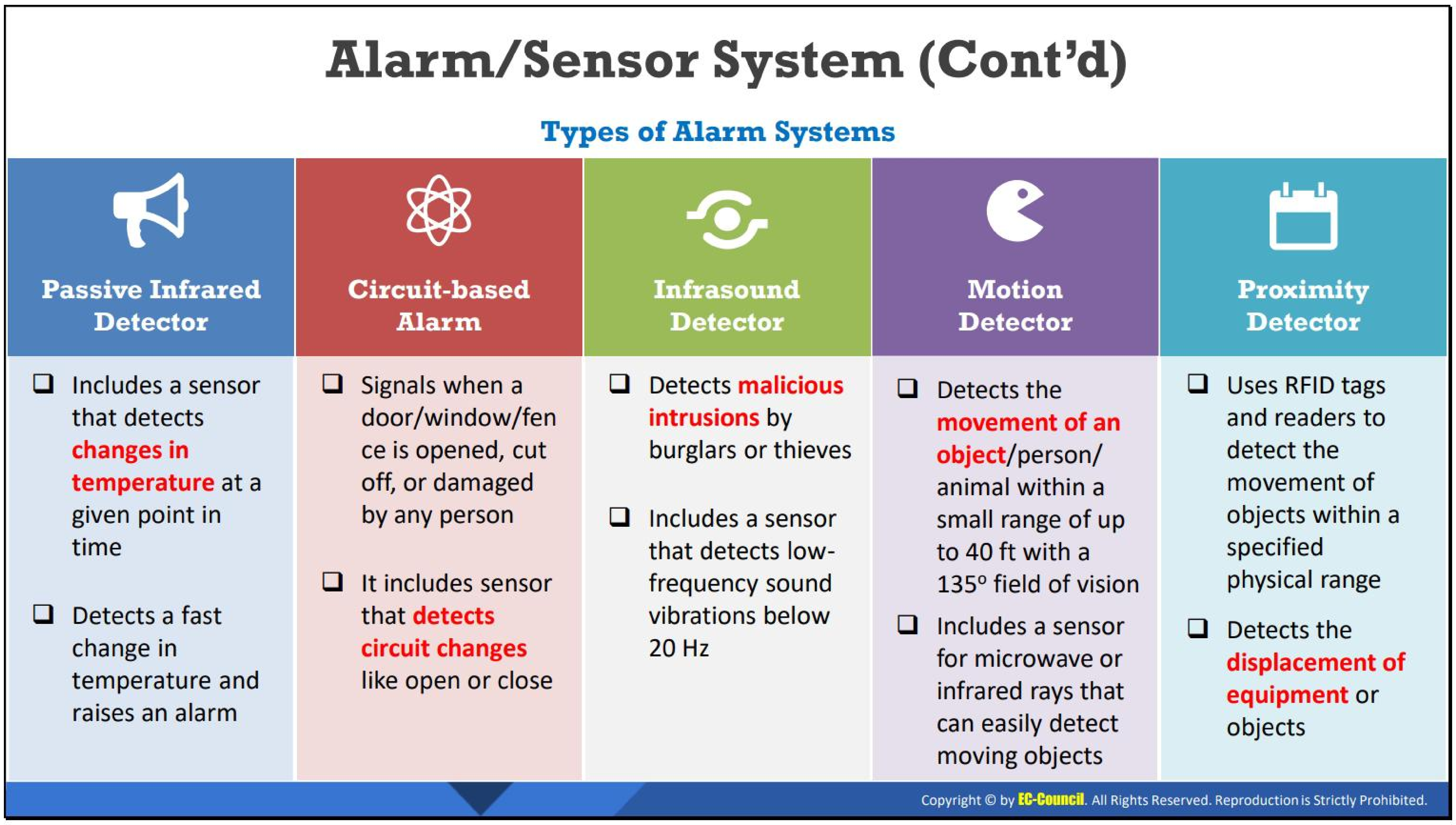
Warning Signs

Warning signs are generally used to restrict unauthorized access in an organization. Warning signs are placed at entrance points, boundaries of the locality, and sensitive areas. They should be visible to users such that people understand prohibited areas and avoid entering them. Warning signs also help organizations prevent a large number of people from entering sensitive areas. They are generally placed in all sensitive areas that have a threat of damage to assets or life or disclosure of information. For example, warning signs are typically placed on electrical fences because unknowingly touching the electric fence may pose a threat to life. Examples of warning signs are “RESTRICTED AREA,” “WARNING,” “CAUTION,” “DANGER,” and “BEWARE.”



Alarm/Sensor 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



Alarm/Sensor System (Cont'd)

Types of Alarm Systems

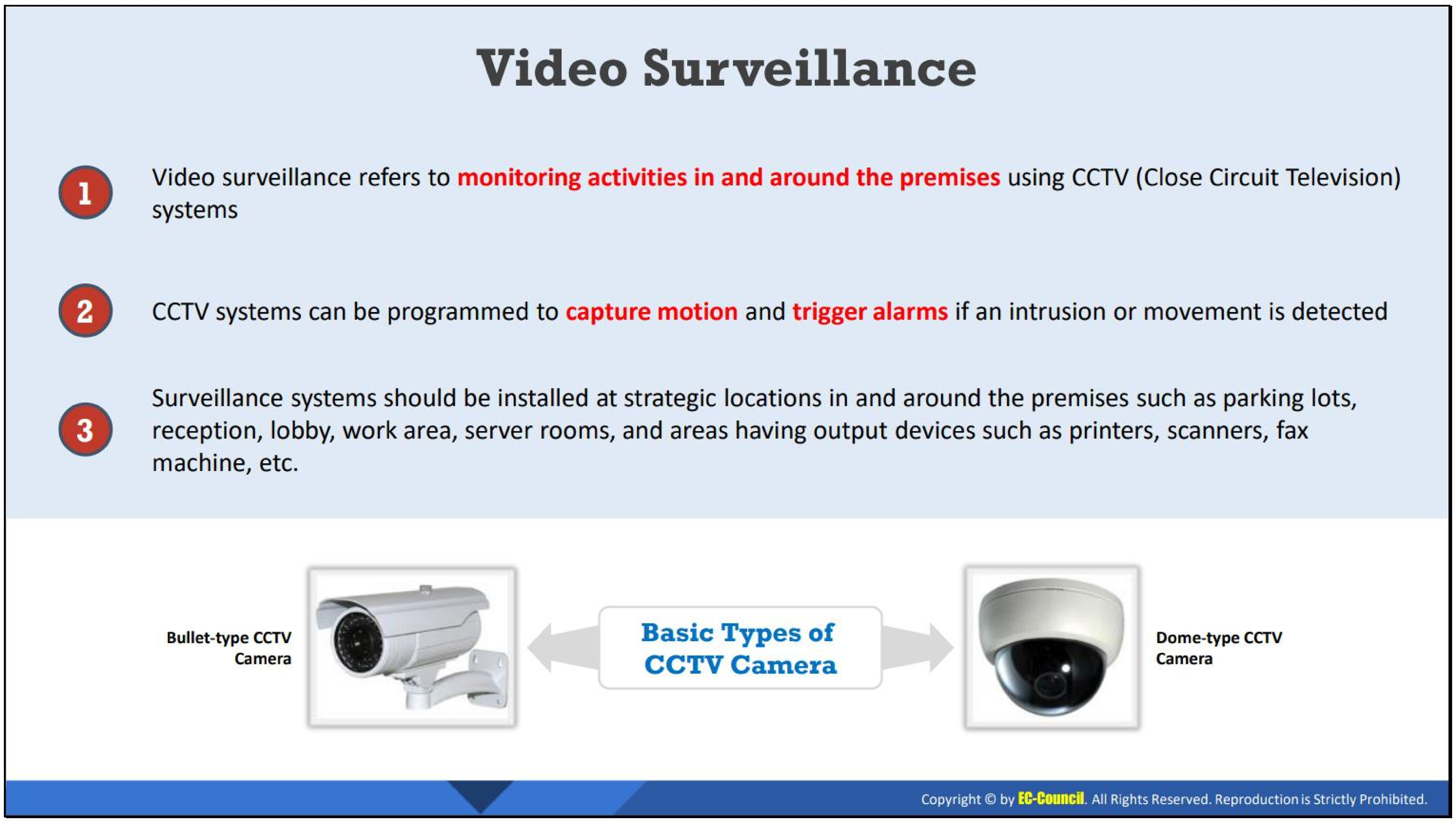
Passive Infrared Detector	Circuit-based Alarm	Infrasound Detector	Motion Detector	Proximity Detector
❑ Includes a sensor that detects **changes in temperature** at a given point in time ❑ Detects a fast change in temperature and raises an alarm	❑ Signals when a door/window/fence is opened, cut off, or damaged by any person ❑ It includes sensor that **detects circuit changes** like open or close	❑ Detects **malicious intrusions** by burglars or thieves ❑ Includes a sensor that detects low-frequency sound vibrations below 20 Hz	❑ Detects the **movement of an object**/person/ animal within a small range of up to 40 ft with a 135° field of vision ❑ Includes a sensor for microwave or infrared rays that can easily detect moving objects	❑ Uses RFID tags and readers to detect the movement of objects within a specified physical range ❑ Detects the **displacement of equipment** or objects

Alarm/Sensor System

Alarms are used to draw attention in case of a breach or an attempted breach. Alarm sounds can be of different types based on the facility; examples include sirens, flash lighting with a sound, emails, and/or voice alerts. The organization should divide large facilities such as buildings, floors, sections, and offices into small security zones; depending on their significance, the appropriate alarm system should be installed. Security zones that store high-priority data are given multilevel security systems such as access restriction with access control devices, biometrics, surveillance, locks, and alarms to draw attention in an event of intrusion. Alarms can be turned on either automatically or manually by smoke detectors, heat detectors, security personnel, etc. They should be audible to everyone in the building and set with three alerts to evacuate in intervals of 5 min. Organizations should have a proper power backup for alarm systems so that they work in emergencies and during power shutdowns. All wiring and components of an alarm should be protected from tampering, and the alarm box should be concealed with proper locks and limited access. Proper management and regular assessments of the alarm system should be performed with emergency drills.

An alarm system contains at least one sensor that detects and alerts of an intrusion. The alarms used for security purposes include the following components: an alarm control panel (ACP), sensors, an alerting system, a keypad, and wired or wireless interconnection with other components. The following are different types of alarms used for physical security.

- **Passive infrared detector/temperature detector:** This type of alarm includes a sensor that detects changes in temperature at a given point of time. For example, if a person comes into the vicinity of the sensor, the temperature at that position changes from room temperature to the body temperature of that person. The sensor detects this fast change in temperature and raises an alarm.
- **Circuit-based alarm:** This type of alarm is used to signal when a door/window/fence is opened, cut off, or damaged by any person. It includes a sensor that detects circuit changes such as open or close.
- **Infrasound detector:** This type of alarm is used to identify malicious intrusions by burglars or thieves. It includes a sensor that detects low-frequency sound vibrations below 20 Hz. When an intruder attempts to unlock a door or window using tools, the sensor identifies the low-frequency vibrations and raises an alarm.
- **Motion detector:** This type of alarm is used to identify the movement of any object/person/animal within a small area of up to 40 ft with a 135° field of vision. It includes a sensor for microwave or infrared rays that can easily detect moving objects.
- **Proximity detector:** This type of alarm is built using RFID tags and readers. They are used to detect the movement of objects within a specified physical range. These alarms are used to identify the displacement of equipment or objects.



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.

Bullet-type CCTV Camera

Basic Types of CCTV Camera

Dome-type CCTV Camera

Video Surveillance

Video surveillance refers to monitoring activities in and around the premises using closed-circuit television (CCTV) systems. Video surveillance is considered an important component of physical security. These systems protect an organization’s assets and buildings from intruders, theft, etc. A CCTV system is used as part of the organization’s security system. It covers a large area and is often placed near gates, the reception, hallways, and at the workplace. It captures footage of illicit activities inside the premises and helps monitor activities inside, outside, and at the entrance. CCTV systems are even programmed to capture motion and initiate an alarm whenever a motion or an object is detected. They help identify activities that need attention, collect images as evidence, and aid in an alarm system. The devices used for video surveillance should be automatic, powerful, and capable of pan/tilt/zoom to capture the action and store them for later review.

Many aspects need to be considered for the installation, management, and maintenance of a video surveillance system in an organization; these include the camera, lens, resolution, recording time, recording equipment, cabling, monitoring system, storage devices, and centralized control system/equipment. Recording activities through CCTV and storing this footage for reference can also help facilities provide evidence in a court of law. It is also important to decide the type of lens, resolution, and area the camera should cover, and the time and date of the footage should be recorded. Another important aspect is the storage of video recordings and the storage duration. The organization must decide what will happen to old video recordings and how they will be disposed of.

The following are a few considerations for video surveillance systems:

- Install surveillance systems at the parking lot, reception, lobby, and workstation.

- Place output devices such as printers, scanners, and fax machine in public view and under surveillance.
- Integrate surveillance with an alarm system.
- Establish a policy for the duration for which recorded videos should be kept and later disposed.
- Store all devices in secure locations with limited access.
- Use proper disposal procedures such as content deletion, overwriting, and physical destruction.

The following are the different types of CCTV cameras available commercially.

- **Dome CCTV:** Mainly used for indoor security and surveillance purposes, dome CCTV cameras are built as dome-shaped devices to prevent any damage to the camera or destruction. It is impossible to locate the direction to which such cameras are moving; thus, they allow for observing areas at a wide angle and cover larger areas. Speed dome CCTV camera units provide a facility with pan/tilt/zoom and spin features, allowing the operator to move the camera according to their need.

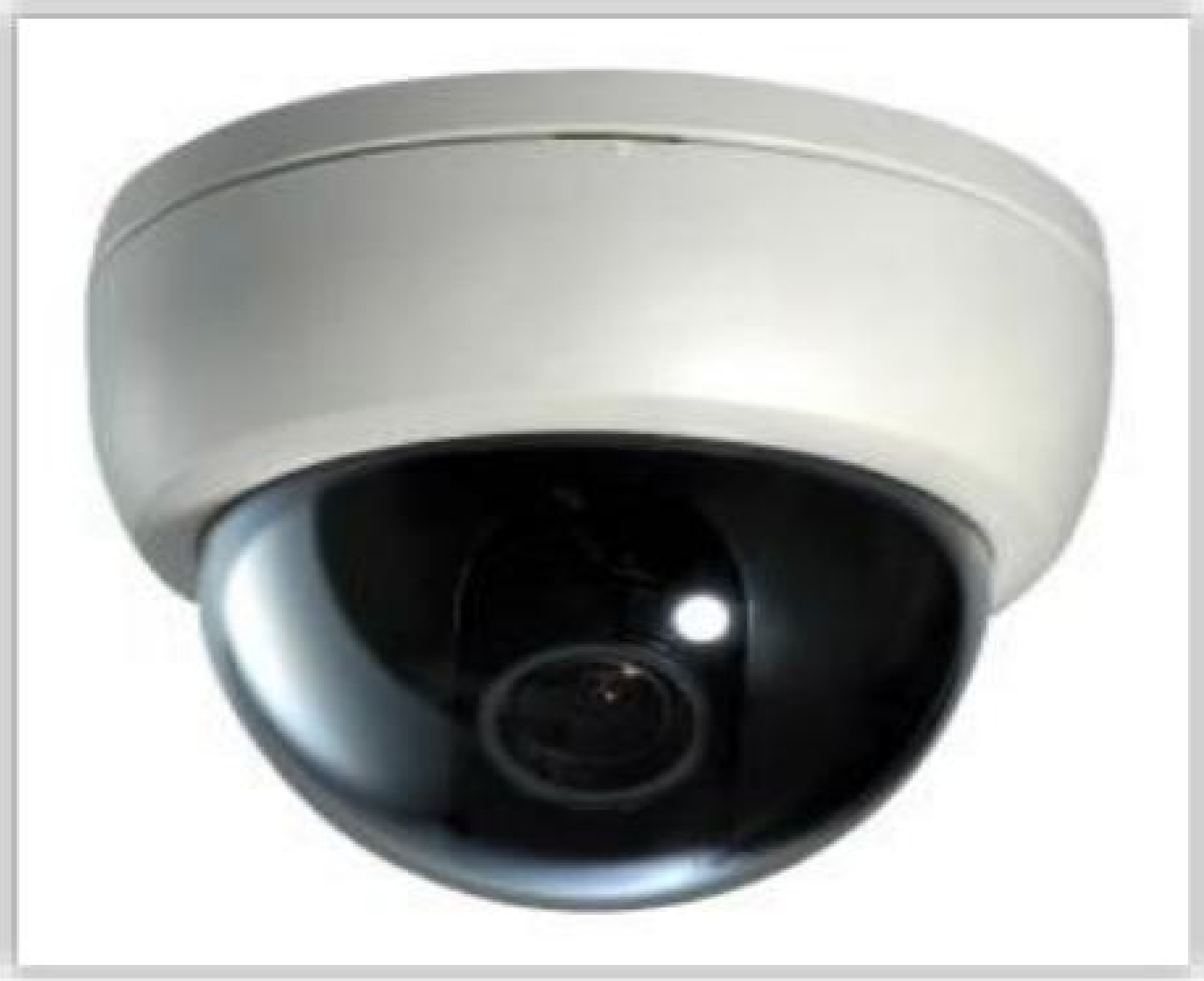


Figure 6.9: Dome CCTV

- **Bullet CCTV:** Bullet CCTV cameras are used for indoor and outdoor surveillance. They are generally placed in protective covers that keep away dust, rain, or any other disturbance. A bullet CCTV camera usually has a long, cylindrical, and tapered shape that facilitates long-distance surveillance.

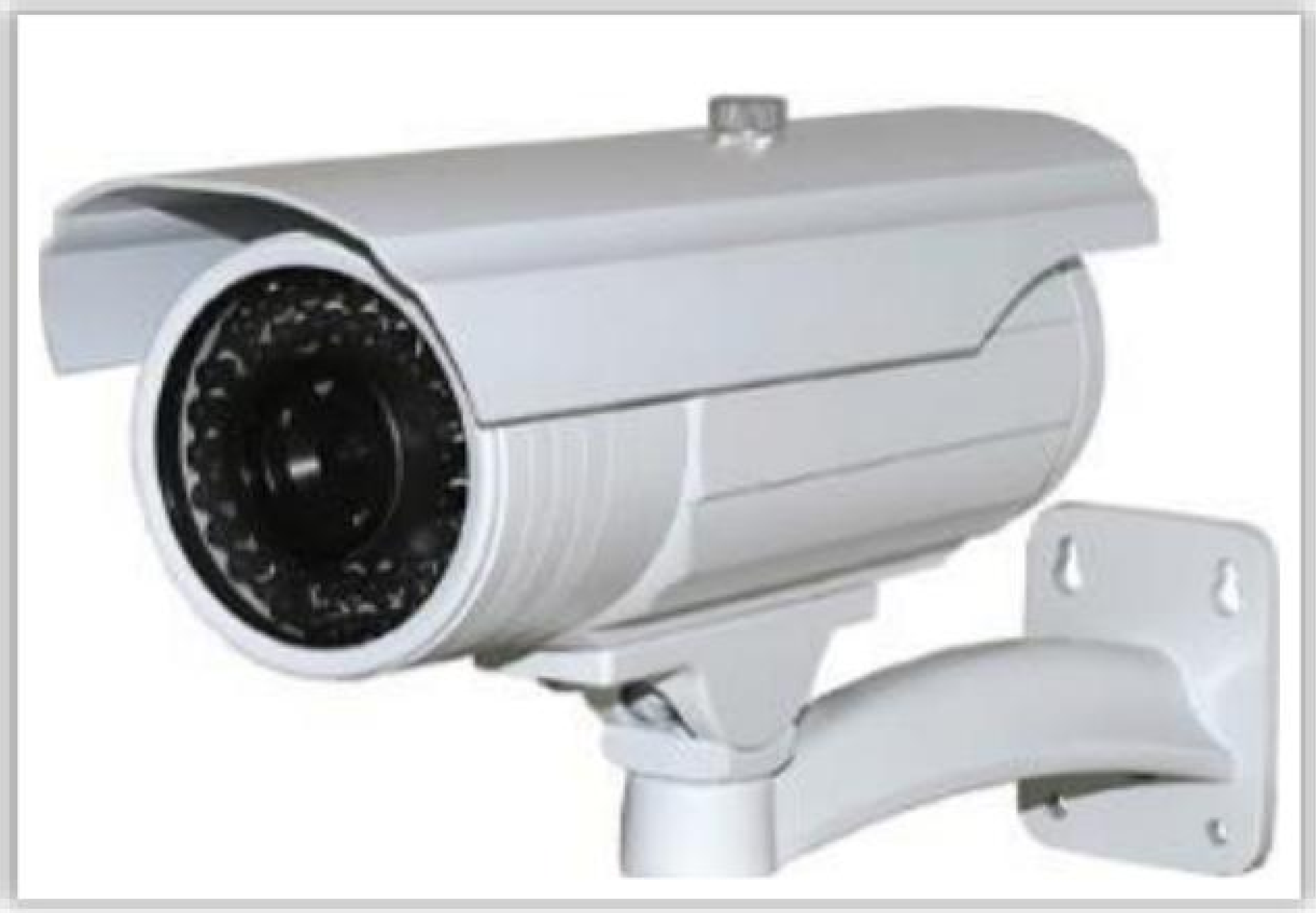


Figure 6.10: Bullet CCTV

- **C-mount CCTV:** A C-mount CCTV camera consists of detachable lenses, which provide surveillance with a coverage distance of more than 40 ft. Other CCTV camera lenses provide a coverage distance of only 35–40 ft. The C-mount allows different lenses to be used according to the distance to be covered.

Figure 6.11: C-Mount CCTV Camera

- **Day/night CCTV:** Day/night CCTV cameras are commonly used for outdoor surveillance. They can capture images even in low light and darkness. These types of cameras do not require infrared illuminators to capture images. They can capture clear images under glare, direct sunlight, reflections, etc.

Figure 6.12: Day/Night CCTV Camera

- **Infrared night-vision CCTV:** Infrared night-vision CCTV cameras are commonly used for outdoor surveillance and can capture images in complete darkness. Infrared LEDs are used for areas having poor lighting.

Figure 6.13: Infrared Night Vision CCTV Camera

- **Network/IP CCTV:** Network/IP CCTV cameras are available as both wired and wireless models. They allow sending images over the Internet. A wireless IP camera is easier to install than a wired camera because the former does not require any cabling.

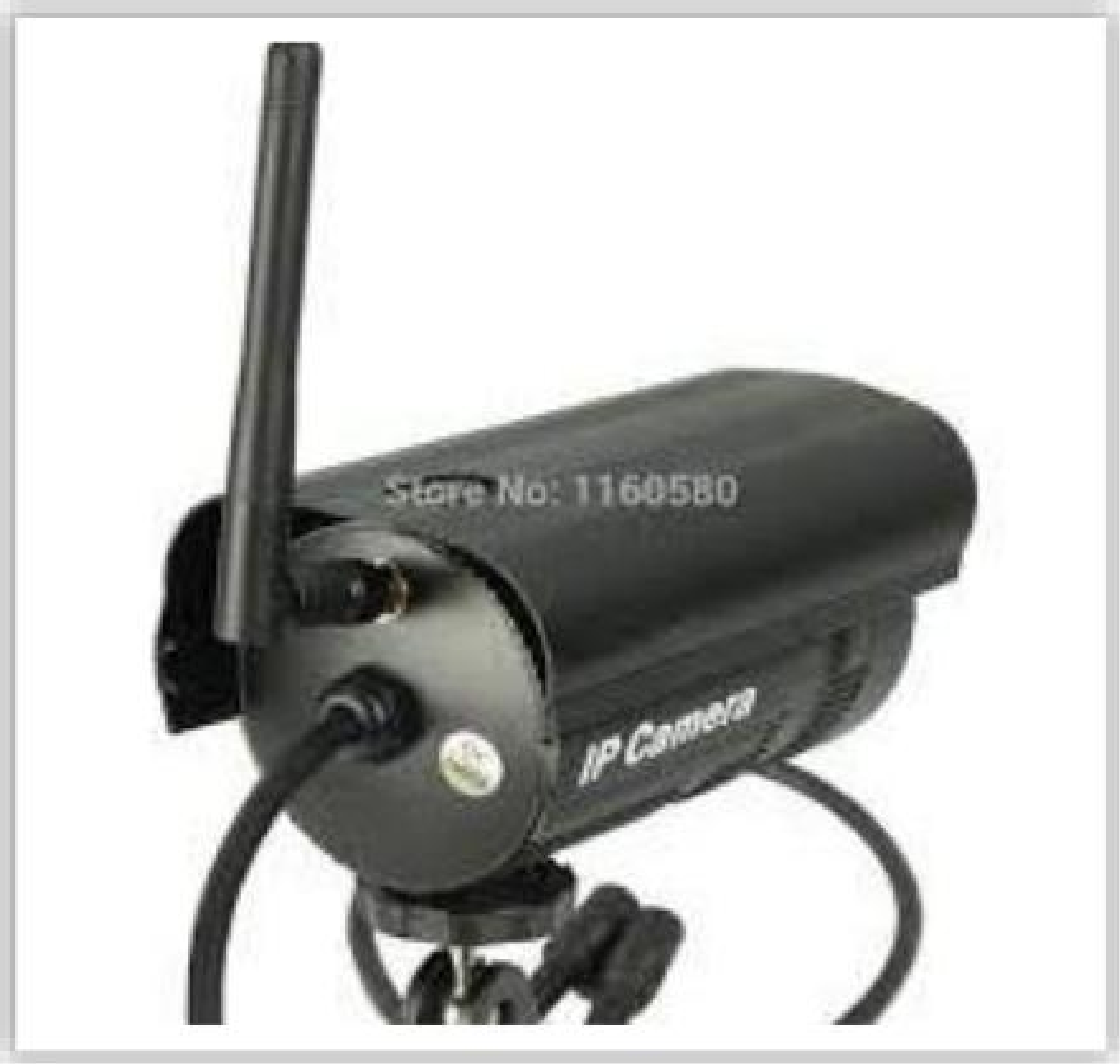


Figure 6.14: Network/IP CCTV Camera

- **Wireless CCTV:** Wireless CCTV cameras are easier to install than wired cameras and use different modes for wireless transmission.

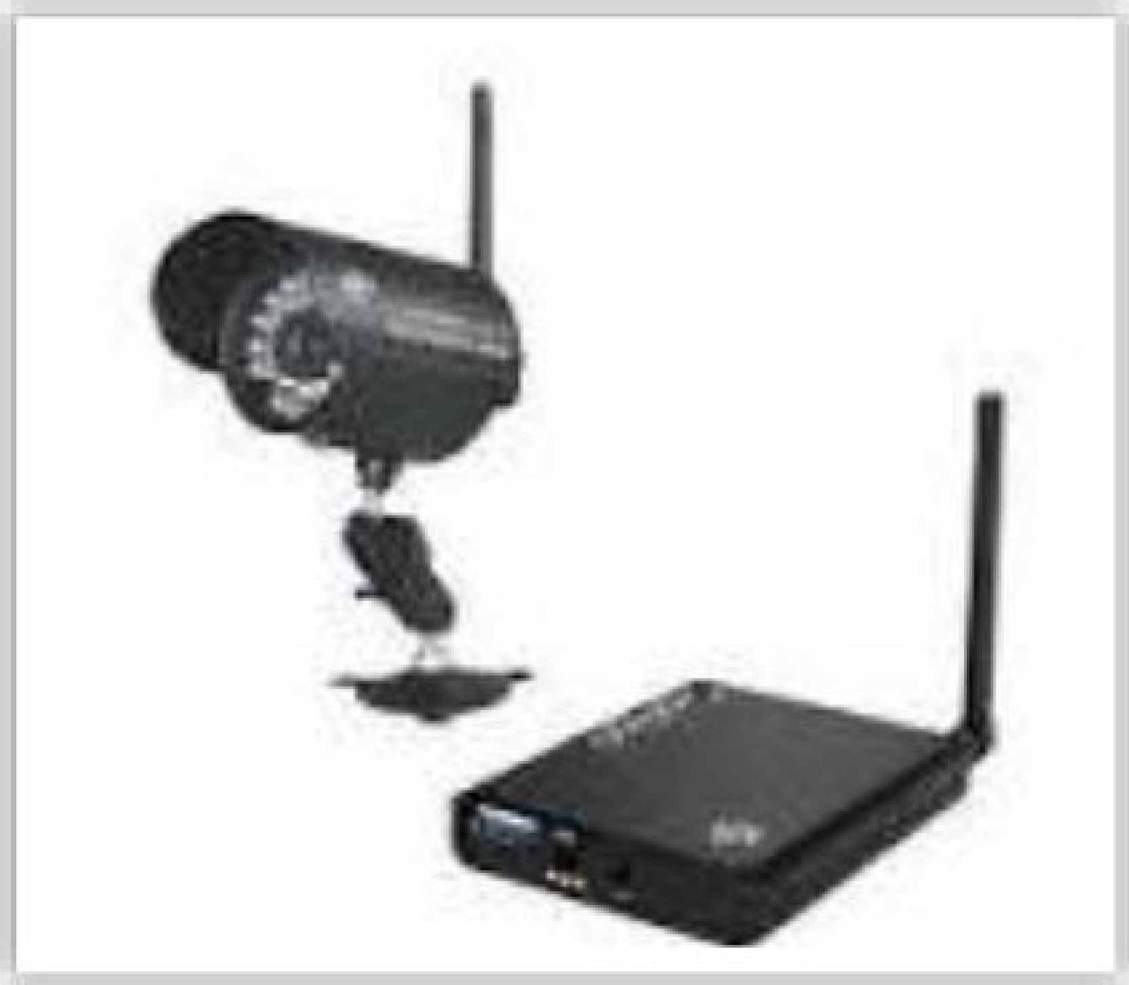
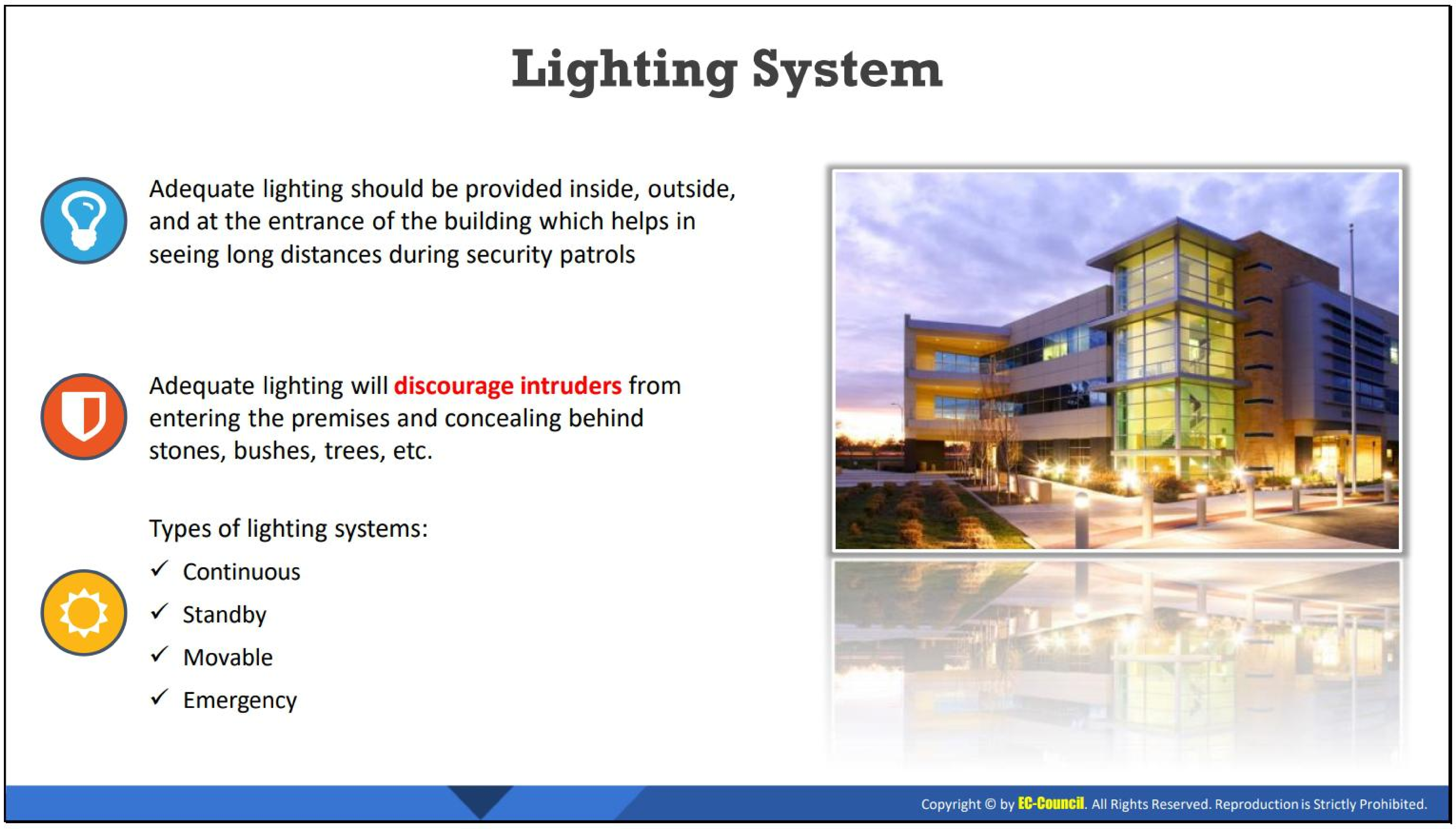


Figure 6.15: Wireless CCTV Camera

- **High-definition CCTV**: High-definition CCTV cameras are mainly used in sensitive locations that require greater attention. They allow operators to zoom into a particular area.



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.

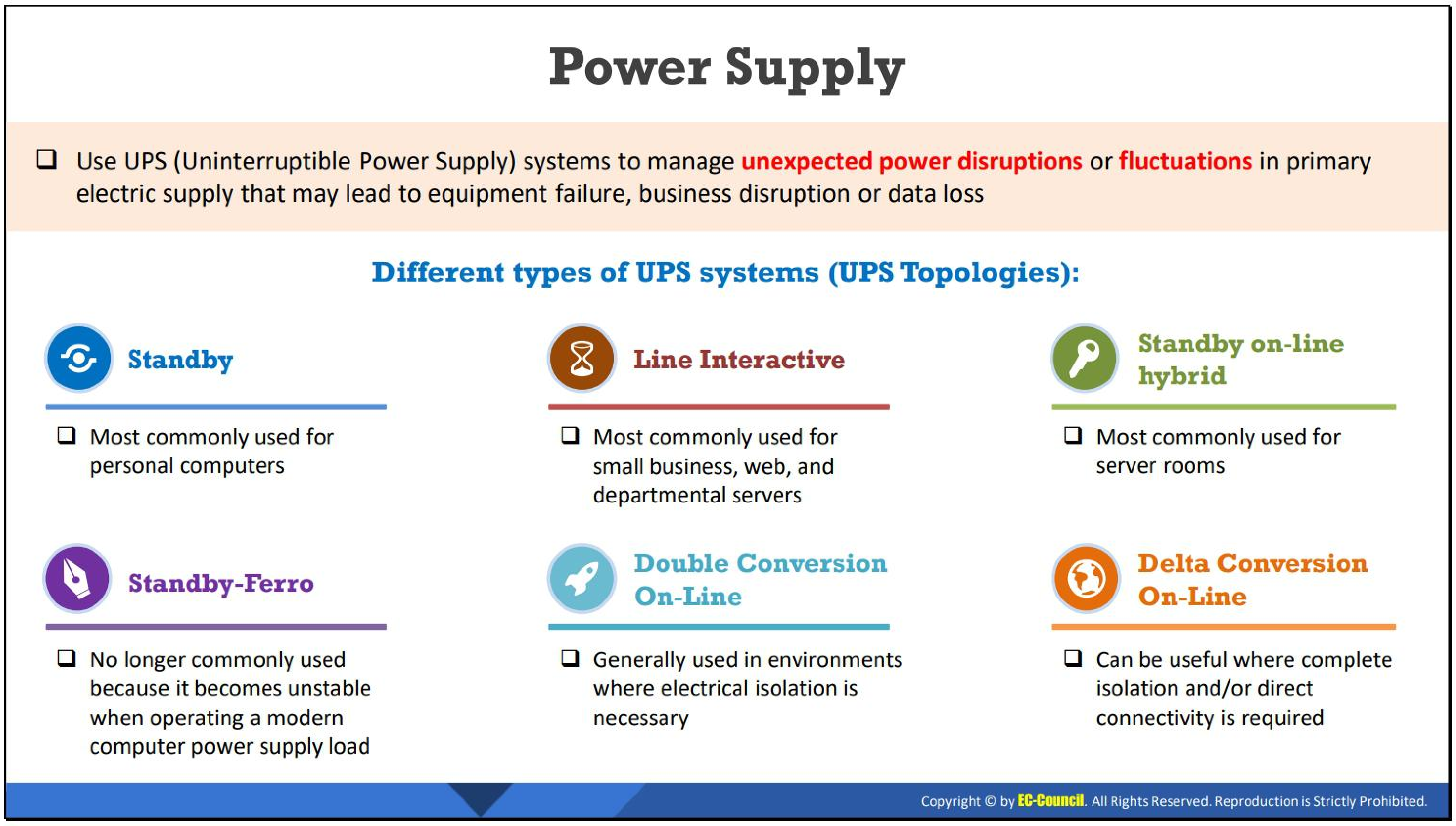
Types of lighting systems:

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

Lighting System

Security lighting is an important aspect of the physical security of a facility. If an organization has not implemented an adequate lighting system in and around its premises, the function or performance of all other security measures can be drastically degraded. For example, if the organization does not have lighting at rear corners, near bushes, plants, parking, and near surveillance cameras, then it is difficult to find people or objects hidden in these locations. With poor lighting, it is difficult to identify people entering the premises, and an intruder may act as an employee or use tricks to circumvent the security systems. The lighting systems to install in an area depend on the layout and sensitivity of the area. Alternate power systems such as generators should be installed to handle power failures and emergencies.

- **Continuous lighting**: Continuous lighting refers to fixed sets of lights arranged such that they provide continuous lighting to a large area throughout the night.
- **Standby lighting**: Standby lighting is used whenever any suspicious activity is detected by security personnel or by an alarm system. These systems operate either manually or automatically.
- **Movable lighting**: Movable lighting is a manually controlled lighting system that provides lighting at night or only when needed. These systems are normally used as an extension of a continuous or standby lighting system.
- **Emergency lighting**: Emergency lighting is used mainly during power failures or when other regular lighting systems fail to operate properly.



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

Power Supply

Facilities may suffer blackouts or power outages that could make systems inoperable unless appropriate alternative power management capabilities are implemented. Power outages could impact the ability to provide IT services as expected as well as the ability to provide physical security. Power spikes, surges, or blackouts could result in excessive or insufficient power and could damage equipment.

Consider the following security measures to handle blackouts or power outages.

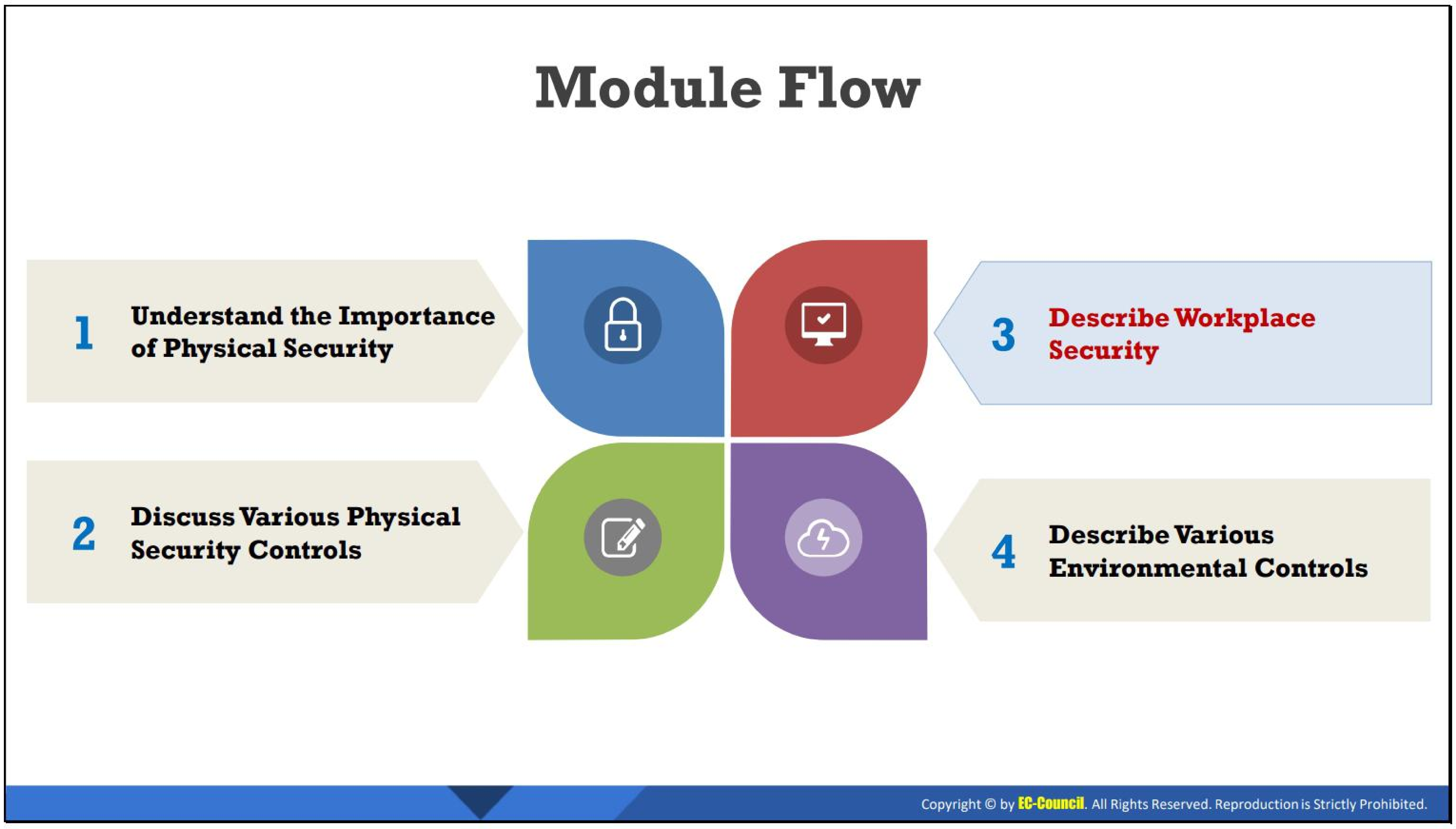
- Be prepared for power fluctuations.
- Use an uninterruptible power supply (UPS) to manage power outages.
- Safeguard systems from environmental threats.
- Protect systems from the adverse effects of static electricity at a workplace.
- Use plugging equipment properly.

A UPS allows computers to function properly during a power failure. It protects computers during fluctuations in the power supply as well. A UPS contains a battery that senses power fluctuations in the primary device. Users need to save all their data when the UPS senses a power fluctuation. The operator must provide procedures to follow at the time of power loss. A UPS is commonly used to protect computers, data centers, telecommunication equipment, etc.

The following are the different types of UPS include.

- **Standby:** Standby UPSes are the most commonly used type of UPS for personal computers. A standby UPS is an offline battery backup facilitating the maintenance of the primary device during a power fluctuation. A standby power supply contains AC-DC circuitry that connects to the UPS during a power fluctuation.

- **Line interactive:** Most commonly used for small business, web, and departmental servers, line interactive mainly handles continuous power fluctuations. This method of power supply needs very little battery usage.
- **Standby online hybrid:** Most commonly used for server rooms, standby online hybrid UPSes are mainly used to supply power below 10 kVA. They are connected to the battery during a power failure.
- **Stand by Ferro:** In this type of UPS, a Ferro resonant transformer is used for filtering the output. A standby Ferro UPS provides ample time for switching from the main power supply to battery power. This type of UPS is no longer commonly used because it becomes unstable when handling a modern computer's power load.
- **Double conversion online:** Generally used in environments where electrical isolation is necessary, a double conversion online UPS is used to supply power above 10 kVA. It provides an ideal electric output presentation, but its power components are subject to continuous wear, reducing its dependability. It exhibits a transfer time only during a large current load.
- **Delta conversion online:** A delta conversion online UPS can be useful when complete isolation and/or direct connectivity is required. It contains an inverter that supplies the load voltage. It can be used to supply power in the range between 5 kVA and 1 MW. It controls the power input performance and charging of the UPS battery.

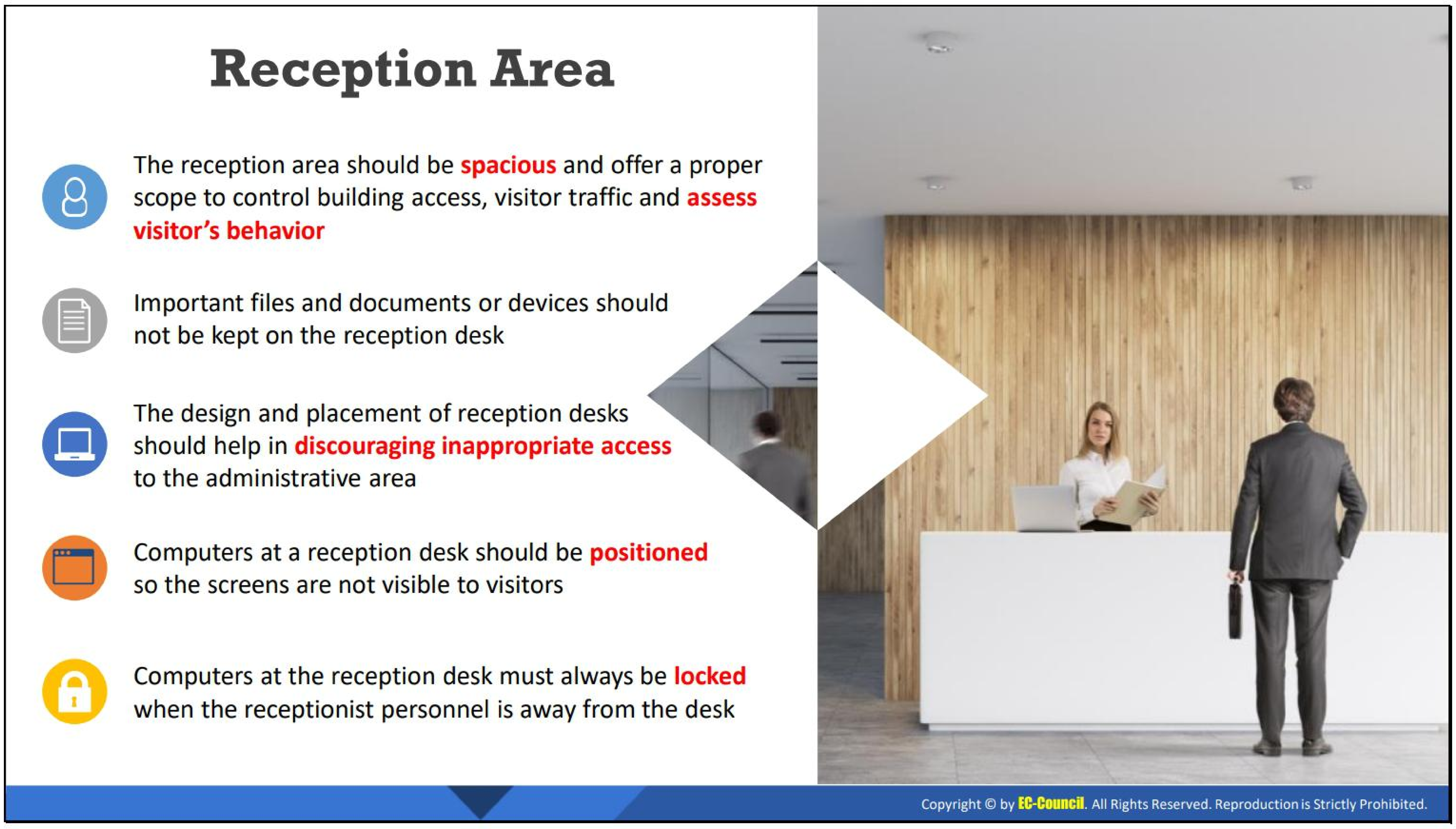


Module Flow

1 Understand the Importance of Physical Security
2 Discuss Various Physical Security Controls
3 Describe Workplace Security
4 Describe Various Environmental Controls
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Describe Workplace Security

This section explains workplace security in an office environment.



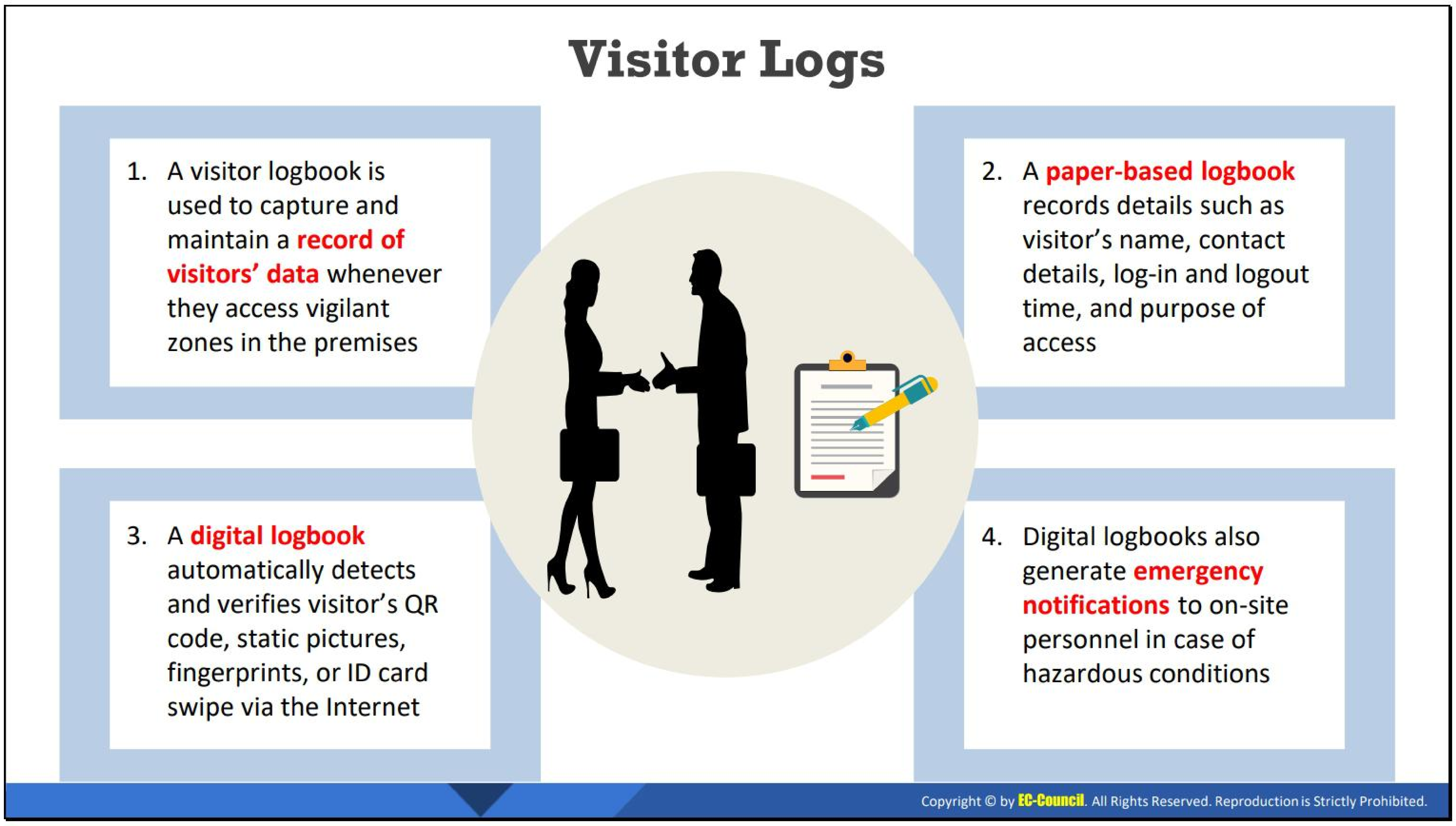
Reception Area

- 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

Reception Area

The reception area is the initial point of contact for an individual approaching the organization. The reception area can be vulnerable to physical security breaches as it provides easy access to strangers. Organizations often have regular visits from clients, the general public, invitees, etc. and require staff to greet, assist, and direct them. Receptionists should be able to recognize or identify any unusual behavior from people such as solicitors and peddlers, charity organizations, and ex-employees. The reception personnel should maintain eye contact and non-confrontational facial expressions or posture while meeting people. They should be proficient enough to handle emergency situations and follow procedures to call immediate attention, issue alarms, call for radio, administer first aid, etc.

The reception area should be spacious and should offer the scope to control building access and visitor traffic as well as assess visitor behaviors. Reception personnel should observe people entering the building. They should notice and record odd behavior from strangers. Benchmarks should be implemented to judge people arriving at the organization. Their intentions must be noted, and the personnel should identify whether a person is searching for someone or something. 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 that the screens are not visible to visitors and must always be locked when the reception personnel is away from the desk.

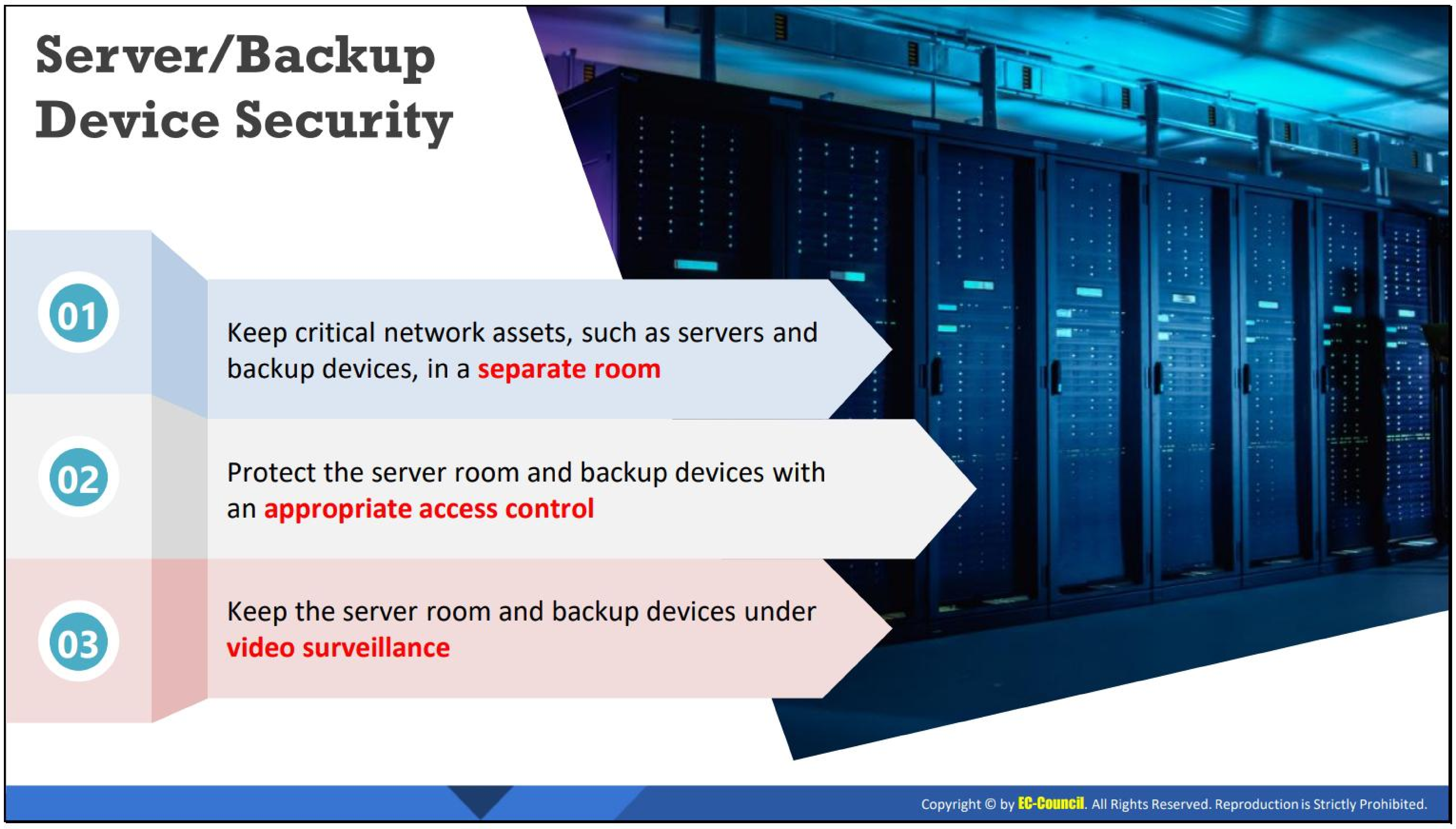


Visitor Logs

1. A visitor logbook is used to capture and maintain a **record of visitors' data** whenever they access vigilant zones in the premises
2. A **paper-based logbook** records details such as visitor's name, contact details, log-in and logout time, and purpose of access
3. A **digital logbook** automatically detects and verifies visitor's QR code, static pictures, fingerprints, or ID card swipe via the Internet
4. Digital logbooks also generate **emergency notifications** to on-site personnel in case of hazardous conditions

Visitor Logs

A visitor logbook is used to capture and maintain a record of visitors' data whenever they access vigilant zones in the premises. The logbook can either be digitally recorded online using automated software or maintained as a traditional paper-based visitor logbook at the entrance gate. A paper-based logbook records details such as the visitor's name, contact details, log-in and logout times, and purpose of visit. Alternatively, a digital logbook automatically detects and verifies the visitor's QR code, static pictures, fingerprints, or ID card swipe via the Internet. Both types of log records provide information about an individual visitor that includes details about the equipment, resources, or premises that they accessed or controlled. Additionally, a digital logbook generates emergency notifications for on-site personnel in case of hazardous conditions.



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**

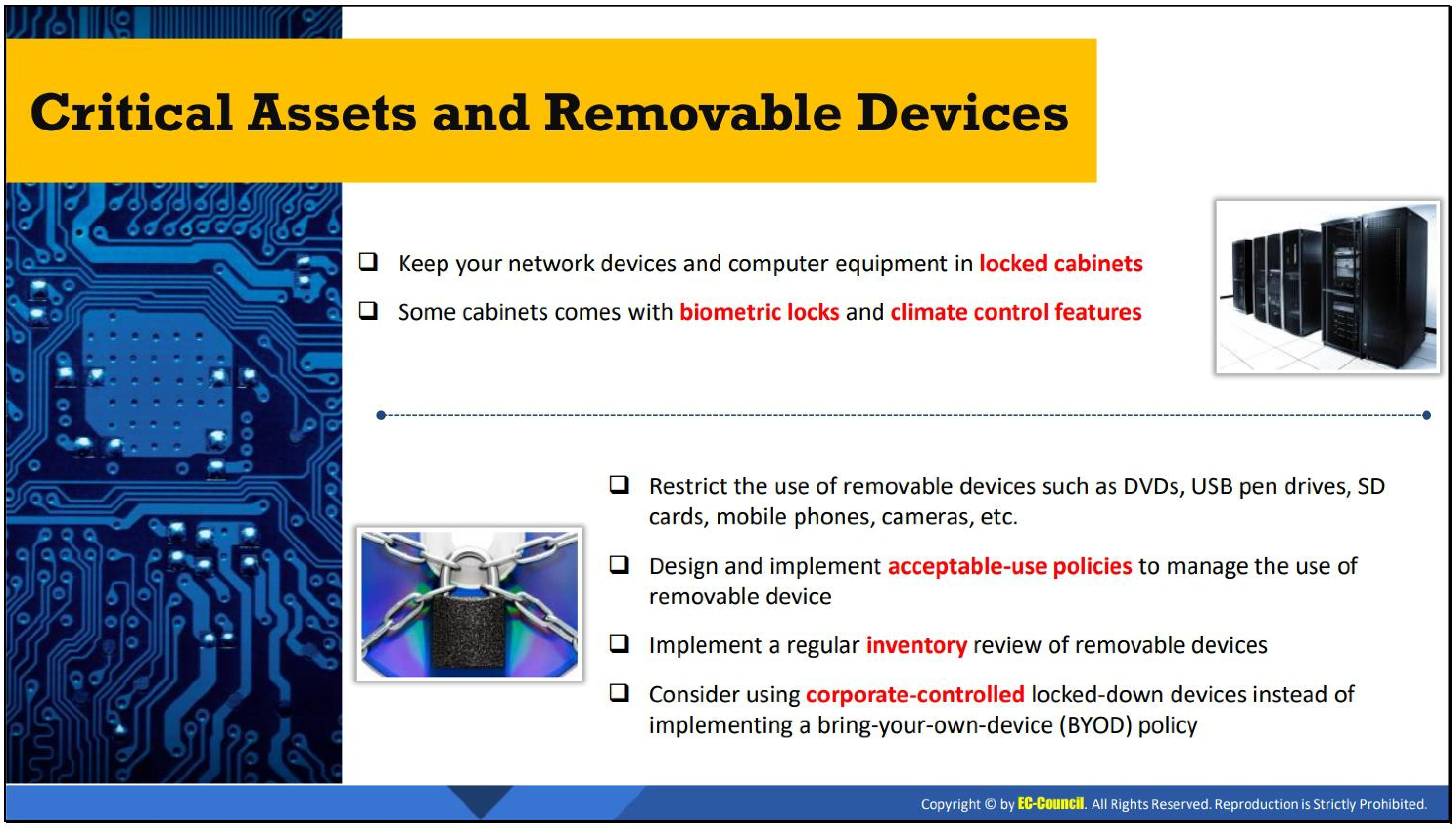
03 Keep the server room and backup devices under **video surveillance**

Server/Backup Device Security

An organization should consider the physical security of their critical servers and backup devices. Physical access to these devices should be restricted to only approved personnel.

The following are the typical physical security measures for server and backup devices:

- Keep the server and backup devices in a separate room. This reduces the accessibility of these devices for the public and unknown people.
- Mount CCTV, smart card, and biometric authentication to track and monitor unauthorized physical access to the server and backup devices.
- Use rack mount servers. This prevents attackers from stealing or damaging the servers.
- The server should be attached to a UPS that protects it from file damage or corruption due to temporary power loss.
- Keep the devices in locked drawers, cabinets, or rooms.
- Backup devices should be stored at off-site locations and secured.
- Discourage employees from taking backups on DVDs, USB drives, or external hard disks. Ensure that the backups are locked at all times in a drawer, safe, or separate room.
- Do not allow employees to leave an area while carrying a backup device. Use motion sensing alarms to detect the movement of any backup device.
- Implement full disk encryption on backup devices.



Critical Assets and Removable Devices

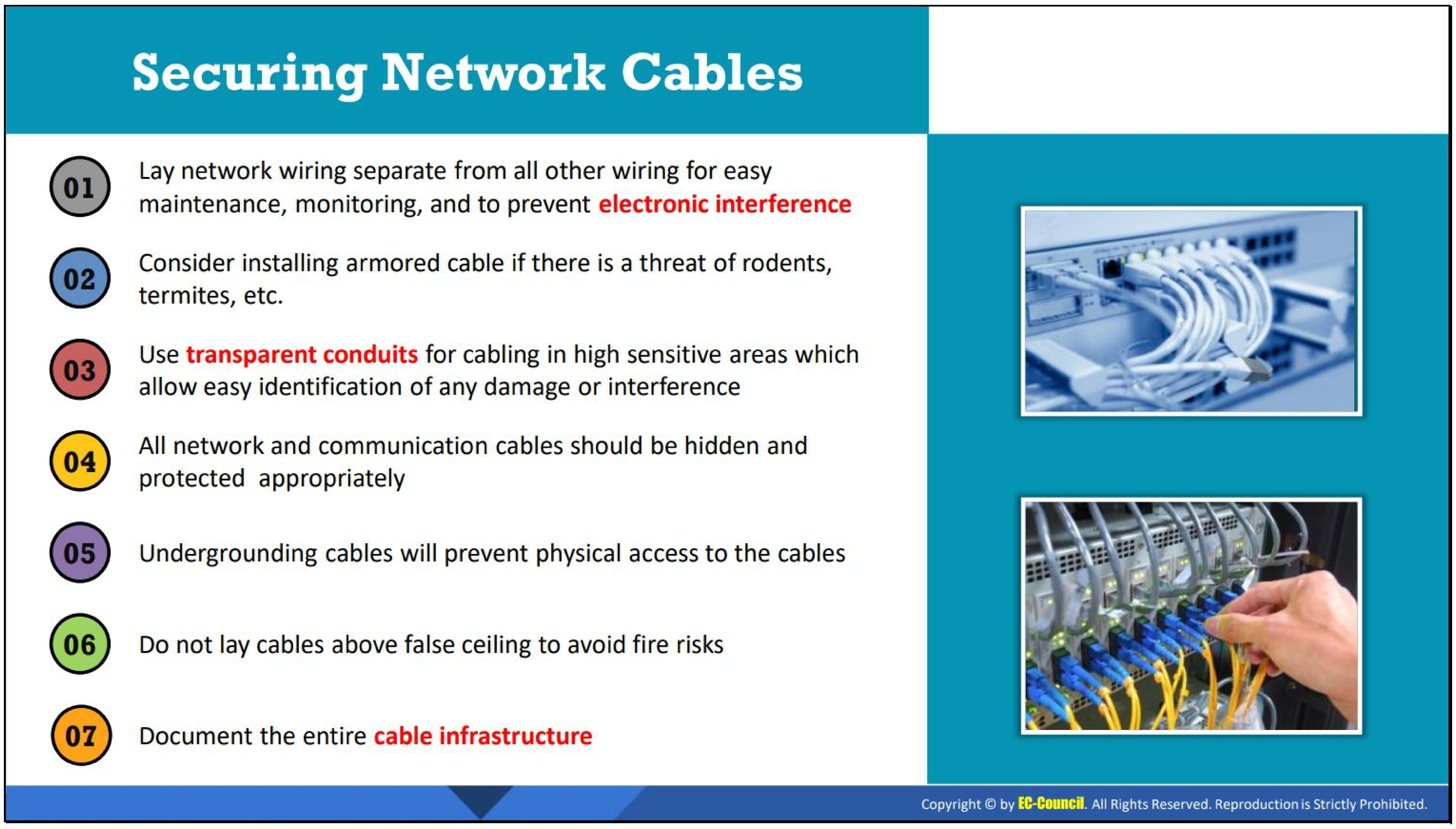
- ❑ Keep your network devices and computer equipment in **locked cabinets**
- ❑ Some cabinets comes with **biometric locks** and **climate control features**

- ❑ Restrict the use of removable devices such as DVDs, USB pen drives, SD cards, mobile phones, cameras, etc.
- ❑ Design and implement **acceptable-use policies** to manage the use of removable device
- ❑ Implement a regular **inventory** review of removable devices
- ❑ Consider using **corporate-controlled** locked-down devices instead of implementing a bring-your-own-device (BYOD) policy

Critical Assets and Removable Devices

An organization should always pay attention to the security of its server and backup storage devices. At the same time, the organization should not ignore the security of other critical assets such as workstations, routers and switches, printers, other network equipment, and removable devices. The organization should employ all the physical security measures of server/backup devices for critical assets and removable devices. Furthermore, organizations must keep their network devices and computer equipment in locked cabinets. Some cabinets come with biometric locks and climate control features. Restrict the use of removable devices such as DVDs, USB pen drives, SD cards, mobile phones, and cameras. Design and implement acceptable-use policies to manage the use of removable devices. Implement a regular inventory review of removable devices. Consider using corporate-controlled locked-down devices instead of implementing a bring-your-own-device (BYOD) policy.

- **Workstations**: Workstations at unoccupied desks, empty offices, reception desk, etc. are relatively more vulnerable to physical security breaches. Disconnect or remove such unoccupied workstations or otherwise lock the doors to the room where the workstation is located.
- **Routers and switches**: Keep these critical network devices in locked rooms.
- **Printers**: Like servers and workstations, printers can store important information, should be bolted down, and installed at separate locations.
- **Removable devices**: Portable removable devices such as laptops, handheld computers, mobile devices, SD cards, USB, and Bluetooth devices can pose physical security risks. Keep these devices in a drawer or safe, or permanently attach a cable lock.



Securing Network Cables

01 Lay network wiring separate from all other wiring for easy maintenance, monitoring, and to prevent **electronic interference**

02 Consider installing armored cable if there is a threat of rodents, termites, etc.

03 Use **transparent conduits** for cabling in high sensitive areas which allow easy identification of any damage or interference

04 All network and communication cables should be hidden and protected appropriately

05 Undergrounding cables will prevent physical access to the cables

06 Do not lay cables above false ceiling to avoid fire risks

07 Document the entire **cable infrastructure**

Securing Network Cables

Network cable security is often overlooked as an aspect of physical security. The organization should consider the importance of cable security before planning and installing any cabling. Network cabling should be neat; else, an organization can suffer from unplanned downtime. With flawed or insecure network cabling, an attacker can easily access sensitive information by bypassing other security controls. The risks associated with network cabling are wiretapping, physical damage, and theft.

The following are the considerations for securing network cabling:

- Lay network wiring separately from all other wiring for easy maintenance, monitoring, and preventing electronic interference.
- Consider installing armored cable if there is a threat of rodents, termites, etc.
- Use transparent conduits for cabling in highly sensitive areas to allow the easy identification of any damage or interference.
- All network and communication cables should be hidden and protected appropriately.
- Undergrounding cables prevent physical access to the cables.
- Do not lay cables above a false ceiling to avoid fire risks.
- Access to cabling pathways and spaces should be restricted to authorized personnel only.
- Create redundancy to avoid a single point of failure in case of a disaster.
- Document the entire cable infrastructure.

Types of Cable Used in Network Cabling

- **Unshielded Twisted Pair (UTP) Cable**

  A UTP cable reduces crosstalk and interference between pairs of wires but is prone to wiretapping. An attacker can easily tap the information transmitted through network cables.

  - **Advantages**
    - Easy to install
    - Suitable for domestic and office Ethernet connections
  - **Disadvantages**
    - Highly susceptible to electromagnetic and radio-frequency interference
    - Less commonly used for long-distance networking

- **Shielded Twisted Pair (STP) Cable**

  In an STP cable, each pair of wires is individually shielded with foil. It is less susceptible to external interference as the shielding absorbs all the EMI and RFI signals.

  - **Advantages**
    - Immune to crosstalk and interference
    - Ensures secure data transmission
  - **Disadvantages**
    - More expensive than UTP cables
    - More difficult to install than UTP cables

- **Fiber-optic Cable**

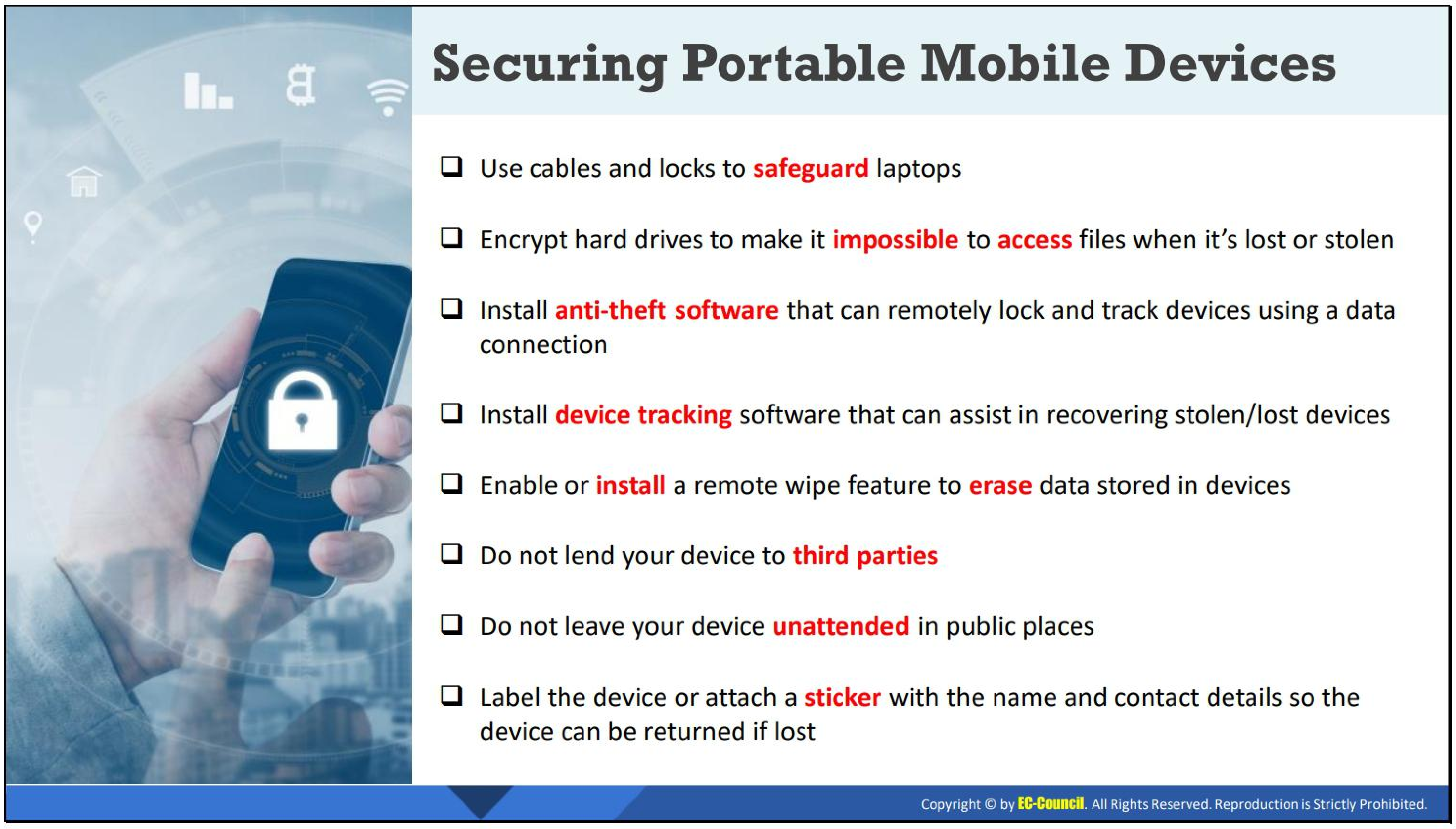
  A fiber-optic cable is made of glass or plastic. Fiber-optic cabling is the least susceptible to wiretapping threats.

  - **Advantages**
    - Can carry information over relatively great distances
    - Immunity to electromagnetic interference
    - No crosstalk
  - **Disadvantages**
    - Limited physical arc of the cable
    - Highly expensive
    - Need for optical transmitters and receivers

- **Coaxial Cable**

  A coaxial cable is made of a single copper conductor at its center. A plastic layer insulates the center conductor and a braided metal shield, which prevents interference from fluorescent lights, motors, etc.

  - **Advantages**
    - Can carry information over relatively great distances
    - Moisture resistant
  - **Disadvantages**
    - Does not bend easily and difficult to install



Securing Portable Mobile Devices

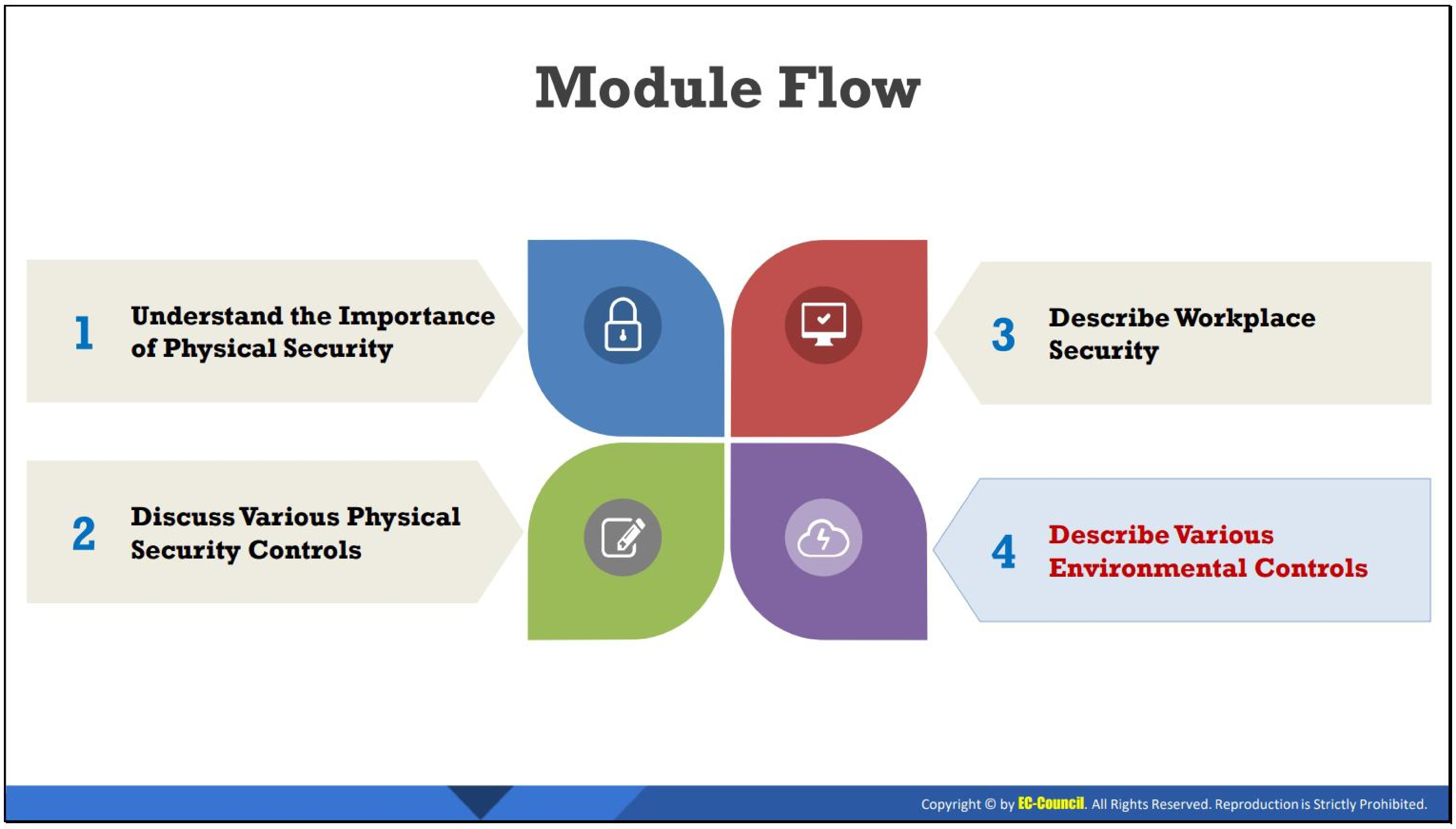
- □ Use cables and locks to **safeguard** laptops
- □ Encrypt hard drives to make it **impossible** to **access** files when it's lost or stolen
- □ Install **anti-theft software** that can remotely lock and track devices using a data connection
- □ Install **device tracking** software that can assist in recovering stolen/lost devices
- □ Enable or **install** a remote wipe feature to **erase** data stored in devices
- □ Do not lend your device to **third parties**
- □ Do not leave your device **unattended** in public places
- □ Label the device or attach a **sticker** with the name and contact details so the device can be returned if lost

Securing Portable Mobile Devices

The use of portable mobile devices in an organization has increased over the past few years. The risk of physical security threats to these devices has also increased. These devices are often vulnerable to physical threats such as theft, loss, damage, and resale. The organization should take proper care to handle any security incidents related to these devices.

- Apply all security measures common to network devices such as servers, backup devices, and portable devices.
- Physically secure the mobile device location.
- Apply proper access control procedures for these devices.
- Use cables and locks to safeguard laptops.
- Encrypt hard drives to make it impossible to access files when a drive is lost or stolen.
- Install anti-theft software that can remotely lock and track devices using a data connection.
- Install device tracking software that can assist in recovering stolen/lost devices.
- Enable or install a remote wipe feature to erase data stored in devices.
- Do not lend a device to third parties.
- Do not leave a device unattended in public places.
- Label the device or attach a sticker with the name and contact details of the user so that the device can be returned if lost.

- Enable the lockout option so that the device is locked when consecutive unsuccessful attempts to login are made.
- Use a docking station that permanently affixes the laptop to the desktop and also locks the laptop securely in one place.
- Use security gadgets such as motion detectors and alarms to issue alerts when the laptop is moved without authorization.



Module Flow

1 **Understand the Importance of Physical Security**

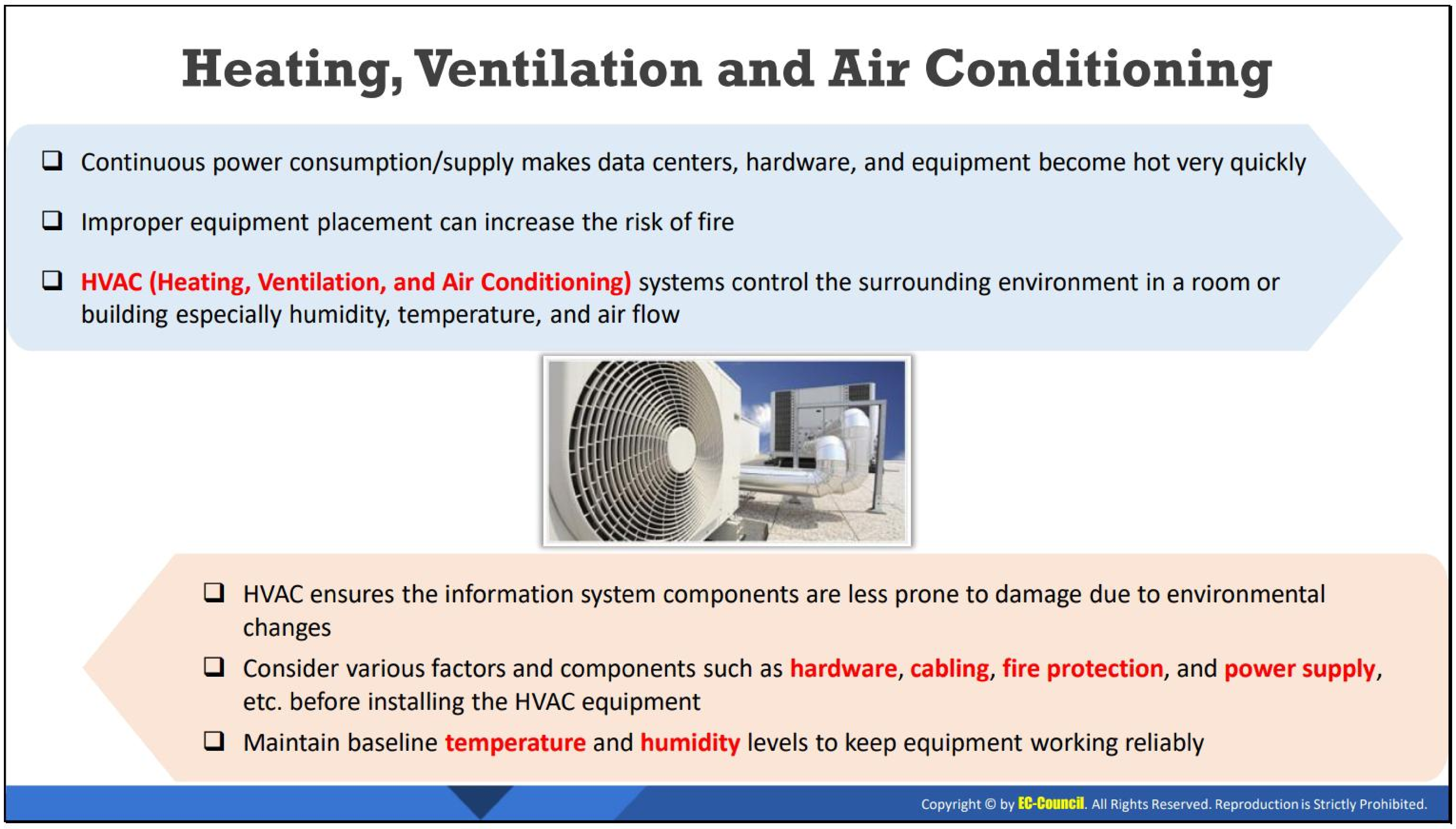
2 **Discuss Various Physical Security Controls**

3 **Describe Workplace Security**

4 **Describe Various Environmental Controls**

Describe Various Environmental Controls

This section explains 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

Heating, Ventilation and Air Conditioning

Continuous power consumption/supply can cause data centers, hardware, and equipment to become hot very quickly. Furthermore, improper equipment placement can increase the risk of fire. The HVAC is a special system that controls the environment in a room or building, especially the humidity conditions of the air and ventilation. It is deployed to maintain comfortable temperatures in a room so that the hardware is not affected by moisture and changes in the air. In these controlled conditions, the hardware and components are also safer and less prone to damage due to environmental factors. The HVAC also purifies the air in rooms and removes smoke, odor, heat, and dust particles. An environment where the air is odor-free and clean and the humidity is controlled provides a good atmosphere for the people working with that organization. These ventilation systems are desired mostly in medium- to large-scale organizations that use heavy equipment and employ a large number of people. A pre-programmed sensing device is used to check for changes in the temperature, and the HVAC acts accordingly. The HVAC can also be manually controlled. Before installing the HVAC equipment, the organization must consider various factors and components such as hardware, cabling, fire protection, and power supply. Baseline temperature and humidity levels must be maintained to keep equipment working reliably. Equipment that emits hot or cold air should be continuously monitored.

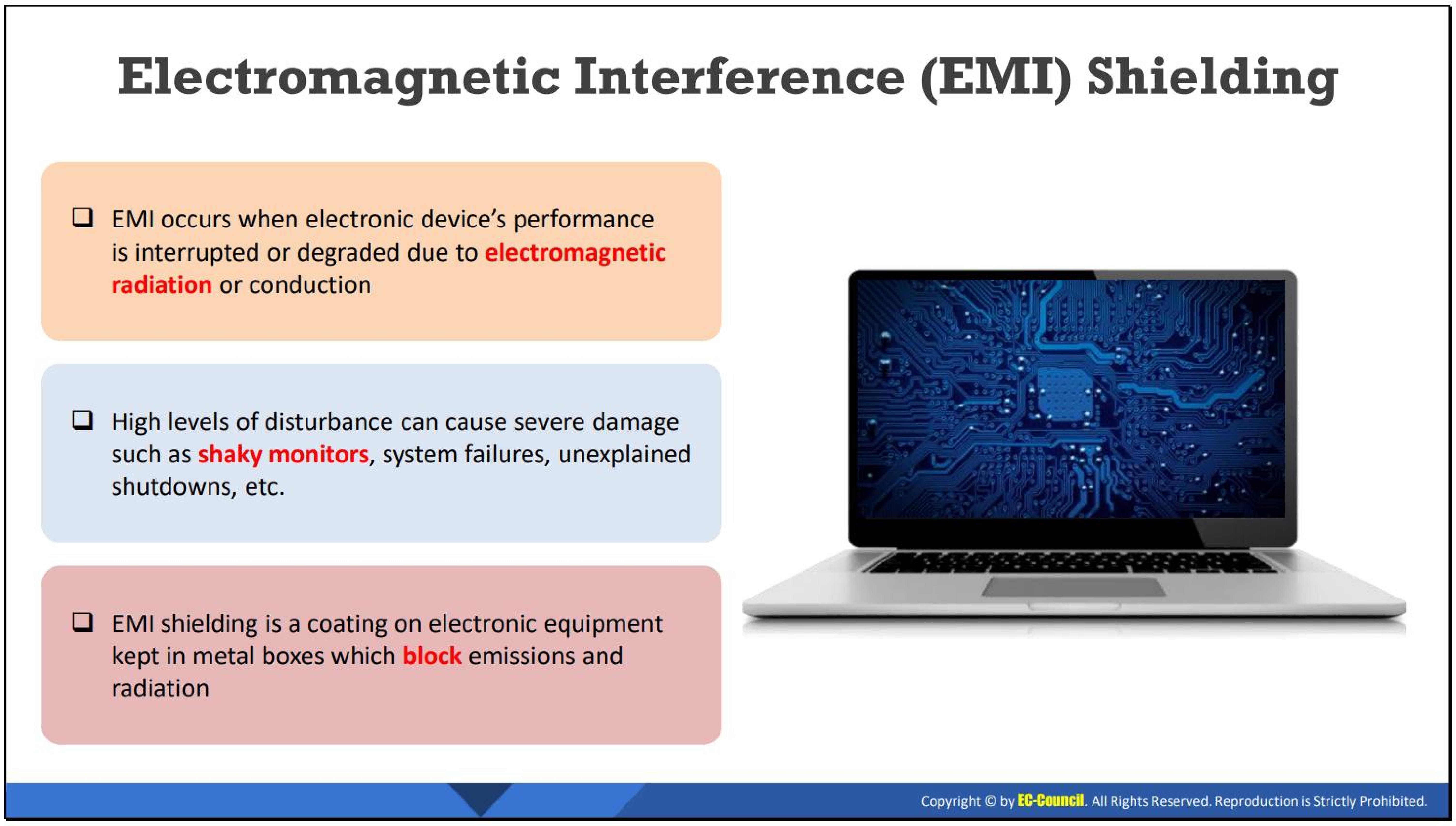
When a refrigeration component is added to an HVAC system, it is known as an HVAC&R or HVACR (heating, ventilating, and air conditioning & refrigeration) system.

Types of HVAC Systems

- **Heating and air-conditioning split system:** The traditional and most commonly used HVAC system is the heating and air-conditioning split system. The components of this system may be found both inside and outside the building. HVAC split systems have the following components:

  - An air conditioner to cool the refrigerant
  - Furnaces, a fan, or an evaporator coil for converting the refrigerant and circulating the air
  - A duct to allow air flow throughout the building
  - Air-quality fittings such as air cleaners and air purifiers

- **Hybrid heat split system:** This is an advanced version of a split system having better energy efficiency. In this system, the heat pump realizes an electrically fueled HVAC instead of gas furnace heat. A typical hybrid heat split system includes the following components:
  - A heat pump to cool/heat the refrigerant
  - Furnaces or an evaporator coil to convert the refrigerant and circulate the air
  - A duct to allow air flow throughout the building
  - Controls or a thermostat as an interface to control the system
  - Air-quality fittings such as air cleaners and air purifiers
- **Duct-free split heating and air-conditioning system:** Most commonly used in locations where traditional split systems cannot be used, a typical duct-free split system includes the following components:
  - An air conditioner to cool the refrigerant
  - A fan coil to convert the refrigerant and circulate the air
  - Refrigerant tubing and wires to connect the outdoor unit to the fan coil
  - Controls or a thermostat as an interface to control the system
  - Air-quality fittings such as air cleaners and air purifiers
- **Packaged heating and air-conditioning system:** This is the most effect air-conditioning system and is used mainly in locations with adequate space for fixing all the components of a split system. Packaged units can be used in spaces that range from an entire building to one-room units. A packaged heating and air-conditioning system includes the following components:
  - Packaged products such as a heat pump or an air conditioner combined with a fan coil or an evaporator coil in a single unit
  - Controls or a thermostat as an interface to control the system
  - Air-quality fittings such as air cleaners and air purifiers.



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.

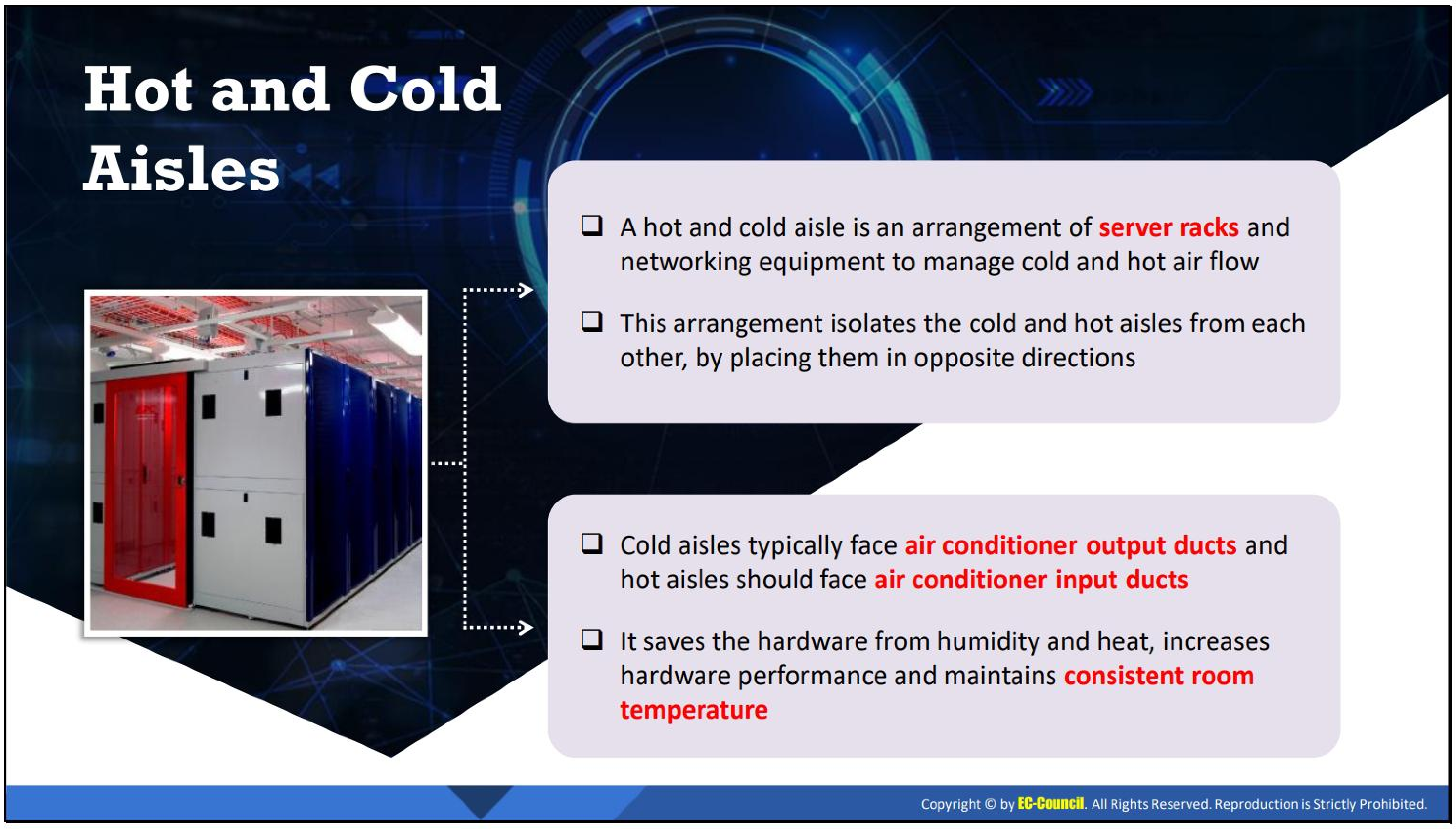
❑ EMI shielding is a coating on electronic equipment kept in metal boxes which **block** emissions and radiation

Electromagnetic Interference (EMI) Shielding

Electromagnetic radiation emitted from different electronic devices interferes with surrounding devices and causes problems with their functioning. High levels of disturbance can cause severe damage such as shaky monitors, system failures, and unexplained shutdowns. EMI shielding is the practice of coating electronic equipment with metals so that electromagnetic waves do not interfere with other devices or the field is blocked with certain materials. EMI shields separate one part of the equipment from another.

Shielding uses materials such as metals or metal foams. An electric field produces a charge on the conducting material, applying an electromagnetic field on a conductor. The conductor produces another charge, which cancels the effect of the electric charge externally applied on it. This causes no change in the conducting material. When the electric field is applied to the material, it produces eddy currents (currents that flow within a material in closed loops). These currents cancel the effect of the magnetic field. In this manner, the shielded material is protected from outside effects or disturbances.

For organizations that use heavy equipment, electronic hardware interference is a problem, and EMI shielding is needed for all devices in these types of environments. Many industries such as the telecommunication and healthcare industries prefer to use EMI shielding.



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**

Hot and Cold Aisles

Hot and cold aisles form a systematic arrangement of equipment to maintain air flow and to save energy. Many organizations follow the hot and cold aisle alignment, which is mostly used in server rooms, data centers, etc. where heavy electronic equipment is used.

Racks of heavy equipment or servers are arranged so that the fronts of the equipment face the cold air from air conditioners. The backs of the equipment face the back of the next rack of equipment. This arrangement is followed for all the equipment in the room, pushing the hot air from the back of the equipment to one end of the room. The cooling conditions are kept so that the hot air exiting the equipment is sucked out and does not mix with the cool air inside the room. Depending on convenience, the cooling system is placed below or above the room. Cold aisles typically face air-conditioner output ducts, and hot aisles face air-conditioner input ducts. This protects the hardware from humidity and heat, increases hardware performance, and maintains a consistent room temperature.

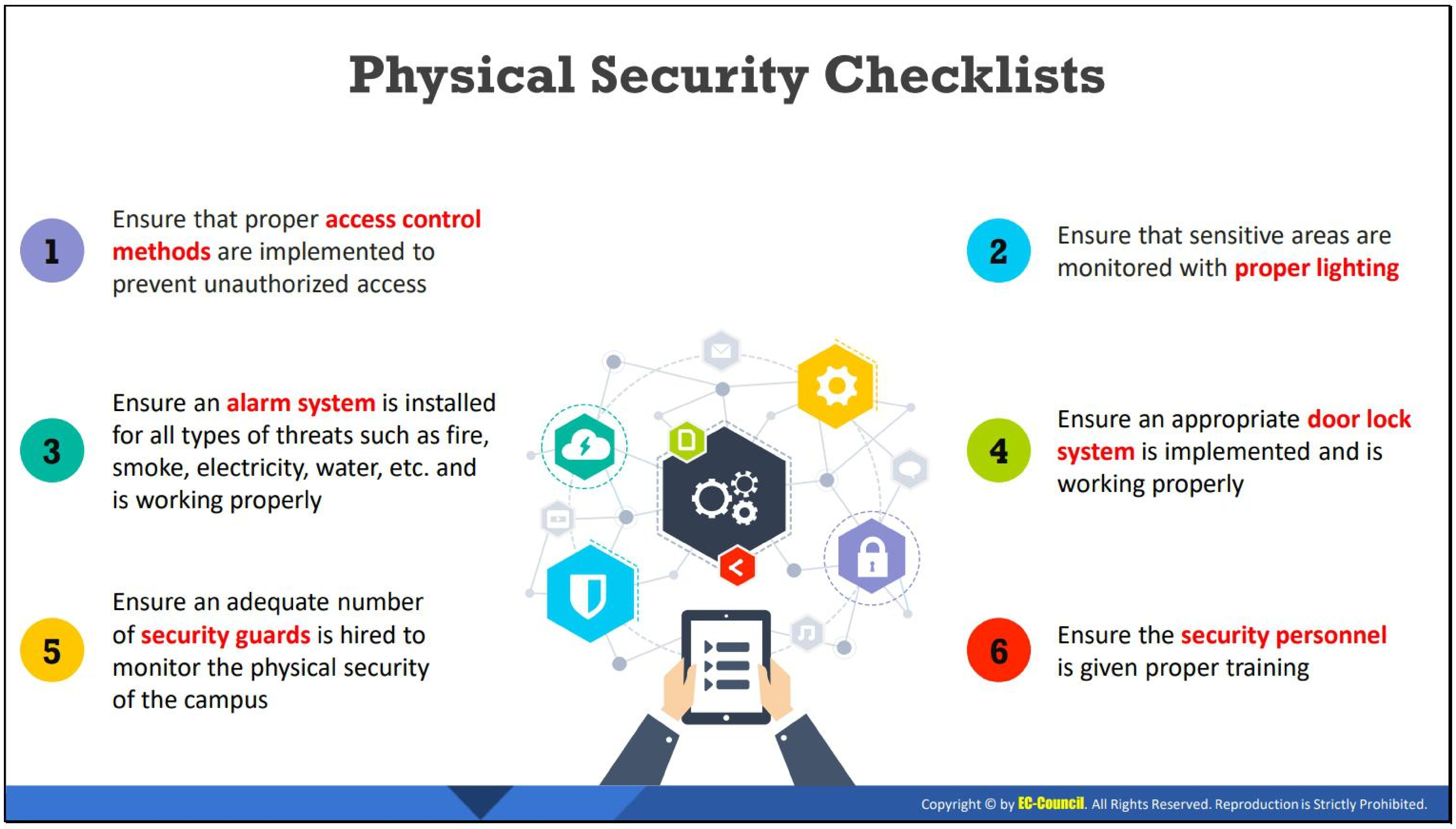
Cold Aisle: Advantages and Disadvantages

- **Advantages:**
  - Easy to implement as it does not require any supplementary architecture to expel air
  - Requires doors only at the end
  - Relatively less expensive
  - Can easily fit into an existing data center in terms of aspects such as power and network distribution
  - Can be used with a raised floor supply space
  - Controls the air supply to match severe airflow

- **Disadvantages:**
  - Creates operational issues if low-density storage or communication racks are installed in the data-center space
  - Most cold aisles have ceilings immediately above the aisle, affecting fire and lighting design.
  - Air leaked from raised floors and openings under the equipment enters the air paths to the cooling units, affecting the efficiency of the system.

Hot Aisle: Advantages and Disadvantages

- **Advantages:**
  - Leakage from raised floor openings is passed over to the cold space
  - Relatively more effective
  - Works well in a slab environment by supplying an adequate volume of air and covering the exhaust air
  - Provides cooling to general data-center space
  - Perfect distribution of air throughout the space
- **Disadvantages:**
  - Always requires additional space for the flow of air from the hot aisle to the cooling unit
  - Very expensive
  - Uncomfortable for technicians during maintenance work



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. Ensure an **alarm system** is installed for all types of threats such as fire, smoke, electricity, water, etc. and is working properly

4. Ensure an appropriate **door lock system** is implemented and is working properly

5. Ensure an adequate number of **security guards** is hired to monitor the physical security of the campus

6. Ensure the **security personnel** is given proper training

Physical Security Checklists

Physical security for an organization can be built in layers or implemented by following a defense-in-depth strategy. The organization should consider implementing all the physical security controls and measures to ensure defense-in-depth physical security.

The following checklist can help an organization ensure that they are implementing the proper security controls and measures.

- **Follow copyright rules and licensing restrictions:** The organization should enforce copyright rules and licensing restrictions to prevent outsiders or insiders from creating illegal copies of copyrighted software.

- **Store all removable and important items in a locker when not in use:** Employees should lock all sensitive information and important devices in a locker. They should not leave any important information unattended, as it may catch the eye of an attacker.

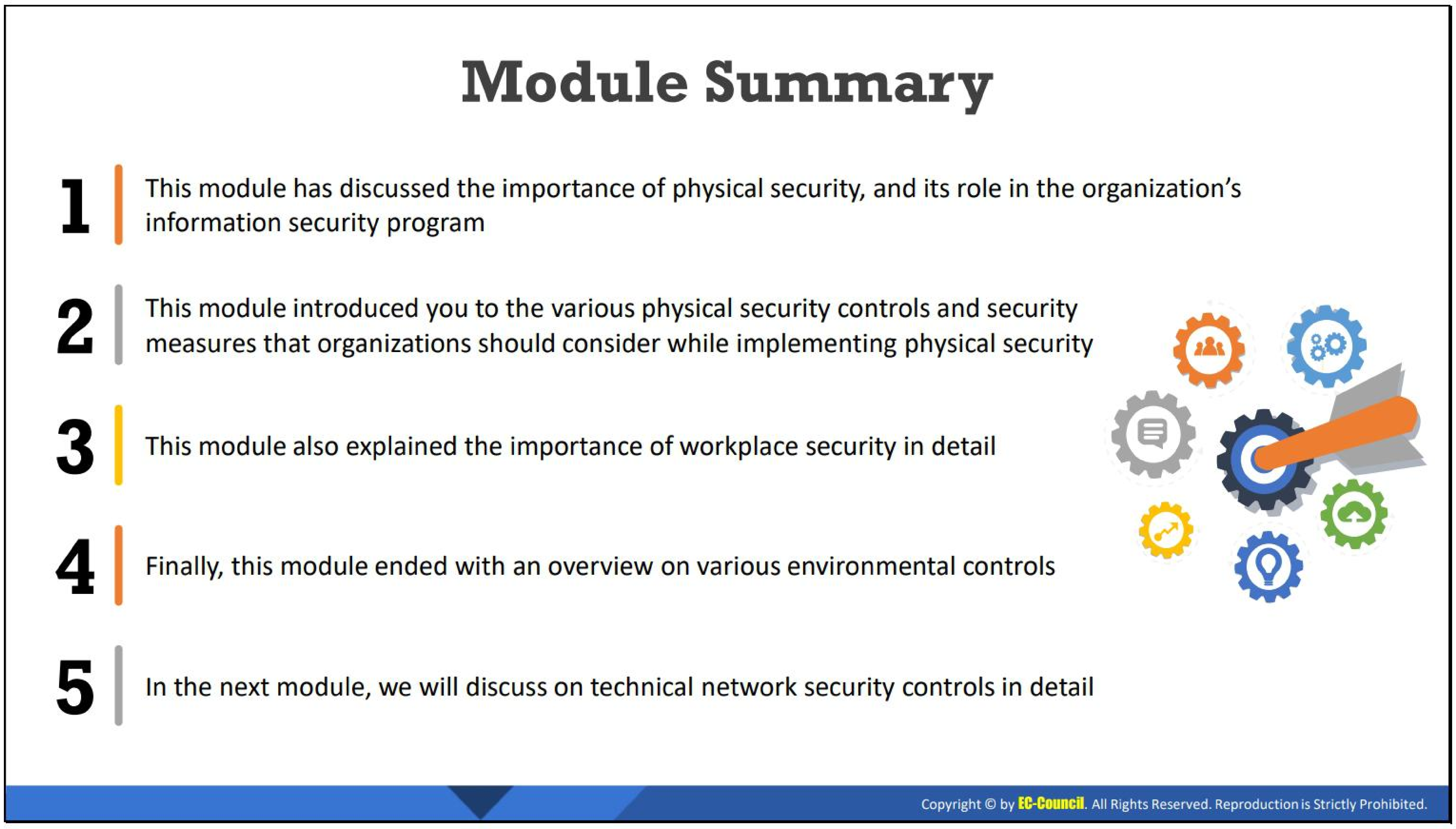
- **Keep sensitive areas under surveillance:** The organization should ensure security for sensitive areas such as server rooms. CCTV surveillance and guards may be employed to maintain security in sensitive areas. The organization should enforce 24 × 7 surveillance for these areas.

- **Always advise employees to swipe their card at the entrance:** Swiping ID cards at the entrance helps an organization audit the login details of employees in case of an incident.

- **Avoid keeping any combustible material in the workplace:** Always keep combustible materials away from the workplace. This ensures the safety of the employees, the information stored, and the devices stored inside the workplace.

- **Always ensure company satisfaction:** Employ security measures that guarantee the satisfaction of the employees. The policies and procedures imposed by the organization should ensure compatibility with the company infrastructure. Physical security measures imposed should detect, report, correct, and prevent attacks.
- **Evaluate the physical security of the location:** Proper security ensures the security of the employees and the information in the organization. The security of the location can be enhanced by preventing attackers from entering the workstations and server rooms as well as authenticating each person using ID cards or biometrics. Other security measures include locking cabinets, doors and windows, proper surveillance using CCTV, and proper lighting.
- **Avoid disconnecting consoles from ports:** Disconnecting cables or consoles from ports will lead to a disconnection for the user. Cables should all be connected to the ports and working properly.
- **Use of alarms and sensors during fire, smoke, etc.:** The organization should ensure the proper use of sensors and alarms to detect fire or smoke on the premises. The organization may include sensors for devices to detect any attempt to take those devices out of the organization's premises.
- **Prevent damage to hardware and software:** Any damage to the hardware or software results in damage to the information systems in the organization. Damage to the hardware leads to damage to the electronic and mechanical systems used in data processing. Damage to the software leads to damage to the programs and instructions used for data development.
- **Avoid leaving any devices or important data in parking areas or cars:** Any unattended devices or data may attract attackers and lead to the loss of these valuable items or information. The organization should employ an adequate number of security guards to monitor all parked cars. Proper lighting must be installed to watch these areas clearly. Security cameras should be employed in sensitive areas, and the personnel accessing those areas should be logged.
- **Avoid storing confidential information on mobile devices:** Storing sensitive information in a mobile device is not recommended, as it is easy to manipulate the data stored in a mobile device. Attackers may gain access to mobile devices and then acquire all of its sensitive information.
- Ensure that proper access control methods are implemented to prevent unauthorized access.
- Ensure that sensitive areas are monitored with proper lighting.
- Ensure that an alarm system is installed for all types of threats such as fire, smoke, power loss, and flood and is working properly.
- Ensure that an appropriate door lock system is implemented and is working properly.

- Ensure that an adequate number of security guards are hired to monitor the physical security of the campus.
- Ensure that the security personnel is properly trained.
- Ensure that the security personnel is hired from a trusted agency.
- Ensure that surveillance cameras are working properly and monitored regularly.
- Ensure that proper procedures are implemented for detecting and reporting physical security incidents.
- Ensure that employee contact information is maintained for use during emergencies.



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 the importance of workplace security in detail

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

Module Summary

This module discussed the importance of physical security and its role in an organization's information security program. Furthermore, this module introduced the various physical security controls and security measures that organizations should consider while implementing physical security. The module also explained in detail the importance of workplace security. Finally, this module presented an overview of various environmental controls.

In the next module, we will discuss technical network security controls in detail.