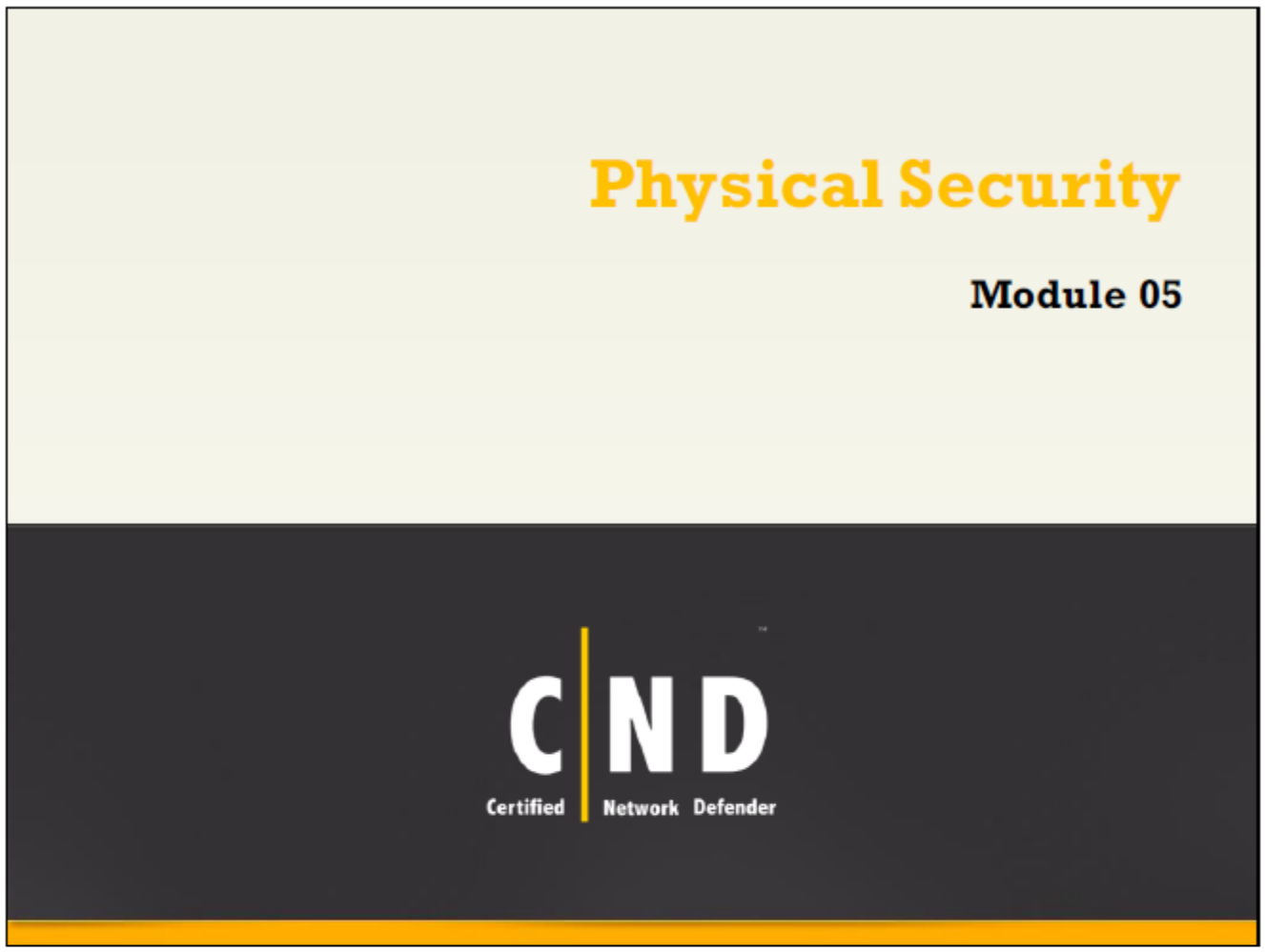
Physical Security

Module 05



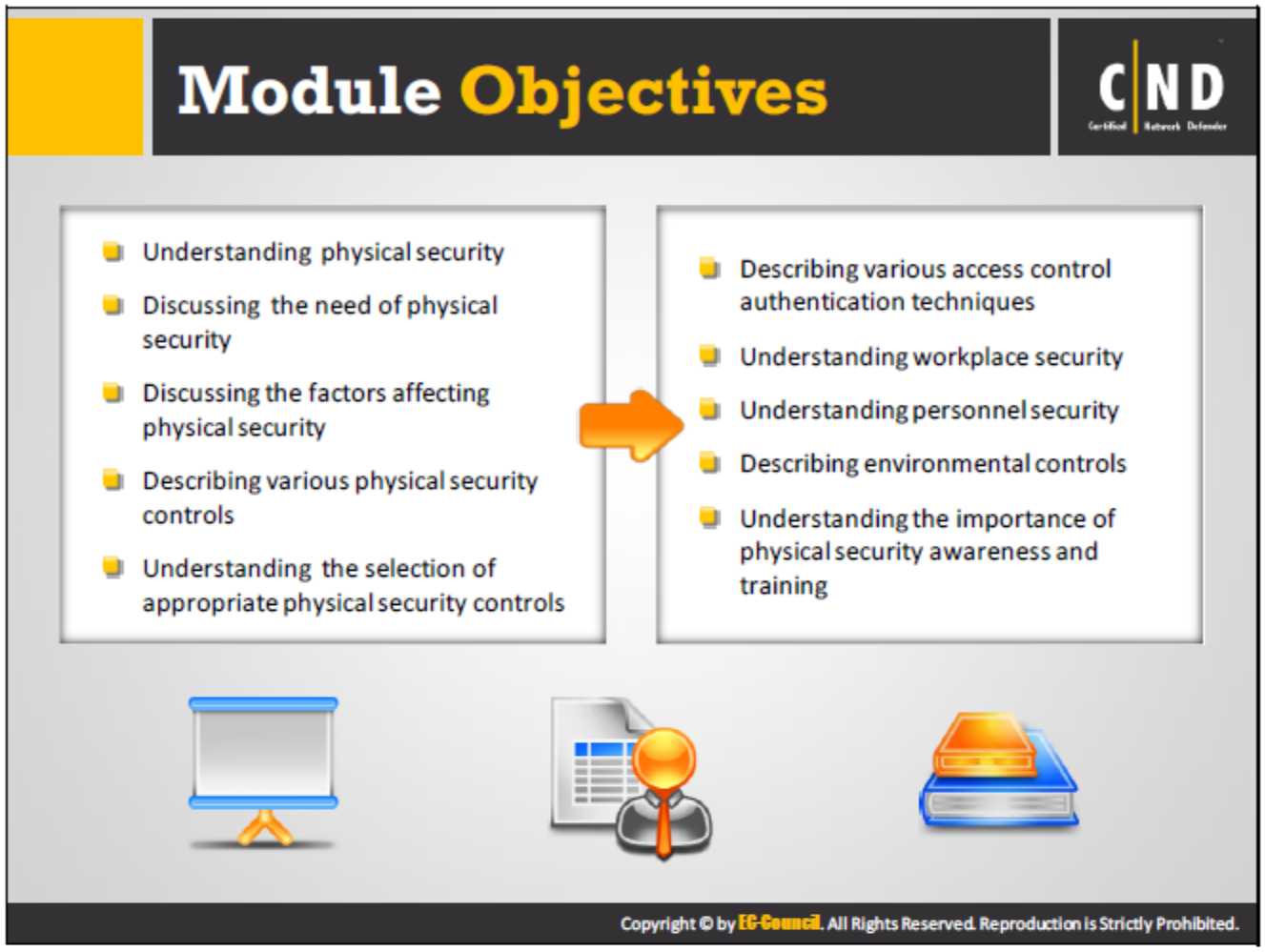
Certified Network Defender

Module 05: Physical Security

Exam 312-38

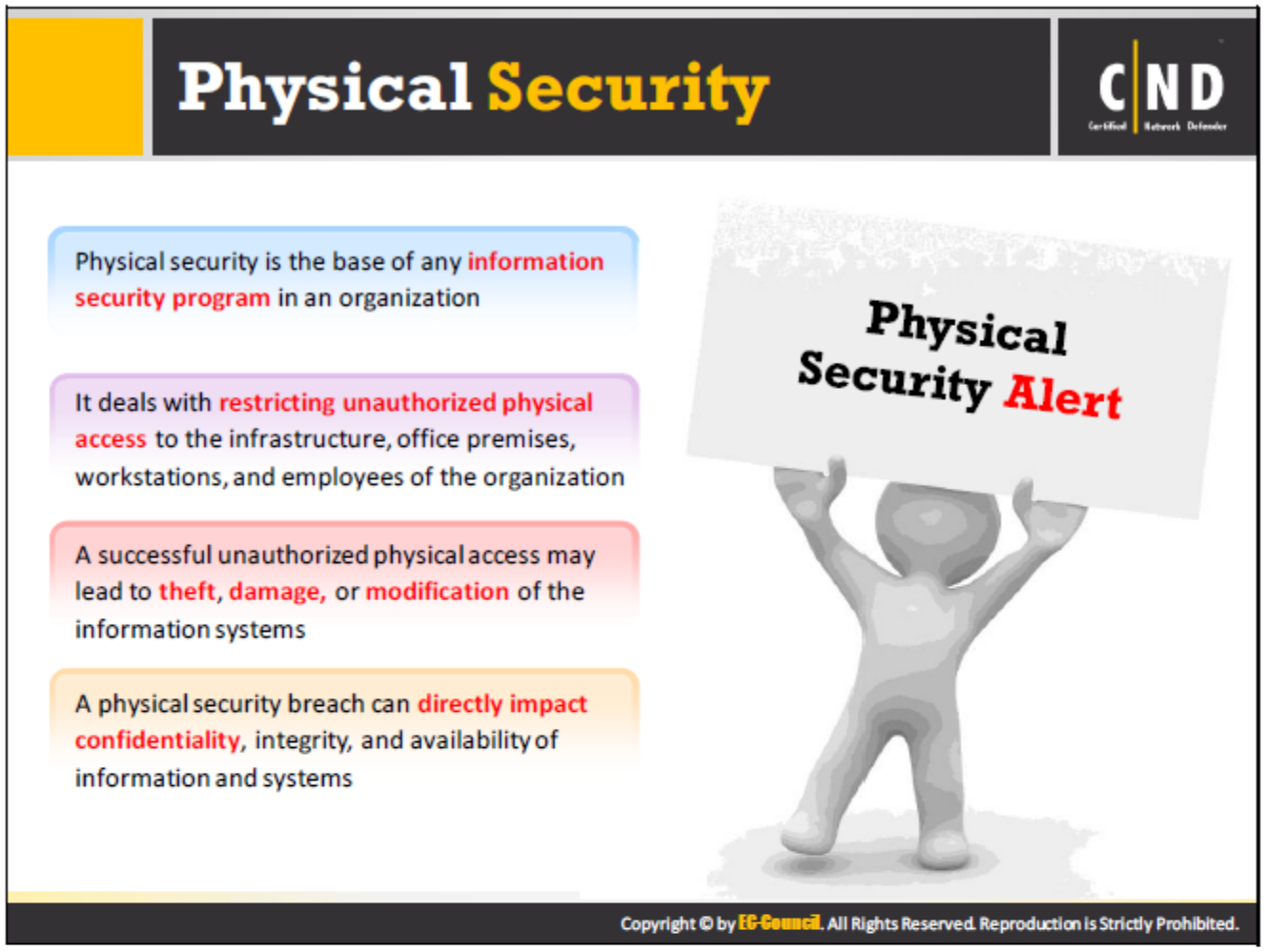
After network policy design and implementation, the next step is the physical security of the network and its equipment. According to John Canavan, the first rule of security is to physically safeguard the systems and networks. Organizations should consider placing appropriate physical security controls to deal with unauthorized physical access, personal security threats, and environmental threats. The administrator should ensure that all the physical security measures are in place and working properly in order to keep the organization away from physical security threats.

As stated in the HIPAA Security Rule, physical safeguards are "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."



Physical Security deals with the security of physical devices, personnel, networks and data from attacks. Any damage to the physical devices or the data may lead to the loss of information and increased cost to the organization. The security of the data, networks and devices, includes protection from environmental and man-made threats. Organizations need to use appropriate preventive measures to ensure physical security. The organization should consider all the ways which may affect the physical security of their infrastructure and information systems.

This module discusses the various physical security controls, security measures, and best practices to deal with physical security threats. It also helps you choose the best possible physical security solution depending upon your organization's need. With this module, you will be able to design a more robust physical security environment for your organization.



Physical security is an important part of the organization's information security program. In the past, people would relate physical security with keys, locks, security personnel, gates, fencing, etc. Now, the physical security paradigm has completely changed. Organizations need to manage manpower, property and assets. It has become a critical task for organizations to manage physical security of these assets. Everything such as planning the building layout, purchase of equipment, manpower recruitment, natural disasters, power supply, temperature control, etc., are all needs to consider while designing physical security for an organization. Every organization, whether it is a small, medium, large or multinational company gives utmost importance to the security of information assets. Implementing security at each level has become the primary function of an organization.

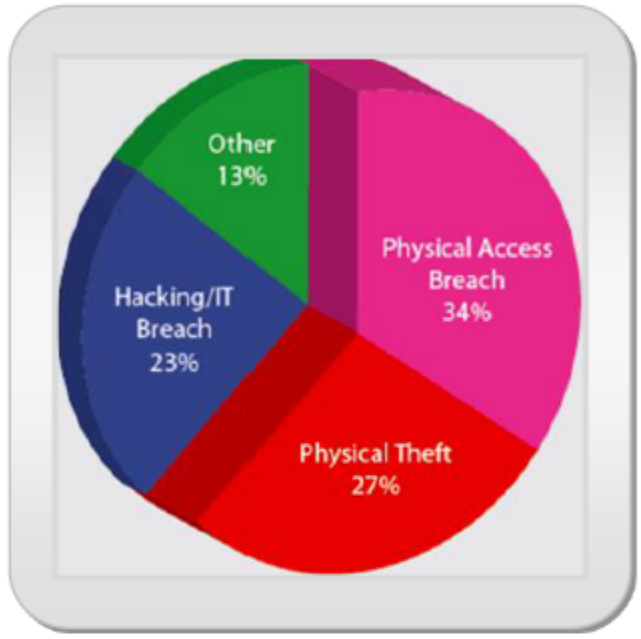
Physical security refers to protecting an organization's building and assets including software and hardware from robbery, vandalism, natural disasters, climate changes, environmental conditions, and man-made threats. Having strong multileveled security at appropriate places will provide effective protection against a physical security breach. The first level of security should effectively deal with external vehicles and control traffic outside the premises of the organization. It should restrict outsiders or intruders from entering the premises without permission thereby minimizing the security risk to a great extent in the first level. The next level of protection should control the vehicles, people and other-related organizational assets from internal and external entities. This level keeps the power supply system in a secure location with appropriate measures such as fire extinguishers, backup systems, etc. The main building will be separated from the parking lot; well-equipped plumbing system should be in place with

proper ventilation, alarm system, etc. The next level is the most crucial part of physical security where managing access of insiders (employees) and outsiders comes into light. At this level if an attacker gains access to physical assets, they can acquire sensitive information related to an organization.

Need for Physical Security

C|ND Certified Network Defender

Physical breaches accounted for 61% of all HIPPA Violations for 2015

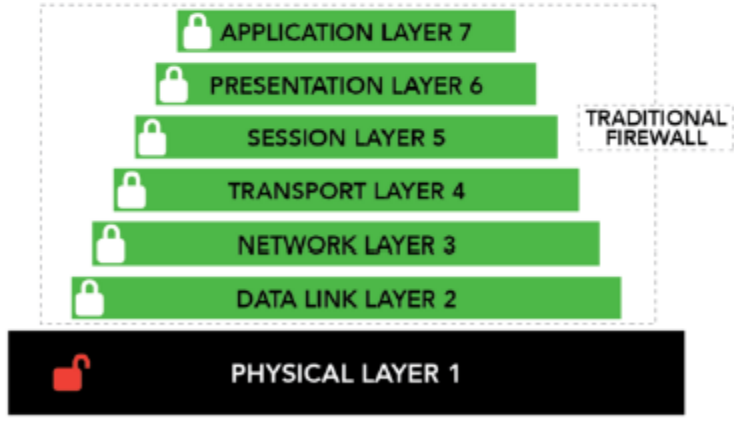


http://www.alphaguardian.ne

Need for Physical Security (Cont'd)

C|ND Certified Network Defender

THE PHYSICAL LAYER OF YOUR NETWORK
IS NOT PROTECTED BY TRADITIONAL FIREWALLS



THE 7 LAYERS OF OSI

http://www.alphaguardian.net

Although cyber-attacks are becoming more complex, attackers are continuing to use various techniques to compromise the physical security of an organization. Organizations are focusing more on strengthening their IT security which overshadows the importance of physical security. Physical security is the most-overlooked aspect of security and it has been brought to the forefront of many organizations over the last five years. Knowing this fact, attackers are taking advantage of loopholes to compromise the physical security of the organization. According to data collected by the US Dept. of Health and Human Services Breach Portal, it has been found that physical security breaches are among the most occurring security incidents in organizations in 2015.

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 concerning the possibility of both an act of terrorism and a security incident such as vandalism, theft or fraud disrupting their organization at some point.

"Physical security poses growing concern for organisations" observes latest BCI Horizon Scan

Posted On 24 Feb 2016 By : Brian Sims

Physical security is now perceived as a growing concern for business continuity professionals. That's according to the findings of the fifth annual Horizon Scan Report published by the Business Continuity Institute in association with the British Standards Institution (BSI).

Among the ranks of potential threats that today's organisations face, acts of terrorism gained six places, rising from tenth in 2015 to fourth, while security incidents moved from sixth place to fifth.

Some 55% of respondents to the global BCI survey expressed a degree of concern about the possibility of both an act of terrorism or a security incident such as vandalism, theft or fraud disrupting their organisation at some point. That compares with 42% and 48% respectively for the previous year's study.

FIGURE 5.1: Fifth annual Horizon Business Continuity Institute (BCI)

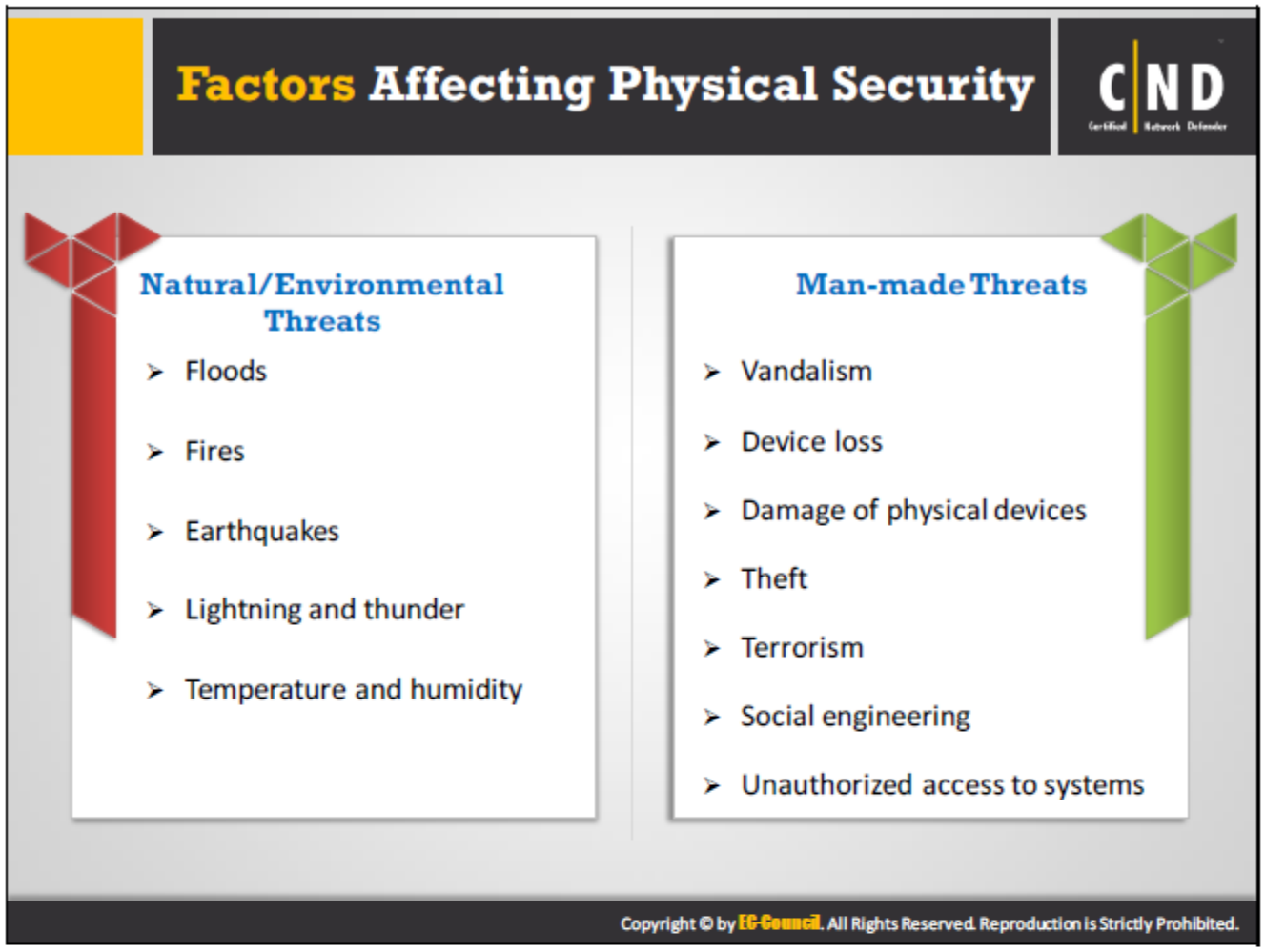
Physical security breaches are totally different than other security breaches. They can be carried out with little to no technical knowledge. The real physical security concerns arise when traditional security measures such as a firewall, IDS, etc., does not ensure physical security. Deploying a firewall at various levels ensures security from different types of attacks but it does not hold true with the physical security of the organization. The firewall has nothing to do with physical security as traditional firewalls work above the physical layer of the OSI model.

Physical security cannot be dealt with in the same way as network, application, or database security. Separate security measures are required to ensure physical security. Physical security should be dealt with at the physical layer of the OSI model.

- **A physical layer includes:**
  - All cabling and network systems.
  - Physical access to cables and systems.

- Power support for cables and systems.
- Environment supporting the systems.

Source: *http://thepaper.uk.com*



Organizations are at risk with the following types of physical security threats:

Natural/Environmental Threats

- **Floods:** Floods commonly occur due to heavy rains or the melting of ice. Heavy rains increase the level of water beyond the carrying capacity of a river and this results in a flood. Floods may affect electrical systems and server rooms in an organization. Server rooms located in the basement have a greater chance of getting affected by floods.
- **Fires:** Fires mainly occur due to short circuits or poor building materials. These may affect the operational facility and computer rooms in an organization. Fires can completely 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. 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 in the cabling system affects the working of the computer systems.
- **Lightning and Thunder**: Lighting and thunder occur due to 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 the system. It may affect memory chips and other hardware components of the system. It may lead to a short circuit in the cabling and other wiring systems, if they are not covered properly. The

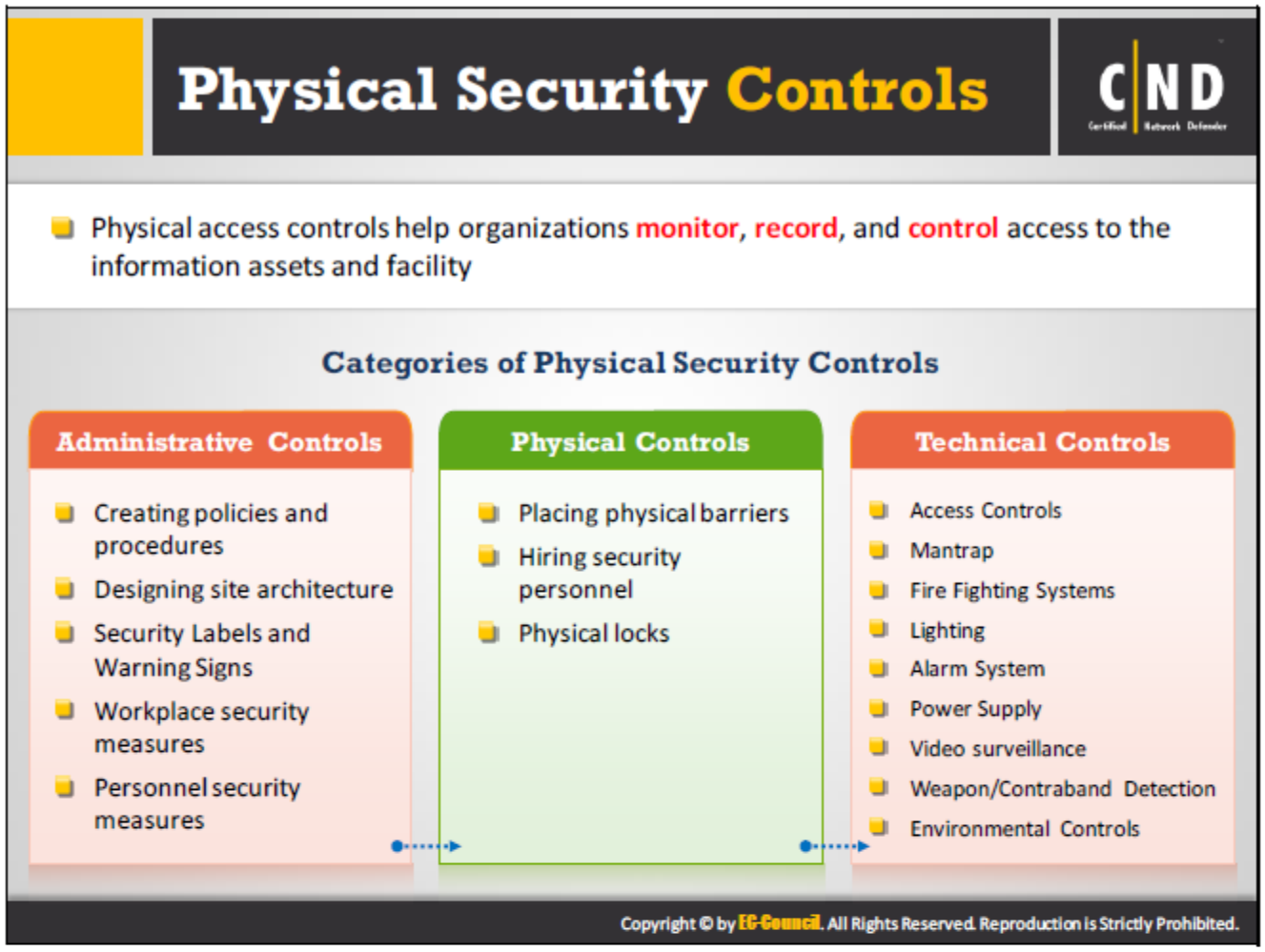
information system may stop working with one strike. Lightning may damage all electrical and electronic appliances and lead to the loss of all sensitive information.

- **Temperature and Humidity**: Computer systems operate between a range of temperatures, otherwise they will function in an inappropriate manner. Computer systems do not like hot areas. Computer systems may get damaged if the temperature rises or lowers by extreme amounts. Even though every computer system has cooling systems, performance of a computer still depends on the exterior temperature conditions. Electrical and electronic appliances in an organization may be affected by the change in the humidity. High humidity leads to issues like Corrosion, short-circuits and damages the magnetic tapes, optical storage media. Low humidity affects the electronic devices mainly due to electric discharge.

Man-made Threats

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

- **Vandalism**: Disgruntled employees or former employees may try to compromise the system by willingly breaking or harming the system components. During civil unrest or a disaster, there is a chance of the systems being mishandled.
- **Device Loss**: Unauthorized access may give way to the loss of important information and devices. Device theft is a concern if not properly secured.
- **Damage of Physical Devices:** Improper device maintenance activities such as how the device is handled or the information, not replacing damaged devices, poor cabling can damage the physical devices to great extent.
- **Theft:** Lack of proper security and locks may result in equipment theft.
- **Terrorism:** Terrorism activities such as planting a vehicle bomb, human bomb, postal bomb in and around the organization's premises, will impact physical security in many ways.
- **Social Engineering:** Social engineering is defined as an illegal act of getting personal information from other people. The attacker gains unauthorized physical access by performing social engineering on an organization's employees.
- **Unauthorized access to systems**: Both internal users and external users can try to gain unauthorized access to a system or information about the organization.



Without proper security controls, it becomes quite difficult to have any physical security at all. Physical security controls should be applied at various levels in order to create a robust physical security environment. Based on the level at which the physical security controls are applied, they are classified as:

Administrative Control

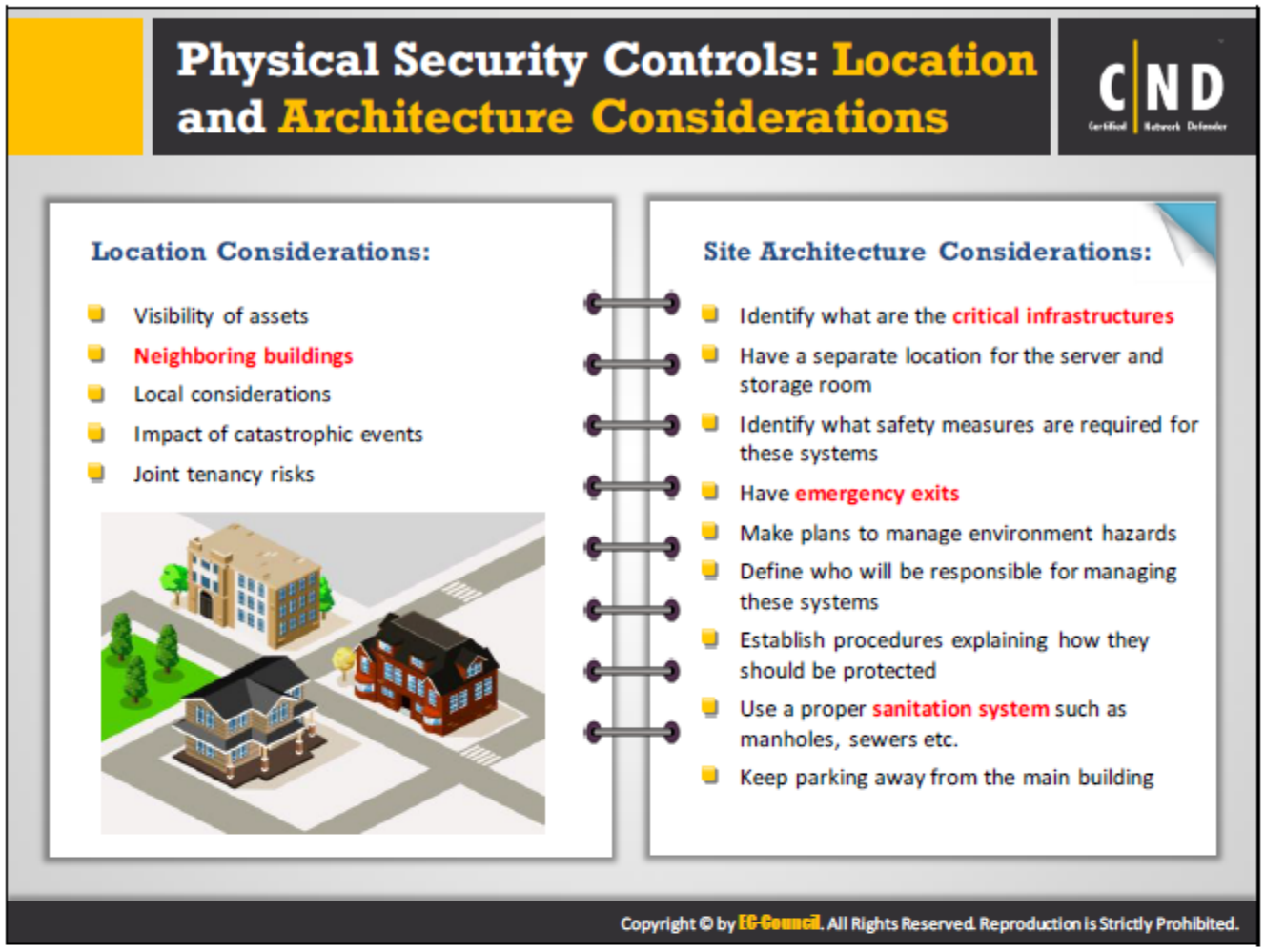
It includes the human factors for security controls. All levels of personnel should be involved in building administrative controls. It is based on the resources and information each user has access to. It involves management constraints, operational procedures, accountability procedures, and acceptable level of protection for the information system. It is basically a personnel-oriented technique implemented to control people's behavior.

Physical Control

Physical control deals with the prevention of damage to the physical systems in an organization. It involves deterring or preventing unauthorized access to devices, the facility or other sensitive areas. In addition, physical security controls are required to deal with physical threats such as device loss/ theft, and destruction or damage by accident, fire, or natural disaster.

Technical Control

Technical control is referred to as logical controls. It makes use of technology to control access to the physical assets or the facility of the organization. It is generally incorporated in the computer hardware, software, operations or applications to control access to sensitive areas.



Location Considerations

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

Site Architecture Considerations

After gaining adequate information about the facility location details, planning and designing of the internal infrastructure and architecture should be done. 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 your 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 and visibility of assets from outsiders
- Think about the joint tenancy factor, if the facility is shared with other companies and their impact on your 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.

These critical infrastructure systems may not use standard information technology [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.

Physical Security Controls: 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 is a risk that can occur with or without any warnings usually from man-made errors, short circuits, defective and faulty equipment. Fire protection is an important aspect of physical security. Firefighting systems mainly deal with detecting and alerting the occupants to the fire incidents. Fire incidents may be identified either manually or automatically.

Different types of firefighting systems include:

Active Fire Protection

Active fire protection provides an alert to 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 in order to protect the storage vessels, processing plant, etc. The main aim of implementing an active fire protection system includes controlling the spread of fire and extinguishing it as soon as possible, thereby facilitating the clearance of occupants in an organization. The system requires a certain amount of actions to handle the 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 the fire and fire extinguishers help put the fire out. Water sprinklers fall under the category of automatic fire protection systems, whereas fire extinguishers and stand pipes fall under the category of manual fire protection systems.

Active fire protection systems include:

- **Fire Detection System:** Fire detection system helps detect a fire incident before letting the fire spread.

  Automatic fire detection systems include:

  - **Smoke Detectors:** Smoke detectors generally detect the presence of smoke and send an alert about the suspected fire incident in an organization. Upon detection of smoke, detectors send out an alarm to the fire alarm control panel or generate an audio/visual alarm.
  - **Flame Detectors:** Flame detectors mainly deal with the detection of flames in a fire incident. Flame detectors normally include sensors which detect the existence of flames. The working of a flame detector includes:
    - Generate an alarm on fire flame detection.
    - Cutting the supply of gas through the fuel line.
    - Activate the fire suppression system.

    Flame detectors work more efficiently and faster than a smoke detector and a heat detector.
  - **Heat Detectors:** Heat detectors are used to detect and respond to thermal energy generated due to 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 quench the fire without much human interaction. Fire suppression systems regulate the destruction and device loss. A fire suppression system can be classified as: manual and automatic. Commonly used fire suppression systems include:

  - **Fire Extinguisher:** Fire extinguishers deal with extinguishing fires at the initial stage. These may not be used in 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 in order to ensure they are working properly in case of fire. Fire extinguishers are usually inspected yearly or bi-yearly by a trained professional. They can also be recharged.

    Dry chemicals, water, wet chemical, water additives, clean agents and carbon-dioxide are used as agents in fire extinguisher systems. The following table provides details about 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		

FIGURE 5.2: Classification for fire extinguishers

- **Standpipe System:** Standpipe systems deal with the connection of hose lines to the water supply. This provides a pre-piped water system for organizations and provides water supply to hose lines in certain locations. Three types of standpipe systems include: Class I – A, Class II – A, Class III – A. These types differ in accordance with the thickness of the hose lines used and the volume of water that is used for fire suppression.
- **Sprinkler System:** Fire sprinkler system maintains a water supply system in order to supply water to a water distribution piping system that controls the sprinklers. Sprinklers are used in order to avoid human and asset loss. These are mainly used in areas where fire fighters are not able to reach with their hose lines.

Passive Fire Protection

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

- Passive fire protection is put into practice in the following ways:
  - Minimal use of flammable materials.
  - Building additional floors and rooms in a building slowing down the spread of the fire.
  - Providing adequate training to the occupants regarding the procedures to follow when a fire occurs.
  - Proper maintenance of fire related systems.
  - Adequate amount of emergency exits.
- Steps to deal with fire incidents:
  - Detect fire.
  - Evacuate occupants in the building to another safe location.
  - Notify the fire department and safety department regarding the fire.
  - Close down all electrical and electronic systems in order to avoid the fire spreading.

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

Types of Physical Barriers used in a building are:

- **Fences/ Electric Fences/ Metal Rails:** It's a first line of defense that stops a trespasser and most commonly used across the globe. Fences/metal rails/electric fences generally mark the restricted areas, controlled areas and prevents unauthorized access.

  The aim of deploying physical barriers is:

  - Blocks and deters attackers.
  - Marks the boundary of the organization.

- Protects the security guards from external attacks.
- Prevents the entry of vehicles.
- Protection against explosive attacks.

FIGURE 5.3: Metal Rails

- **Bollards:** A bollard may be defined as a short vertical post which controls and restricts motor vehicles to the 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 5.4: Bollards

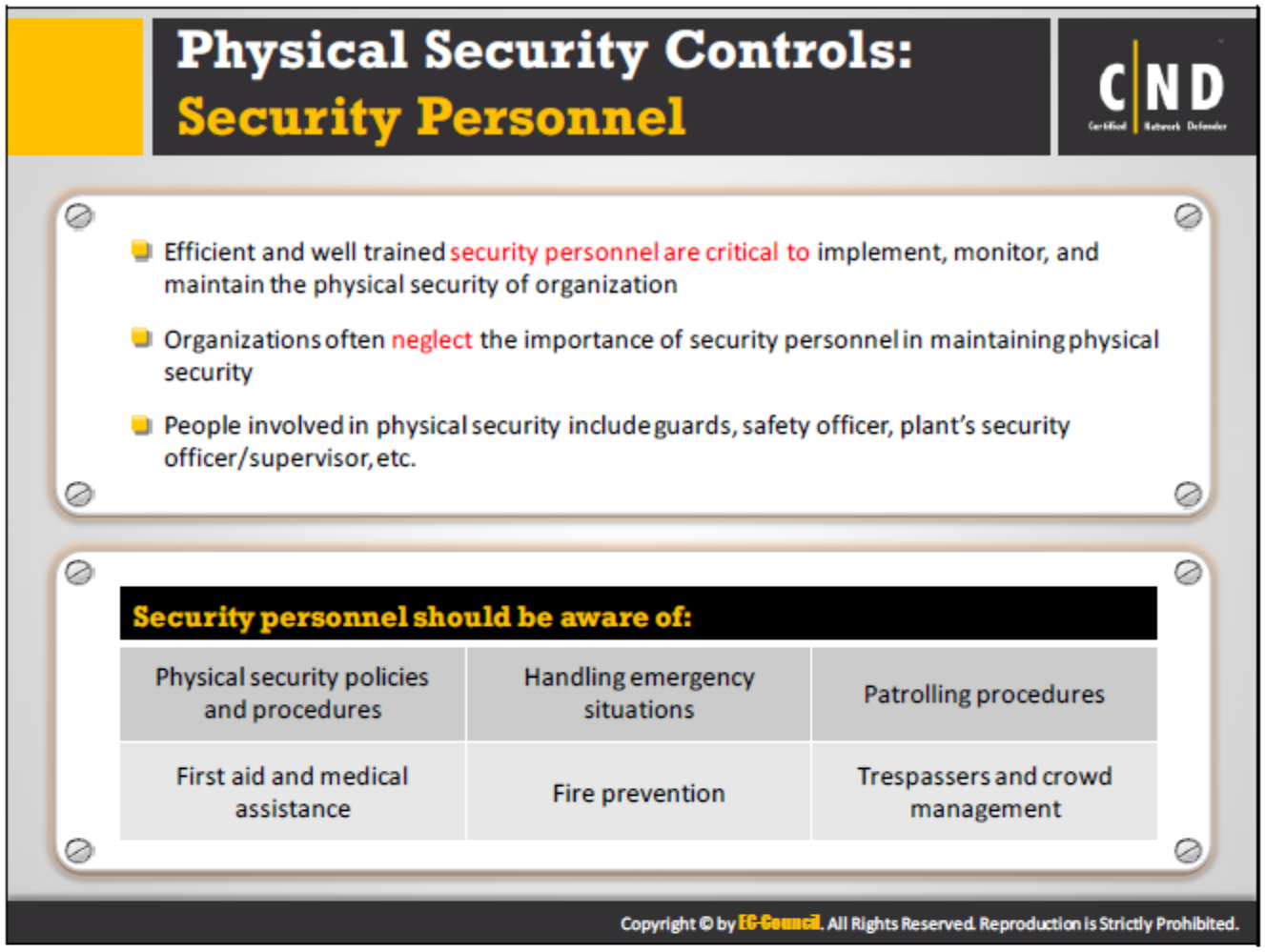
- **Turnstiles:** This type of physical barrier allows entry to only one person at a time. Entry may be achieved only by the insertion of a coin, ticket or a pass. It allows the security personnel to closely watch the people entering the organization and stop any suspicious persons at the gate. However,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

FIGURE 5.5: Turnstiles

- **Other Barriers:** It includes installing doors, windows, grills, glass, curtains to limit the access to certain area.
  - **Doors:** It can be used as a good source in controlling 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:
    - Method of opening the window.
    - Assembling and construction of window.
    - Technique used in locking the window.
    - Hinges used for the window.
  - **Grills:** Grills should be used with doors and windows for better security. Grills may be used for internal as well as external security.
  - **Glass:** Sliding glass doors, sliding glass windows provide a better level of physical security.

FIGURE 5.6: 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 inner building.
  - Lock doors and windows.
  - Use electric security fences to detect climbing and cutting of wires.
  - Use alarms to alert any intrusions from the fences.



Security personnel/guards are hired to implement, monitor and maintain the physical security of an organization. They are individuals who are responsible for developing, evaluating, and implementing security functions such as installing 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. Organizations are not considering them as a core competency that they want to invest in as part of their strategic plan.

Organizations should hire security personnel by themselves and provide adequate training on physical security or they can contact dedicated physical security service firms who handle physical security for them. There are organizations that are dedicated to training security officers, provide standardized procedures, and manage the security on a 24x7x365 schedule, by sharing guards across different organizations.

People involved in Physical Security are:

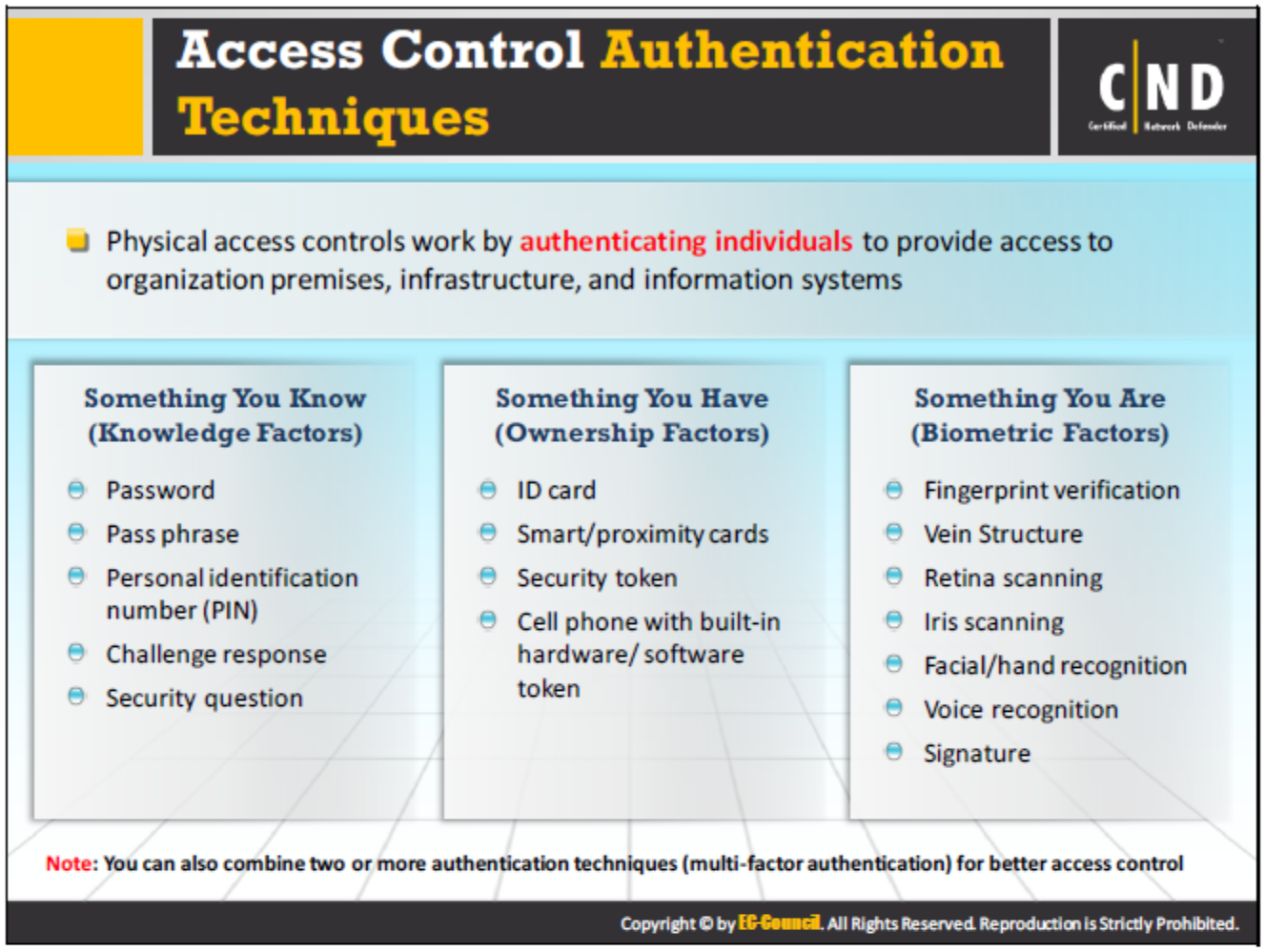
- **Guards**: Their responsibilities include screening visitors and employees at the main gates or entrance, documenting names and other details about the visitor, conducting regular patrols in the premises, inspecting packages, luggage, and vehicles, managing vehicle traffic, guiding visitors to the reception area after noting their details, etc. Guards should maintain visitor logs and record entry and exit information. (CCTV) to act as a deterrent as well as provide a mechanism to detect and possibly prevent an intrusion is normally handled by guards.

- **The plant's security officers/supervisors**: Their responsibilities include training and monitoring activities of the guards, assisting guards during crisis situations, handling crowds, and maintaining 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 proper functioning of this equipment.
- **Chief Information Security Officer (CISO)**: In the past, it was common place for the CISO of an organization to be an extremely technically competent individual who has held various positions within an enterprise security function or may even have come from 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 in order to successfully dispatch their duties and establish the appropriate level of security and security investment for their organization.

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

An organization should train newly hired security personnel on following areas:

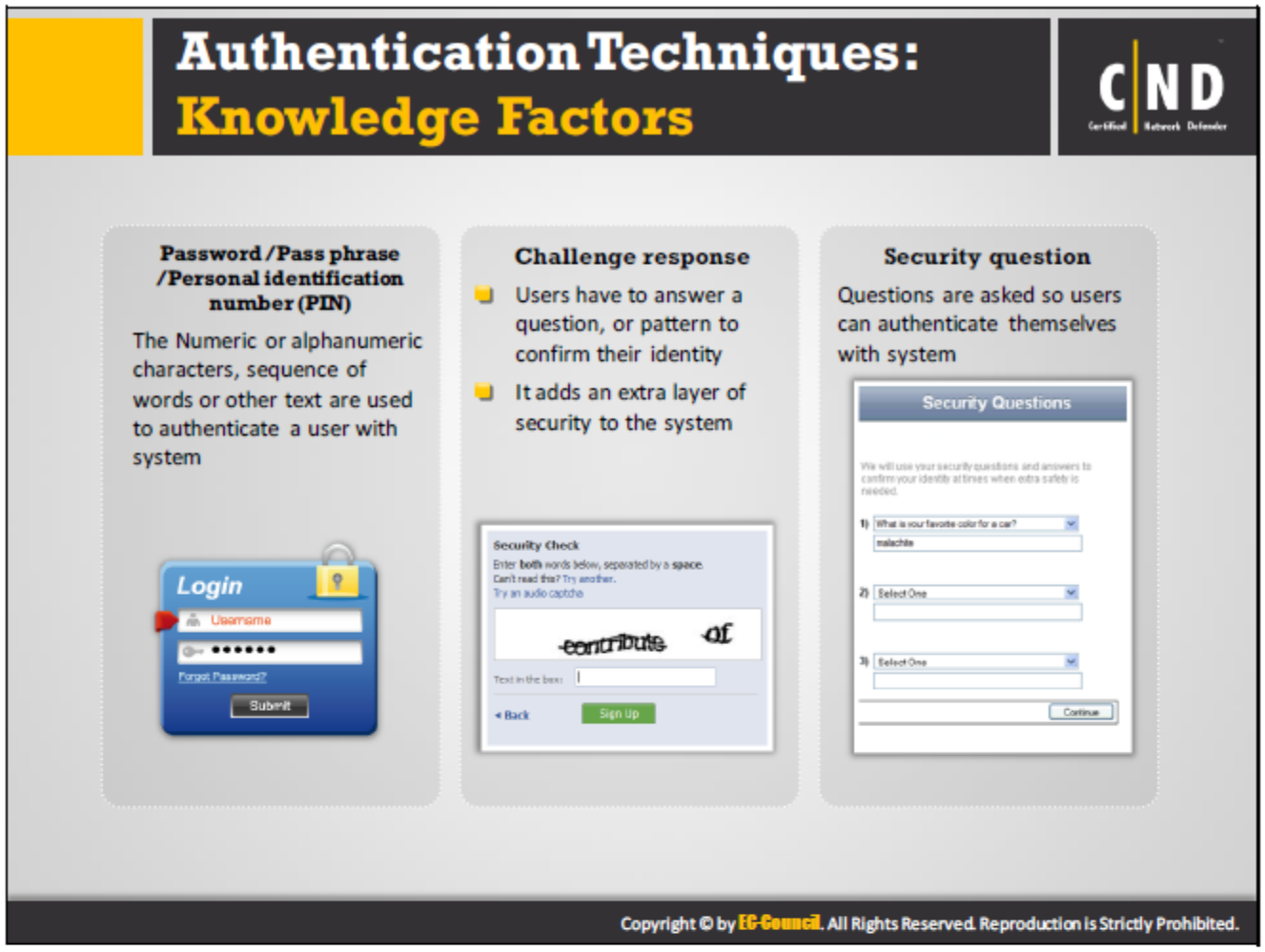
- Organizational culture, ethics and professionalism.
- Security policies and procedures.
- Policy enforcement.
- Trespassers and crowd management.
- Handling emergency situations.
- Human and public relations.
- Patrolling procedures.
- Managing workplace violence.
- First aid and medical assistance.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



Access control restricts the unauthorized access of the properties of an organization. The access control mechanism uses various types of authentication to verify the user's identity with the system.

The different types of access control authentication schemes are:

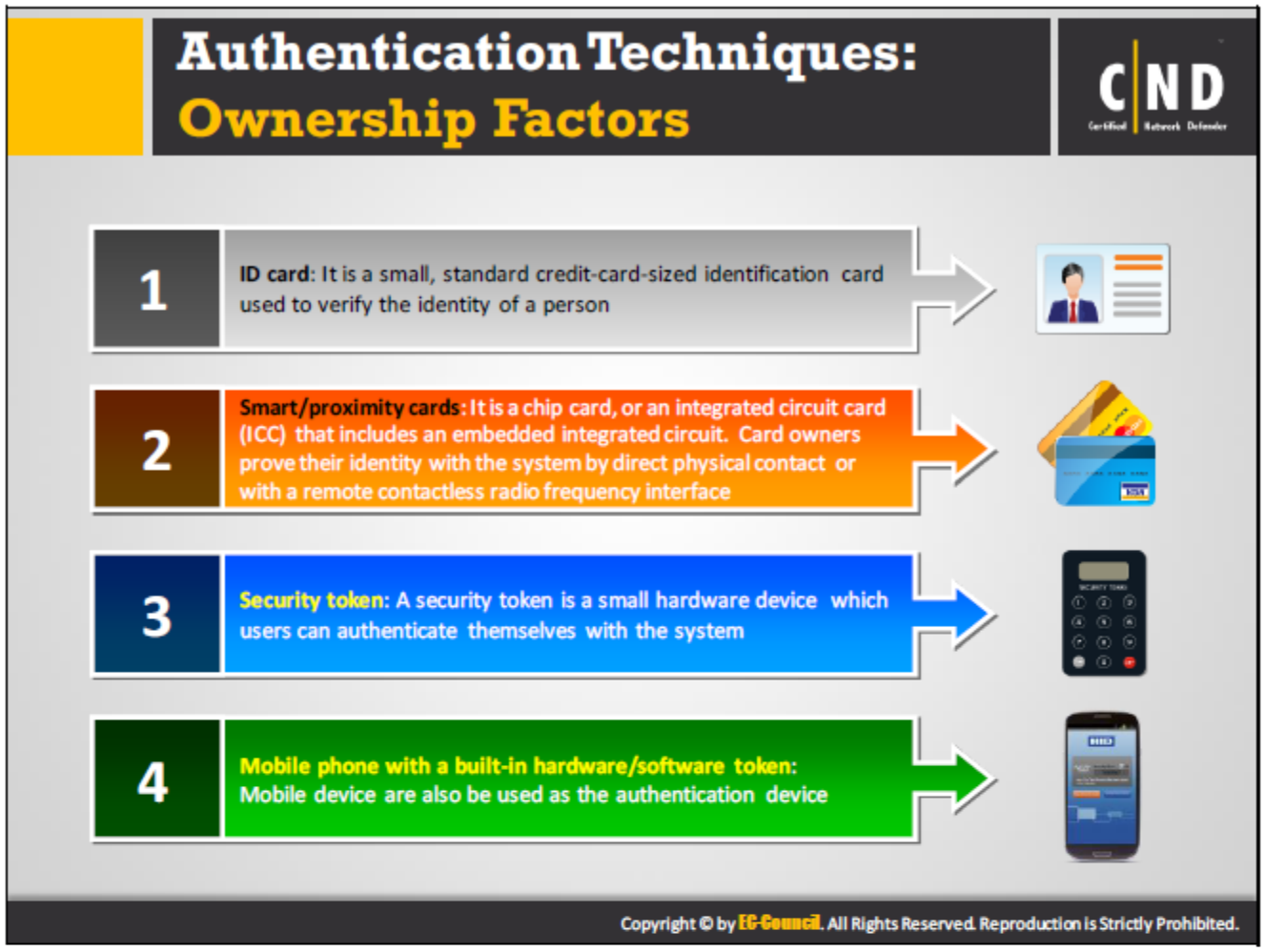
- **Knowledge Factors:** Authentication with the system is done with knowledge factors. Users have to prove knowledge of a secret they hold to authenticate themselves with the system. The user may hold secret knowledge, such as a unique password, pass phrase, personal identification number (PIN), challenge response, security question, etc.
- **Ownership Factors:** Ownership factors may also be described as "Something You Have". Authentication with the system is done with these possession factors. Users have to prove their identity with the system by using the physical devices such as an ID card, Smart/proximity cards, Security token, mobile phone with a built-in hardware/software token, etc. The users possess these physical devices to authenticate themselves with the system. It is always recommended that a 2-factor authentication be used with physical devices in order to add an extra layer of security.
- **Inherence Factors:** Authentication with the system is done with inherence factors. Users prove their identity with the help of biometric data that they hold. Biometric data depends on the behavioral and psychological characteristics of the user. The Biometric authentication scheme may include fingerprint verification, vein structure, retina scanning, iris scans, facial/hand recognition, voice recognition, signature, etc.



Passwords, passphrases or PIN based authentication offers an easy way of authenticating users. Users have to supply their unique password, passphrase or PIN to authenticate with the system.

- **Passwords**: Passwords generally contain a combination of letters and numbers. Users created their password at the time of their first login with the system. Organizations should enforce a strong password creation policy.
- **Passphrase:** Passphrase is similar to a password, but is generally longer for added security. It is generally used with cryptographic programs and systems. The user supplies a passphrase as an encryption key to these cryptographic programs and systems.
- **Personal Identification Number (PIN)**: A numerical password provided in order to authenticate a user with system. The PIN is generally used for authentication while using an ATM card. PIN lengths can be a maximum of 12 characters long.
- **Challenge Response**: A question and answer type authentication where the system throws a challenge to users and users have to provide a valid response in order to confirm their identity. One of the examples of the challenge response system is CAPTCHA. CAPTCHAs are distorted images with hidden letters. The user needs to retrieve the hidden letters and respond to it to confirm their identity. This kind of authentication system is used to ensure the input is human generated not computer generated.

- **Security Questions**: Security questions are used as an extra step for authentication. These are generally used by banks and wireless providers to reconfirm the identity of the user. Security questions are generally implemented with "forgot password" features which reconfirms or proves your identity.



ID Card

Identity document (ID card) can be used to authenticate users with the system. It includes ID cards such as a driver's license, photo ID card, passport, etc. Generally, an ID card is the same size as a credit card.

Smart Card

A smart card is a credit card-sized plastic device that contains a silicon computer chip and memory. It can store, process, and output data in a secure manner. It commonly stores cryptographic keys, digital certificates, identification credentials, and other information. It provides strong two-factor authentication using a PIN number. The International Organization for Standardizations (ISO) uses the term Integrated Circuit Card (ICC) instead of smart cards. The smart card has the dimension of 85.6 mm x 53.98 mm x 0.76 mm which is similar to ATM cards and credit cards. Smart cards can provide additional functionality such as credential storage.

- **Benefits of Smart Cards**: There are many benefits of smart cards such as:
  - **Lower Administrative Costs**: As there are fewer passwords in the network, the cost to support and manage the system decreases.
  - **Reduce Losses and Liabilities**: Security is increased as encryption and a strong two-factor authentication protects the data.

- **Increased Convenience**: Smart cards are portable and simple to use. The convenient factor for this system of authentication is high.

- **Smart Card Uses**: One of the important factors behind smart card use is the fact that multiple applications are involved. A smart card provides portable secure storage for the digital certificates. The smart card can also be used for many applications, such as:
  - Logon/logoff authentication of an operating system.
  - Authentication to website.
  - Sending/receiving of source email.
  - Encryption of data files.

Proximity Cards

A proximity card is also similar to a credit card. Several companies use proximity cards to control physical access. When using this card, the employee holds their card within a few inches from the reader. The card reader receives a unique ID from the card and transmits it to the central computer that tells the receiver whether or not to open the door.

Proximity cards are harder to duplicate and have more control when turning off access. Some systems combine the logical and physical access on the same card. Different techniques are used for card sensing like an integrated circuit which is embedded in the card to generate a code magnetically or electrostatically and circuits are embedded with the code that is tuned to varying resonant frequencies. It is a best practice to place the company's logo and address on the keycard so if it is lost or stolen, it can be returned.

Security Token

Security tokens are generally used for verifying the identity of a user by means of electronic devices. Users may store cryptographic keys like digital signatures, biometric data etc. as a security token. Tokens consist of secret information that verifies the identity of the user. The information may be stored using the following tokens:

- **Static Password Token**: Contains hidden information that is available during each authentication step
- **Synchronous Dynamic Password Token**: Uses a cryptographic algorithm that uses a synchronized clock between the token and the authentication server
- **Asynchronous Token**: Generates a one-time password using a cryptographic algorithm
- **Challenge Response Token**: Uses public key cryptography

Mobile phone with a built-in Hardware/Software Token

Mobile phone with built-in hardware/software tokens is a two-factor authentication security device that authenticates the services running on a computer device. Software tokens are placed on the devices and are easy to replicate. Hardware tokens are stored as credentials inside the hardware device and are unable to be replicated.

Fingerprinting

Fingerprint verification or scanning is a popular biometric authentication technology used for authenticating individuals. In the fingerprint verification, the entire fingerprint image of an individual is obtained and stored in a database. The identity of the user is confirmed by comparing the fingerprint with the stored image. If it matches, authentication becomes successful. Biometric fingerprint scanning systems do not store a full image of the fingerprint in a database. A small template created from the fingerprint is stored.

Fingerprint scanning devices come in different packages. For example: a stand-alone device for the desktop PC, to small portable devices for laptop computers, built-in keyboards and built-in mice.

Retinal Scanning

It is another method of biometric authentication where authentication is made based on a retinal scan of the individual. The retina is a part of the human eye and holds different characteristics for each person. Even identical twins have a different retinal pattern. The retina is a thin layer of nerves (about 1/50thof an inch, or a 0.5 mm thick) found on the back of the eye. As a part of the eye, the retina transmits impulses through the optic nerves to the brain. Retina scanning is difficult compared to other scans in biometric technology. To present the raw biometric data, users must move their head into position with their eye very close (less than an inch) to the scanner for it to read the retina through the pupil. During the scan process, the user

will focus on a green light in the scanner. After generating the template, it provides an excellent matching.

Iris Scanning

Each individual holds a unique iris pattern same as the retina. It can be different in structure such as ligaments, furrows, striation, ridges, and zigzags. Iridian technology measures 247 independent variables in an iris.

Iris scanning is a process of taking images of an iris and creating biometric templates used in matching functions. Similar to fingerprints, it also requires a device to capture the image and software to process the image. The iris scanning device uses a camera, which can be either a still or a video camera to capture the iris information. The camera captures a high-resolution image of the iris and then the device will locate the border between the pupil and the iris. The device will then convert the data to a grayscale image. This gray scale image identifies the unique feature of the iris.

Vein Structure Scanning

Vein structure scanning is also known as vascular biometrics and mainly depends on the patterns in a user's vein. The vein scanning technique focuses on authenticating a person's identity by checking the patterns of the vein structure. Veins are normally found under the skin and scanning requires the flow of blood in the veins.

Users need to place the palm, the back of the hand or the wrist on the scanner. The scanner takes a picture of the part placed on the scanner using infrared light. Hemoglobin absorbs infrared light and it highlights the veins in the picture. A reference template is created according to the shape and location of the vein structure.

Face or Hand Recognition

- **Facial Recognition**: Facial scanning or facial recognition is famous due to large-scale implementations that have taken place for surveillance purposes. It works by picking out the unique characteristics of a human face and matching these against facial images in a database. These are the facial characteristics that a face scanning system looks for:
  - Size of eyes
  - Distance between the eyes
  - Depth of the eye sockets
  - Location of the nose
  - Size of the nose
  - Location of the chin
  - Size of the chin
  - Jaw line
  - Size, position, and shape of the cheekbone

The facial scanning process starts with the acquisition of an image of a human face. This image can be acquired by using any imaging source, static cameras or video cameras, both analog and digital. After capturing the isolated facial image, the system will create a face print of that image. The face print is the template for the system. This is the process of translating the facial image into unique code or a data set that can represent the facial image.

- **Hand Recognition:** Hand Recognition is a biometric technique used to identify a user by the shape of their hand. It is a simple and accurate procedure. The use of this technique requires special hardware and can integrate into any system or device. It uses finger width/height, thickness and shape for identification purposes. The user places the hand on a metal surface, which has a guidance page on it. The pages align the hand in a proper position so the device can read the hand attributes. The device then verifies the user details in its database.

Voice Recognition

Human voice scanning and recognition is another method of biometric authentication where a user's voice is recorded using voice recognition software and it performs a matching function to identify the individual. It is based on identifying a unique characteristic of the human voice. This system uses voice recognition software to allow users to interact with the computer by issuing commands verbally instead of using an input device, such as a mouse. Any microphone, landline telephone, cellular telephone, or any other device is used to capture the human voice.

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.

Different types of locks are:

- **Mechanical Locks**: 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**: Contains a spring loaded bolt attached to a notch. A key inserted into the notch moves the bolt backward and forward. Only the correct keys can be inserted into the notch and it blocks the wrong key.
  - **Tumbler Lock**: Consists of pieces of metal inside a slot in the bolt. This prevents the bolt from movement. A correct key contains grooves that allow the bolt to move by raising the metal pieces above the bolt. It is further classified into Pin Tumbler, Disk Tumbler and Lever Tumbler locks.
- **Digital Locks:** Digital locks use fingerprint, smart card or a PIN on the keypad to unlock. It is easy to handle and does not require keys, so there is no chance of forgetting or losing the keys. It provides automatic locking for doors. The user only has to use their fingerprint impression, swipe the smart card or enter the PIN to unlock it.

- **Electric/Electromagnetic Locks**: Electric locks or an electronic locking system operates on an electric current. Locking and unlocking is achieved by supplying and eliminating power. It mainly uses magnets or motors to activate or deactivate the locks. It does 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 consists of two types of status "Fail Safe" or "Fail Secure". Fail secure locks remain locked even during power loss, whereas Fail safe remains inactive when de-energized. The electromagnetic part may be placed on the door frame and the armature plate may be placed on the door. The magnetic flux created by the electromagnet gets attracted towards the armature plate and this initiates the door closing process.

- **Combination Locks:** It has a combination of numbers and letters. The user needs to provide the combination to open the lock. 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.

Contraband Detection Devices act as an important physical security control as it restricts activities and/or a person carrying contraband substances from entering the premises. Contraband substances are illegal materials such as explosives, bombs, weapons, etc., which should be banned from the premises. The person trying to enter into the office with contraband substances can be considered an act of terrorism. Contraband Detection Devices are able to detect substances, even though it is covered with other objects.

Different types of devices are used to detect contraband materials such as a handheld metal detector, walkthrough metal detector, X-ray inspection system, etc.

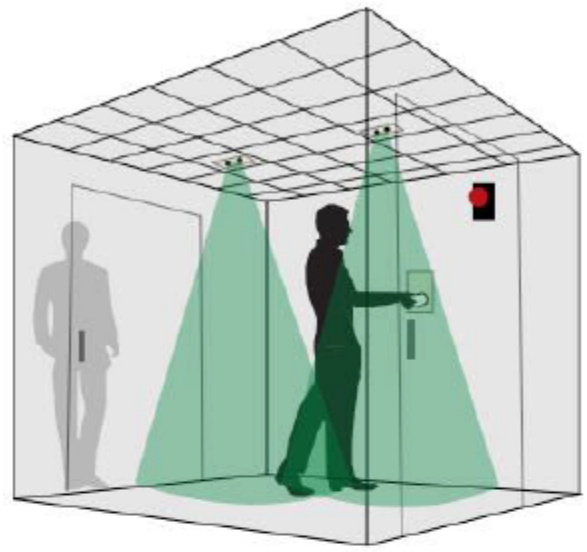
Walkthrough metal detectors are mainly used in airport terminals, schools, sports stadiums etc. These help check people who have admission to certain areas. The walk through detectors should be maintained and properly monitored. It should be deployed at each entry point of the organization.

Handheld metal detectors allow people to be screened more closely and to detect any suspected elements. Handheld detectors are used in all places where the walk through detectors are used.

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

Physical Security Controls: 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.
- It operates automatically, useful in authorizing visitors, reduces the manpower with using security systems and guarantees the safety of the organization



Mantrap is another type of physical access security control which 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 comprised 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/PIN or biometric verification. The closing and opening of doors is handled automatically or through security guards.

How Do Mantraps work?

- **Step 1:** Authenticates the person trying to access
- **Step 2:** The first door opens after authentication. The person walks in.
- **Step 3:** First door closes soon after the person enters the room. Now the person gets locked inside the room. This signals the second door to get unlocked.
- **Step 4:** The second door opens with the person walking out of the room. The first door gets automatically locked soon after the second door opens.
- **Step 5:** The second door gets into locked state soon after the person walks out the second door.

Physical Security Controls: Security Labels and Warning Signs

- Security labels are used to mark the security level requirements for the information assets and controls access to it
- Organizations use security labels to manage access clearance to their information assets
- Security label scheme:
  - Unclassified
  - Restricted
  - Confidential
  - Secret
  - Top Secret

- Warning signs are use to ensure someone does not inadvertently intrude in any restricted areas
- Appropriate warning signs should be placed at each access control point

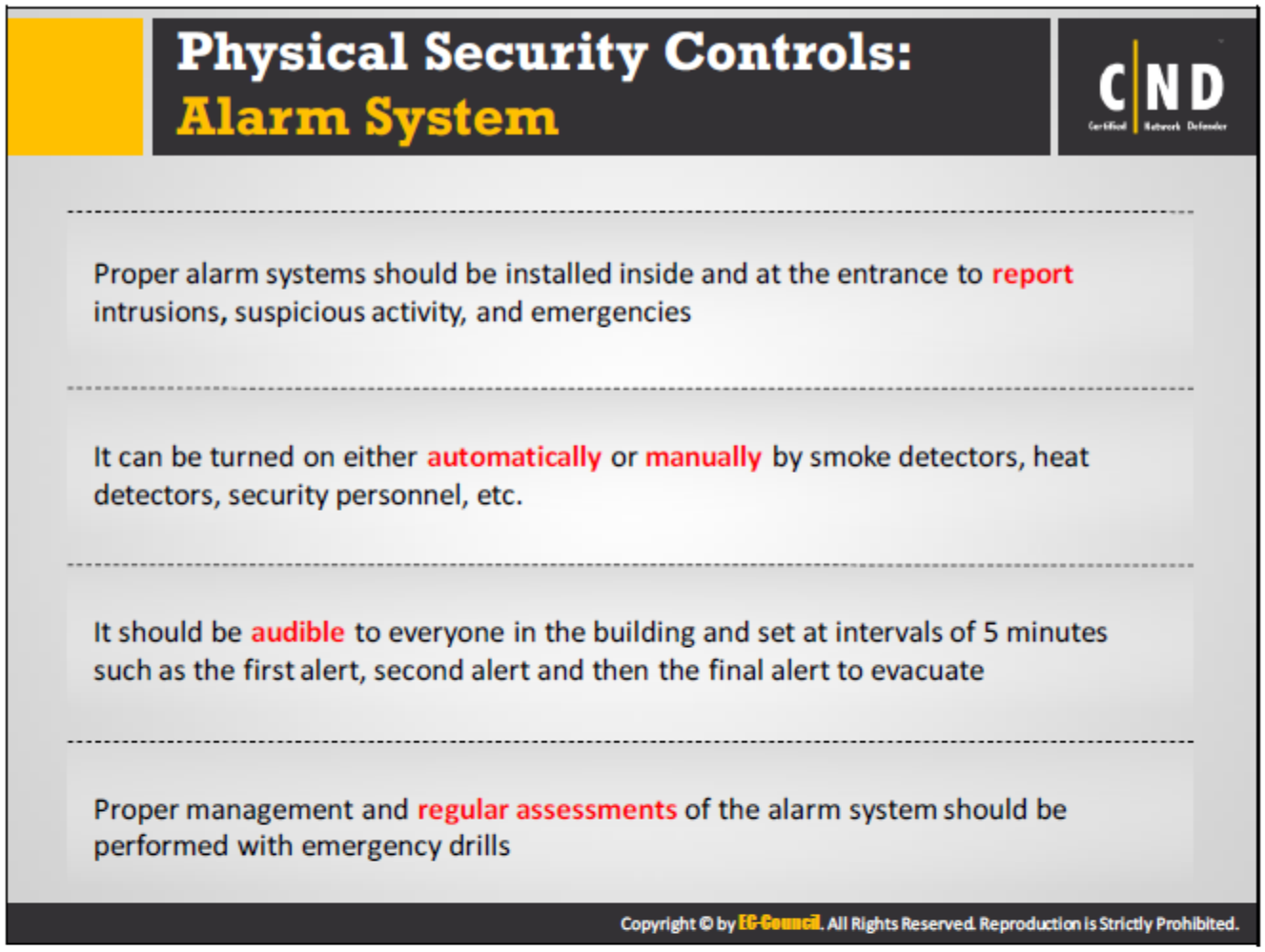
Security labels are used to restrict access to information in high and low security areas as a part of mandatory access control decisions. This enables easy understanding for users with and without permission to access and easy clearance of a large group of users. It defines the sensitivity of the data or the object and authorizations required for accessing the object or data. It provides a list of users who can access the document or the device and enables the user to understand the documents that they can access.

Security labels are categorized into different types based on who can access the data or object.

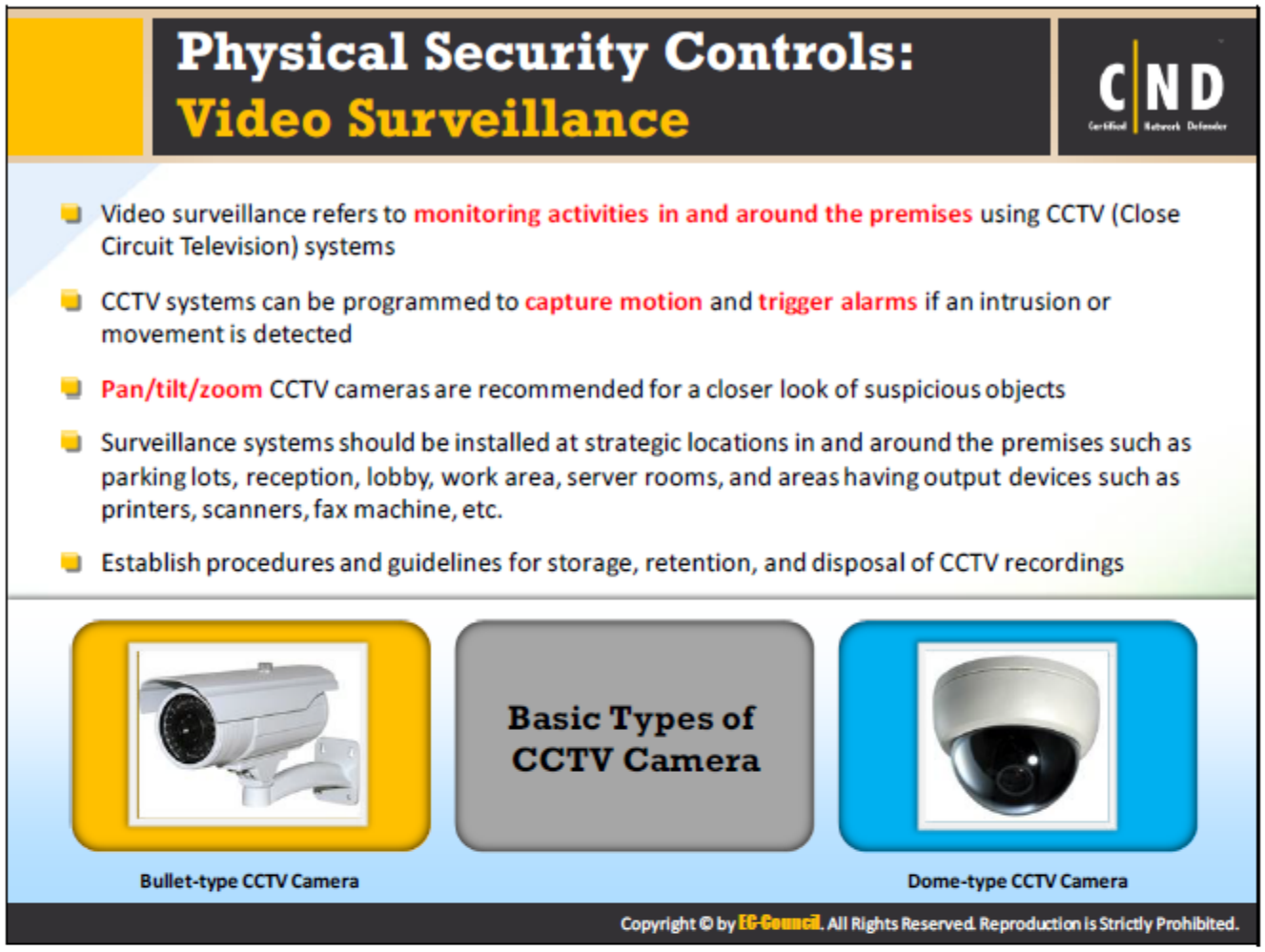
- **Unclassified**: No access permissions are required in order to access unclassified documents. Any person at any level may access these documents.
- **Restricted**: Only a few people can access the data or object. Sensitive data may be restricted for use in an organization due to its technical, business and personal issues.
- **Confidential**: Confidential data or objects exposed may lead to financial or legal issues in an organization. Documents may be highly confidential or just confidential. Revealing this data is irrespective of whether it is confidential or highly confidential, either will lead to the loss of critical information.
- **Secret**: Users authorized to access secret files may access secret, confidential, restricted and unclassified data. Users cannot access documents or objects labelled as top secret as it requires a higher clearance level.

- **Top Secret**: Users accessing top secret documents may access top secret, secret, confidential, restricted and unclassified data.

Warning signs are generally used in order to restrict any unauthorized access in an organization. Warning signs are kept at entrance points, boundaries of the locality and sensitive areas. Warning signs should be visible to users such that people will understand the prohibited areas where they should not enter. Warning signs also help organizations to clear a large amounts of people from entering into sensitive areas. Warning Signs are generally kept at all sensitive areas where there could be a threat of damaging and distrusting of information, assets, or life. For example, a typical use of warning is kept on an Electrical fence. It may pose a threat to life, when someone touches an electric fence unknowingly. Typical warning signs are RESTRICTED AREA, WARNING, CAUTION, DANGER, BEWARE, etc.



Alarms are used to draw attention when there is a breach or during an attempt of breach. Alarm sounds can be different types based on a facility such as sirens, flash lighting with a sound, email, and/or voice alerts. The organization should divide their large facilities such as buildings, floors, sections, and offices into small security zones and depending upon their significance, the appropriate alarm system should be placed. Security zones that store high priority data are given multilevel security, such as restricting access with access control devices, biometrics, surveillance, locks and alarms to draw attention in any event of intrusion. Organizations should have a proper power backup to alarm systems so that it will work in emergencies and also during a power shutdown. All wiring and components of an alarm should be protected from tampering and even conceal the alarm box with proper locks and limited access.



Video surveillance is considered as an important component of physical security. These systems protect an organization's assets and building from intruders, theft, etc. CCTV is used as part of the organization's security system. CCTV covers a large area and is often placed near gates, reception, hallways, and at the workplace. It captures illicit activities inside the premises and also helps monitor activities inside, outside and at the entrance. They are even programmed to capture motion and initiate an alarm whenever it detects a motion or an object. 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.

There are many things that need to be considered for installation, management and maintenance of a video surveillance system in an organization such as 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 what type of lens, resolution, and coverage area your camera should cover, along with recording the time and date of the video. Another important aspect is storing video recordings and for how long they will be stored. What will happen with the old video recordings and how will they be disposed?

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, fax machine, etc., in public view under surveillance.
- Integrate surveillance with an alarm system.
- Establish a procedure for the amount of time the recorded video should be kept and then later disposed.
- Store all devices in a secure location with limited access.
- Use proper disposal systems such as deleting contents, overwriting, and physical destruction.

Different types of CCTV cameras available are:

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

FIGURE 5.7: Dome CCTV

- **Bullet CCTV:** It is used for indoor and outdoor surveillance. These are generally placed in protective covers that prevent it from dust, rain or any other disturbances. Bullet CCTV is normally a long, cylindrical and tapered shape that facilitates for long distance surveillance.

FIGURE 5.8: Bullet CCTV

- **C-Mount CCTV Camera:** It consists of detachable lenses, which provide surveillance for more than 40.ft. Other CCTV camera lenses provide only 35 – 40 ft. coverage. C-Mount allows different lenses to be used according to the distance to be covered.

FIGURE 5.9: C-Mount CCTV Camera

- **Day/Night CCTV Camera:** It is commonly used for outdoor surveillance. It can capture images even during low light and darkness conditions. These types of camera do not require infrared illuminators in order to capture images. These can capture clear images during glare, direct sunlight, reflections etc.

FIGURE 5.10: Day/Night CCTV Camera

- **Infrared Night Vision CCTV Camera:** It is commonly used for outdoor surveillance and can capture images in complete darkness. You can use an infrared LED's for areas having poor lighting.

FIGURE 5.11: Infrared Night Vision CCTV Camera

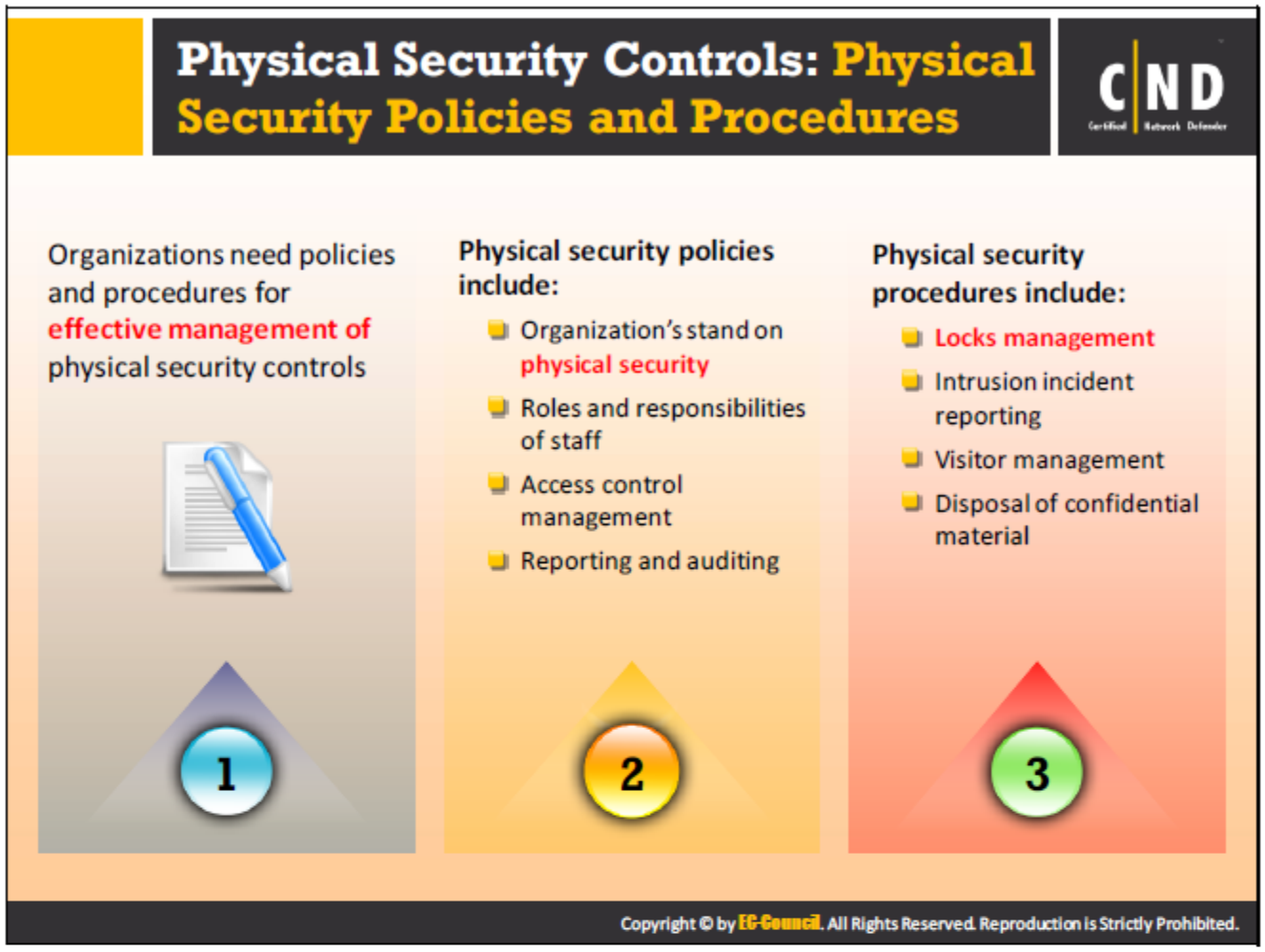
- **Network/IP CCTV Camera:** It consists of wired and wireless models. It allows sending images over the internet. It is easier to install a wireless IP camera than a wired camera as they do not require any cabling.

FIGURE 5.12: Network/IP CCTV Camera

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

FIGURE 5.13: Wireless CCTV Camera

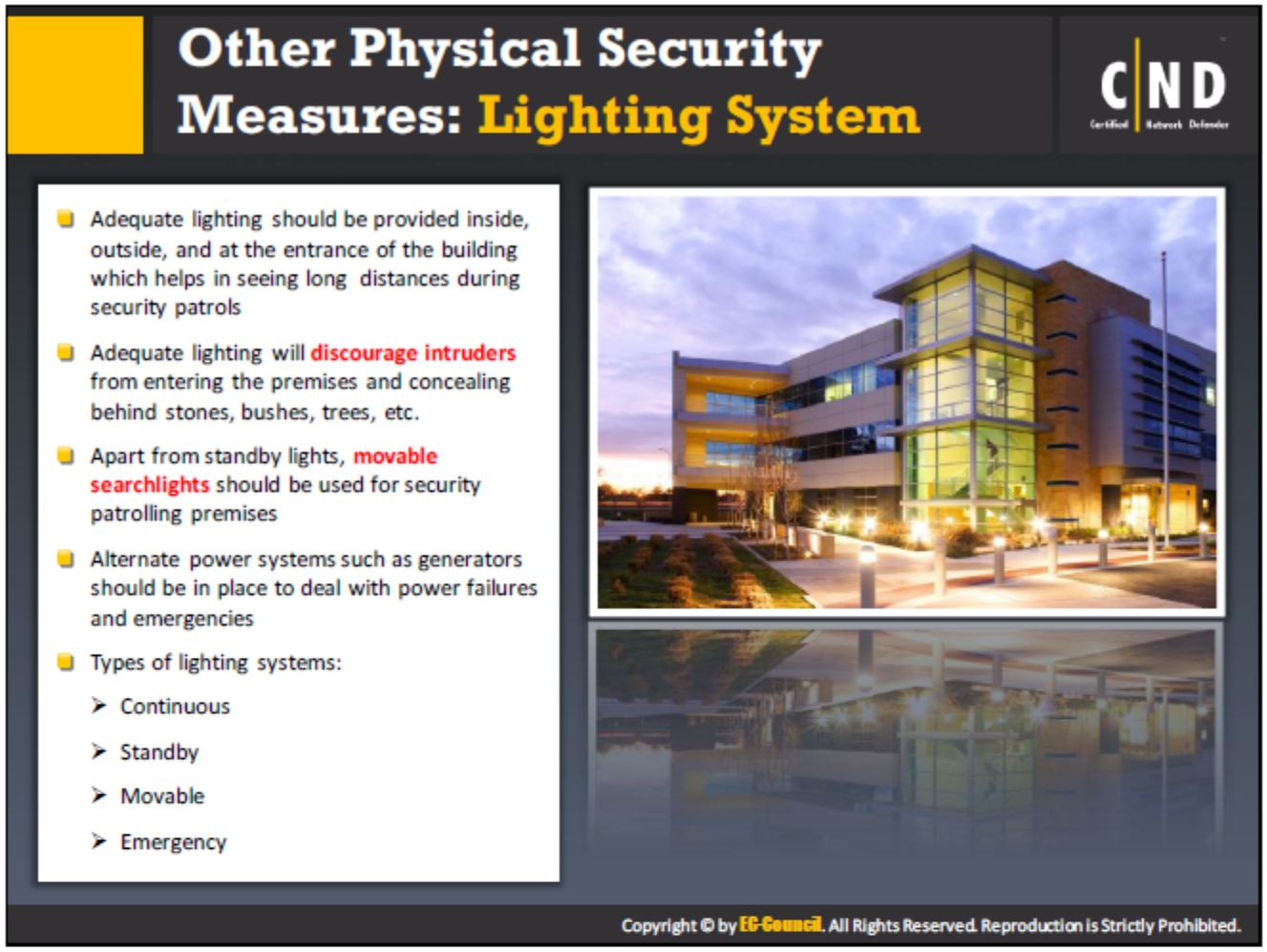
- **High-Definition HD CCTV Camera**: It is mainly used in sensitive locations that require more attention. It allows operators to zoom into a particular area.



Organizations should enforce required physical security policies and procedures for effective physical security management. Physical security policies may differ from one organization to another.

- Typical physical security policies may include:
  - **Organization's stand on Physical Security**: It defines an organization's scope of physical security such as what it wants to achieve with an effective security policy.
  - **Roles and Responsibilities of the Staff**: It explains the roles clearly and the responsibilities of every person associated with the facility. It also identifies how they should perform their duties in order to maintain the security posture of the organization.
  - **Access Control Management**: Organizations need physical security equipment and technologies in order to maintain the security posture. They need to focus on different types of devices and technologies that are required in order to provide adequate physical security.
  - **Reporting and Auditing**: Organizations need to have proper documentation, reporting and auditing mechanisms to archive for future reference.
- Physical Security procedures may include**:**
  - **Locks management**: It includes a procedure about the management of locks and alarms.

- **Intrusion incident reporting**: It includes steps and procedures to adopt when an event is found or has occurred.
- **Visitor management**: It includes basic procedures that define different types of visitors and how to manage new visitors, clients, stakeholders, new employees, etc.
- **Disposal of confidential material**: It includes confidential material procedures and how these should be disposed, using different techniques such as degaussing, physical destruction, and overwriting.



Security lighting is an important aspect of physical security of a facility. If the organization has not implemented an adequate lighting system in and around the organization, it can drastically degrade the function or performance of all other security measures. 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 will be difficult to identify people entering the premises, as an intruder may act as an employee or use tricks to circumvent the security. Lighting systems in a location depend on its layout and sensitivity.

- **Continuous Lighting**: Fixed sets of lights arranged so they provide continuous lighting to a large area throughout the night.
- **Standby Lighting**: Used whenever any suspicious activity is detected by security personnel or by an alarm system. These operate either manually or automatically.
- **Movable Lighting**: Manually controlled lighting system that provides a lighting system at night or only when needed. Normally used as an extension of a continuous or standby lighting system.
- **Emergency Lighting**: Used mainly during power failures or if other normal lighting systems do not operate properly.

Facilities may suffer blackouts or power outages that could make the systems inoperable unless appropriate alternative power management capabilities are kept in place. Power outages could impact the ability to provide information technology as expected and also in maintaining physical security. Power spikes, surges, or blackouts could result in too much or not enough power and could damage equipment.

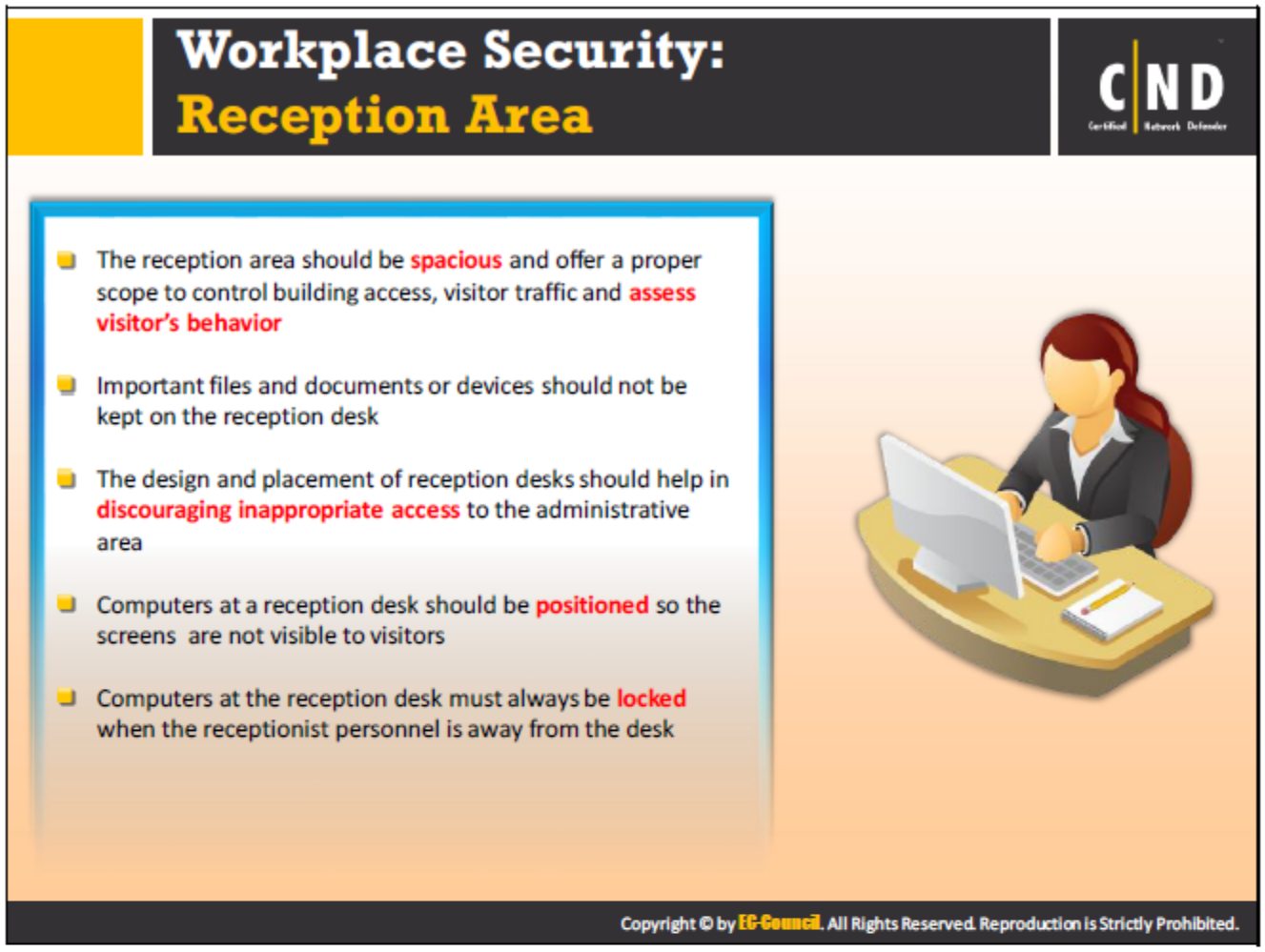
Consider the following security measures to deal with blackouts or power outages:

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

An Uninterruptible Power Supply (UPS) allows computers to function properly during a power failure. It protects the computers during fluctuations in the power supply as well. An UPS contains a battery that senses power fluctuations in the primary device. Users need to save all the data when the UPS senses the power fluctuation. The operator needs to provide measures which must be followed at the time of power loss. An UPS is commonly used to protect computers, data centers, telecommunication equipment etc.

Different types of UPS include:

- **Standby:** An offline battery backup facilitating the maintenance of the primary device from a power fluctuation. A standby power supply contains AC-DC circuitry that connects to the UPS during a power fluctuation.
- **Line Interactive:** Line interactive mainly deals with maintaining continuous power fluctuations. This method of a power supply needs very little battery usage.
- **Stand by On-line hybrid:** These are mainly used to supply power below 10k VA. It is connected to the battery during a power failure.
- **Stand by Ferro:** A Ferro resonant transformer is used for filtering the output. Stand by Ferro provides ample time for switching from main power to battery power.
- **Double conversion on-line:** It is used to supply power above 10k VA. It provides an ideal electric output presentation, and its constant wear on the power components reduces the dependability. It exhibits a transfer time only during a large load of current.
- **Delta conversion on-line:** It contains an inverter that supplies the load voltage. It is available in a range between 5k VA to 1 MW. It controls the power input performance and charging the UPS battery.



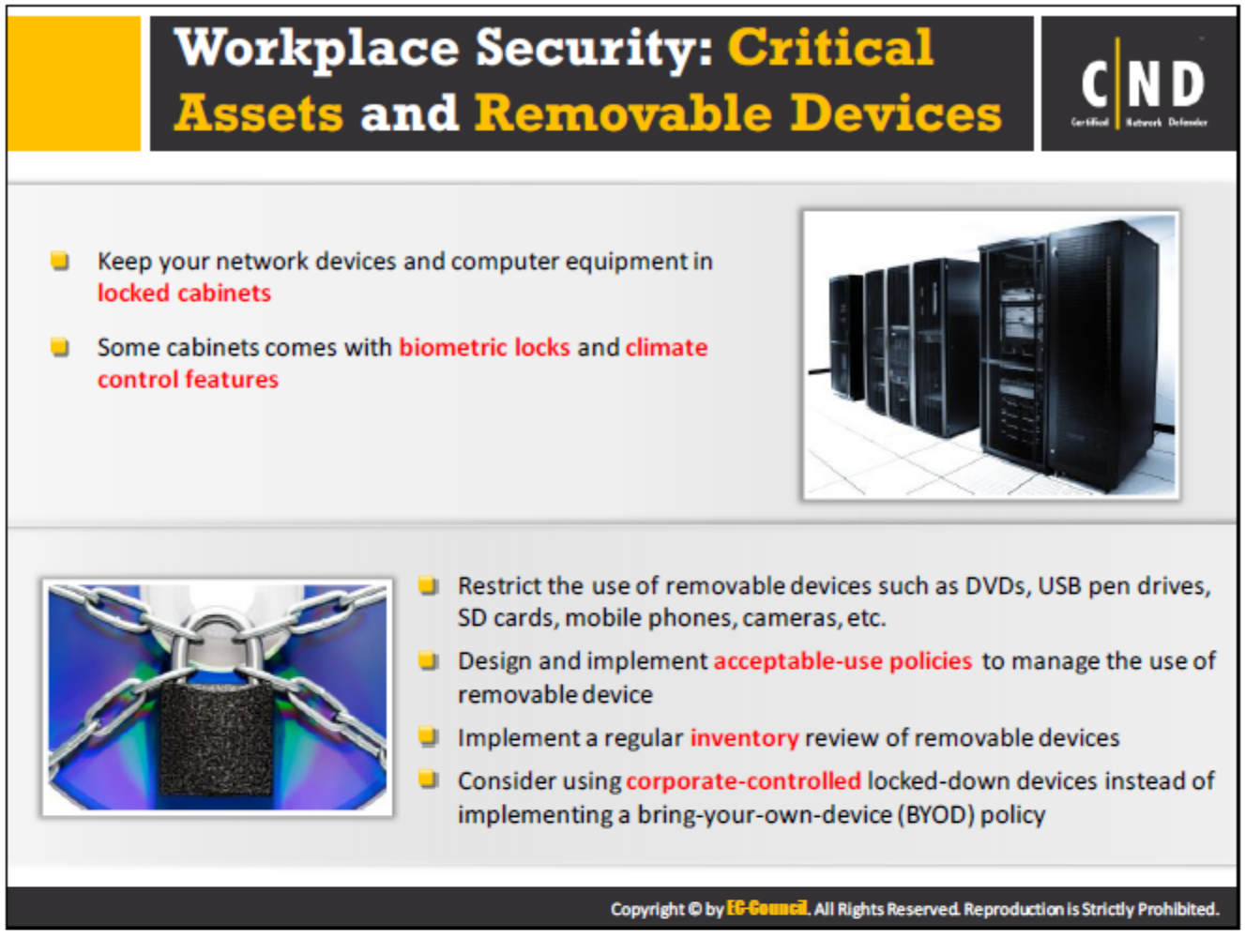
The reception area is always the initial contact for an unknown between them and the organization. The reception area can be vulnerable to physical security breaches as it provides easy access to strangers. Organizations often have regular visits from clients, the general public, invitees, etc., and require staff to greet, assist and direct them. Receptionists should be able to recognize or identify any unusual behavior, including solicitors and peddlers, charity organizations, ex-employees, etc. The reception personnel should maintain eye contact, 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, alarm, radio, first aid, etc.

The reception area should be small in size. This provides a better area to closely monitor visitors and the reception area. Reception personnel should observe people entering the company. They should notice and record odd behavior for any strangers. There should be certain benchmarks to judge people arriving to the organization. Their intentions have to be noted, whether a person is searching for someone or for something.

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

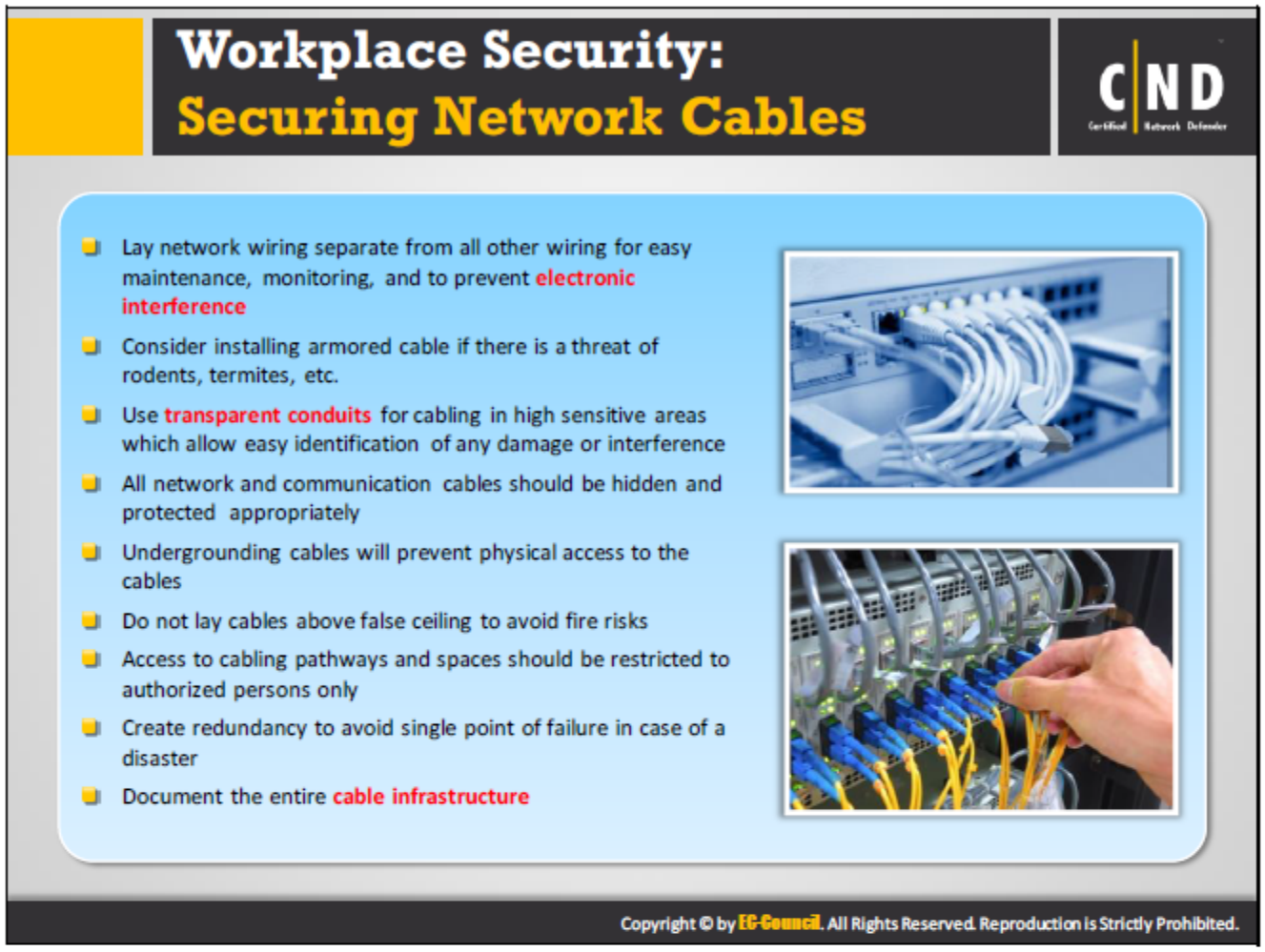
Typical physical security measures for server and backup devices are:

- Keep the server and backup devices in a separate room. This reduces the accessibility of these devices from the public and unknown people.
- Mount the CCTV, smart card, biometric authentication to track and monitor unauthorized physical access to the server and backup devices.
- Use rack mount servers. This restricts attackers from stealing or damaging the servers.
- The server should be attached to an UPS so that it protects the server 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 ensure that they are secured.
- Do not encourage employees to take backup on CD, DVD, USB, or external hard disks. Ensure the backups are locked up at all times in a drawer, safe or separate room.
- Do not allow employees to leave an area carrying a backup device with them. Use motion sensing alarms to detect movement of any backup device.
- Implement full disk encryption on backup devices.



The organization should always pay attention to their server and backup storage device security. At the same time, they should not ignore the security of their other critical assets such as workstations, routers and switches, printers, other network equipment, removable devices, etc. The organization should employ all the physical security measures of server/backup devices to critical assets and removable devices.

- **Workstations**: Workstations at unoccupied desks, empty offices, receptionist's desk, etc. are 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 a locked room.
- **Printers**: Like servers and workstations, printers can store important information, should be bolted down, and located in separate places.
- **Removable Devices**: Portable removable devices such as laptops, handheld computers, mobile devices, SD cards, USB, Bluetooth etc. can pose physical security risks. Keep these devices in a drawer, a safe or permanently attach a cable lock.



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 nice and neat, if it is not an organization can suffer from unplanned downtime. With flawed or insecure network cabling, an attacker can easily access sensitive information by passing other security controls. Wiretapping, physical damage or thefts are the risks associated with network cabling.

Types of Cable used in Network Cabling

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

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

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

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

  In 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 secured data transmission.
  - **Disadvantages:**
    - More expensive than UTP.
    - More difficult to install than UTP.

- **Fiber Optic**:

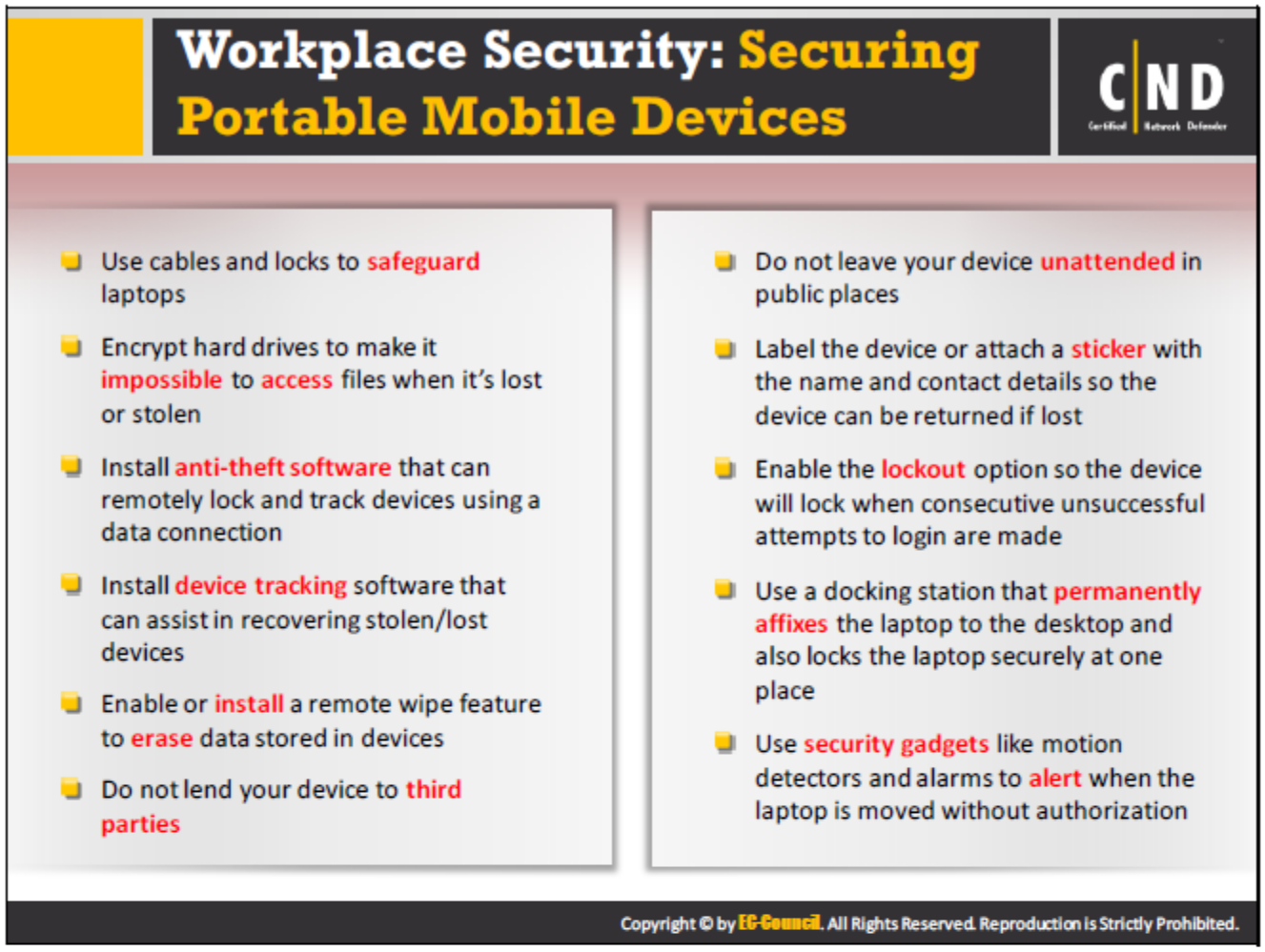
  It is made up of made of glass or plastic. Fiber optic cabling is least susceptible to wiretapping threats.

  - **Advantages:**
    - Can carry information over greater distances.
    - Immunity to electromagnetic interference.
    - No crosstalk.
  - **Disadvantages**:
    - Limited physical arc of cable.
    - Highly expensive.
    - Need optical transmitters and receivers.

- **Coaxial Cable:**

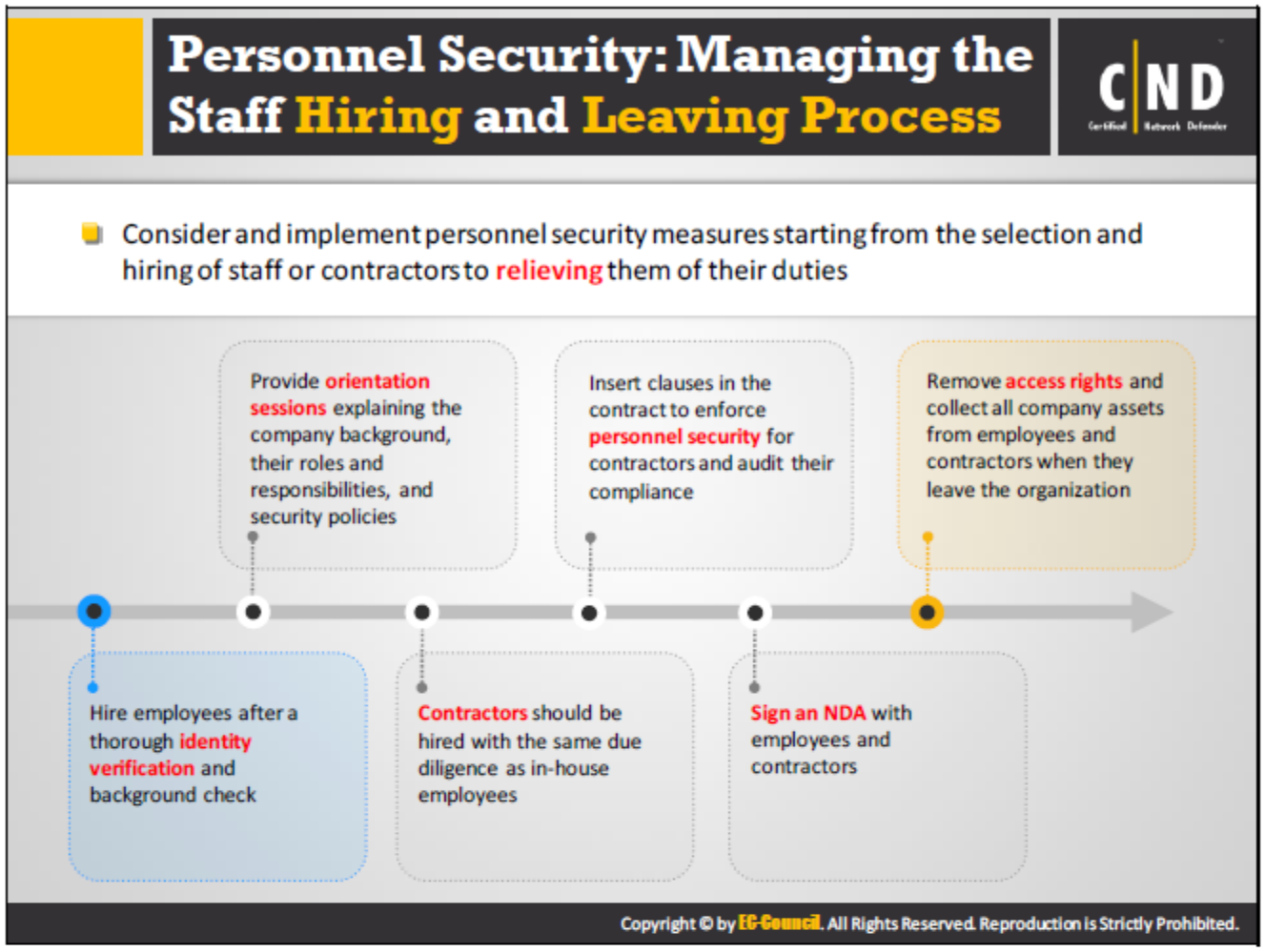
  Coaxial cable is made up of a single copper conductor at its center. A plastic layer provides an insulated center conductor and a braided metal shield. The metal shield prevents interference from fluorescent lights, motors, etc.

  - **Advantages:**
    - Can carry information over greater distances.
    - Moisture resistant.
  - **Disadvantages:**
    - It does not bend easily and is difficult to install.



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

- Apply all security measures common for these network devices such as servers, backup devices, portable devices, etc.
- Physically secure the mobile device location.
- Apply proper access control procedures for these devices.



Employees, regardless of their designation should understand the confidentiality of information and their separate personal and professional identities. A uniform procedure should be in place to explain the risks associated with a particular designation. Non-performance and disregard of an organization's sensitive data can affect the organization's security adversely.

Personnel Security for Employee/Contractors

- Establish an effective background screening process to find out the working potential of an employee.
- Perform background checks to find criminal, financial screening, education, past experience, and other certifications.
- Provide an orientation session for new employees and explain the company's background.
- Clearly explain the roles and responsibilities of each employee.
- Create security awareness and explain the concept of data confidentiality.
- Sign contracts/agreements with employees so they know not to share confidential data with others. It may include a confidentiality/nondisclosure agreement, acceptable use agreement, user rules of behavior, and a conflict-of-interest agreement.
- Hold employees accountable for every action performed and take disciplinary actions against those who oppose or neglect the security policies.

- All physical security practices for employees also apply to contractors. In addition, the organization should:
  - Make sure only contractors with proper clearance level have access to sensitive information.
  - Contractors should have an office identity card with their photo and personal details. It may even have an expiration date.
  - All contractors should carry their ID cards when they work on the floor. Contractors must exhibit their ID cards clearly to the security officer. Contractors should submit their ID cards when they are terminated by the office and also submit their ID card when they resign.

Employee/Contractors resignation and Clearance Procedures

The employee should send their resignation or retirement letter to the department head and Human Resource Department (HRD). HRD will consult with the relevant department head to discuss and accept the resignation. They collect various items such as their ID card, laptop, parking cards, etc., from the employee before the clearance procedures conclude. All related access controls provided to the employee are terminated.

The following steps are to clear an employee from his responsibilities:

- An employee has to submit their resignation and/or retirement letter to the department head with a copy going to the HR (Human Resource) department. The department head will forward the resignation letter to the central leave coordinator to relieve the employee from their responsibilities.
- After receiving the resignation letter from the employee, the department head will provide the last working day for the employee.
- An employee should fill out the clearance form and have a meeting with the central leave coordinator of the HR department who will provide a plan for the last working days of the employee.
- After having a chat with the employee, the HR department will send a notice to obtain clearance from all departments specified in the clearance form.
- After receiving the notice from the HR department, all departments will send the certificates to the central leave coordinator, within two days.
- The employee should inform the central leave coordinator on their last day, so the employee can complete the clearance process.
- After verifying all the clearance certificates from all departments, the central leave coordinator will clear the employee through the clearance form.
- After getting all the clearance certificates, the central leave coordinator will provide the employee with the following forms:
  - W-2 change of address form.

- Insurance form.
- Exit interview form (optional).

- The central leave coordinator will sign the clearance form, which depends on the clearance certificates received from all the departments.

EXO5 helps you track and locate laptops, smartphones and tablets across your organization in real-time

Features:

- **Real-time Agent:** The EXO5 agent uses a persistent and secure connection to provide asset inventory, geolocation and command execution in real-time. Information is always up-to-date, which is critical in developing a theft scenario.
- **Ultra-accurate Location:** EXO5 uses multiple methods to locate assets to provide the best location accuracy worldwide, including Wi-Fi and cellular triangulation, GPS, MAC address correlation, and IP address databases from multiple providers.

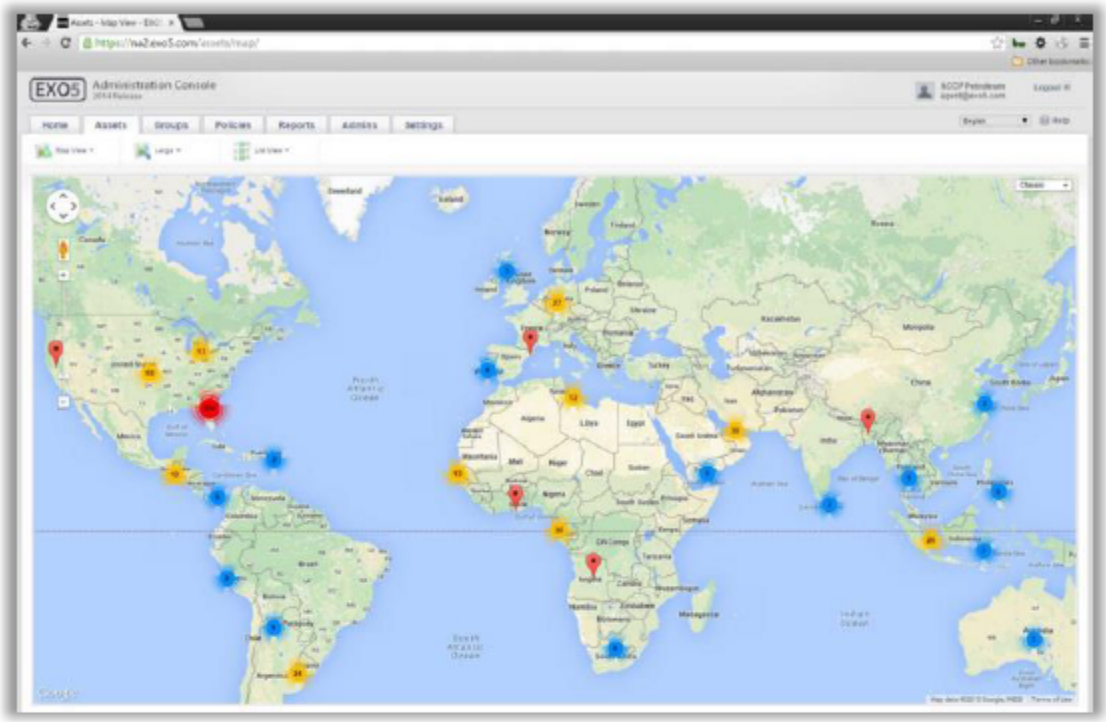


FIGURE 5.14: EX05 Maps

- **Dynamic Maps:** Use the Google Maps interface to quickly locate assets, or the real-time LiveMap and Google Earth display for a commanding view of your entire organization.

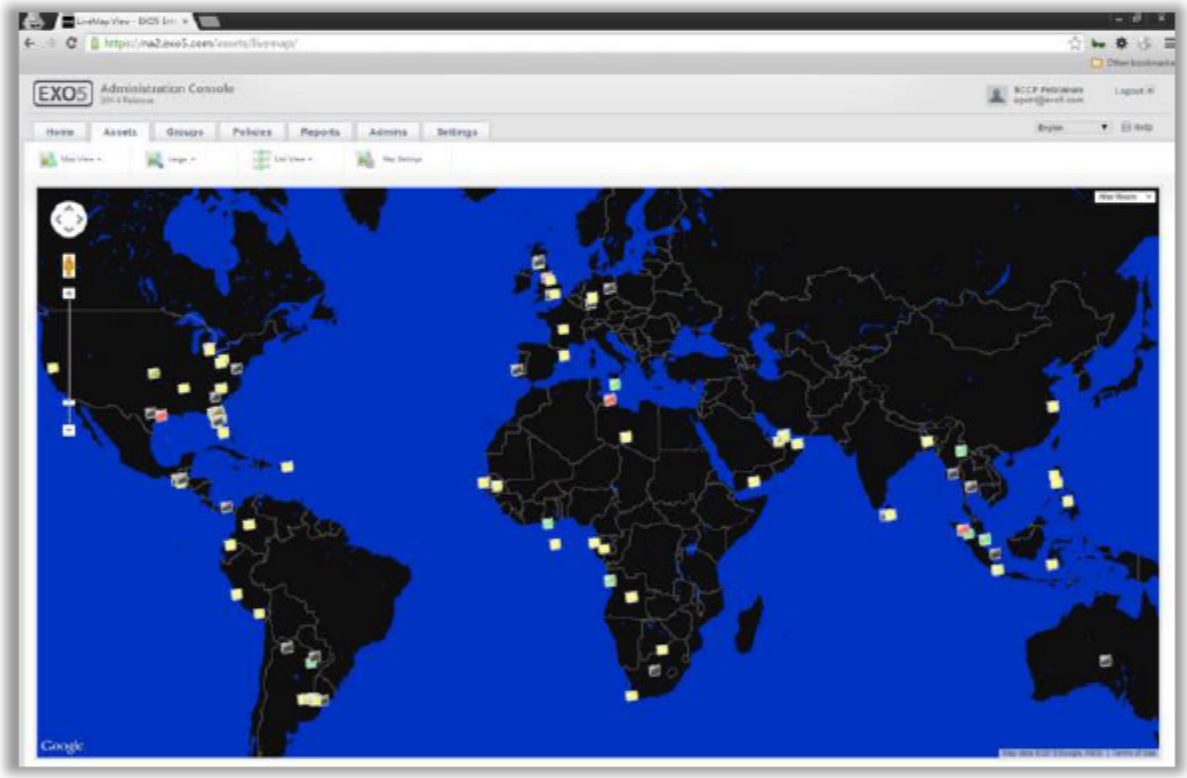


FIGURE 5.15: Dynamic Maps

Source: https://www.exo5.com

Ztrace Gold

Source: *http://www.ztrace.com*

ZTRACE GOLD is an invisible software security application that traces the location of missing laptops for recovery. It is undetectable and cannot be removed from a laptop hard drive.

Prey

Source: *http://preyproject.com*

It is tracking software that helps users find, lock and recover their computer, tablet or smartphone when stolen or missing.

Snuko Anti-Theft and Flamory

Source: *http://flamory.com*

Snuko Anti-Theft and Flamory help you to track your Android device when it is lost or stolen. You can remotely activate geolocation tracking, data encryption, data backup and device lock down to protect against unauthorized use.

Laptopcop

Source: *https://awarenesstechnologies.com*

LAPTOP COP allows you to identify, track, and control who accesses data on a stolen laptop, what data is accessed, and what can and cannot be done with that data.

GadgetTrak

Source: *http://www.gadgettrak.com*

GadgetTrak provides mobile security software for a range of mobile devices including mobile phones, laptops, flash drives, external hard drives and more. It helps you in finding your lost or stolen laptop.

LoJack

Source: *http://www.lojack.com*

LoJack allows you to track, manage, secure and recover mobile computers. It has remote data and device security to prevent use of a lost laptop, protect privacy remotely, and map a laptop's location.

Adeona

Source: *http://adeona.cs.washington.edu*

Adeona allows you to track the location of your lost or stolen laptop that does not rely on a proprietary central service.

TrackMyLaptop

Source: *http://trackmylaptop.net*

TrackMyLaptop helps you track your stolen laptop.

MyLaptopTracker

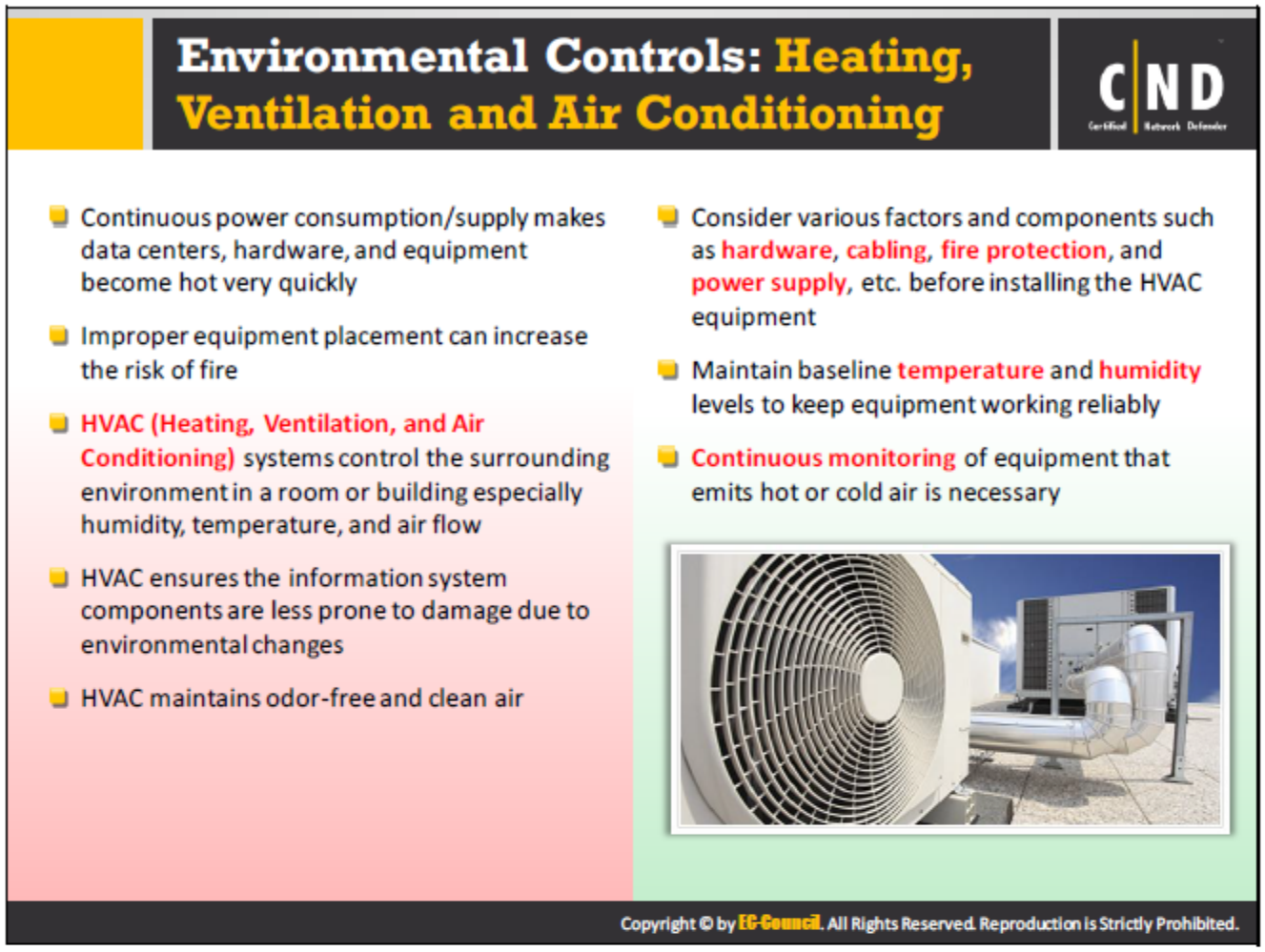
Source: *http://www.mydevicetracker.com*

My Laptop Tracker can track down your stolen or lost laptop within minutes.

Locate Laptop Desktop Security

Source: *http://www.unistal.com*

Locate Laptop protects your laptop from being stolen. It is used to locate and recover lost or stolen laptops.



It is a special system that controls the surrounding environment in a room or building, especially the humidity conditions in the air and ventilation. It is deployed to maintain comfortable temperatures in a room so the hardware is not affected by the moisture and changes in the air. In these controlled conditions, the hardware and the components are also safer and less prone to damage from environmental factors. The HVAC also purifies the air in the room from smoke, odor, heat and dust particles. Having an environment where the air is odor free, clean and the humidity is under control provides a good atmosphere for the people working with that organization. These ventilation systems are desired mostly in medium to large scale organizations involving heavy equipment and a larger amount of staff. A pre-programmed sensing device is used to check for changes in the temperature and it acts accordingly. Manual controlling the HVAC also can be done.

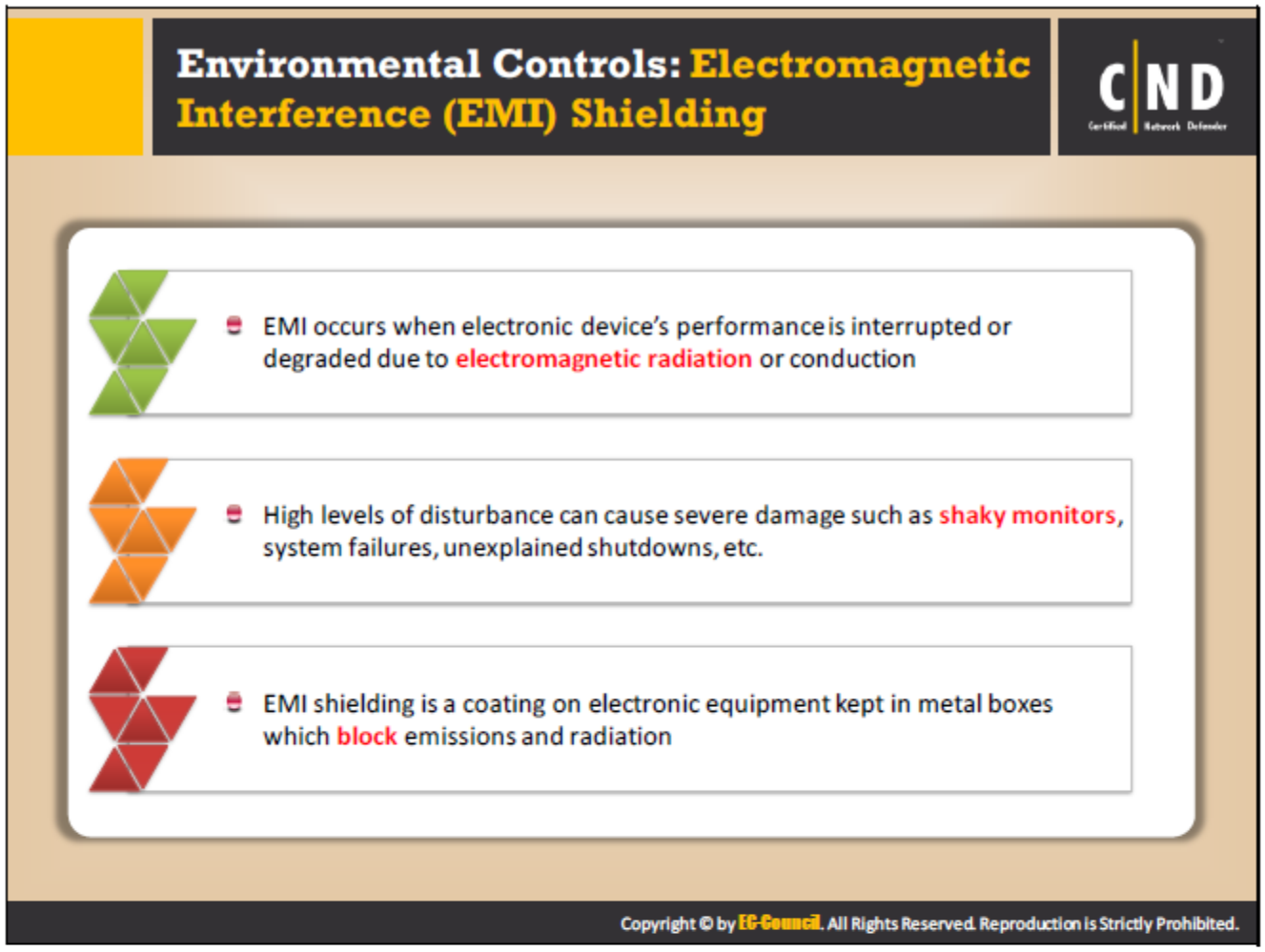
A refrigeration component is added to a HVAC system, also known as HVAC&R or HVACR (heating, ventilating and air-conditioning & Refrigeration) system

Types of HVAC Systems

- **Heating and Air-Conditioning Split System:** The most traditional and commonly used HVAC system. You may find the components of the system both inside and outside the building. HVAC split systems have:
  - An air conditioner in order to cool the refrigerant.
  - Furnaces, a fan or evaporator coil: Converting the refrigerant and circulates the air.

- Duct: Allow air flow throughout the building.
- Air quality fittings like air cleaners, air purifiers etc.

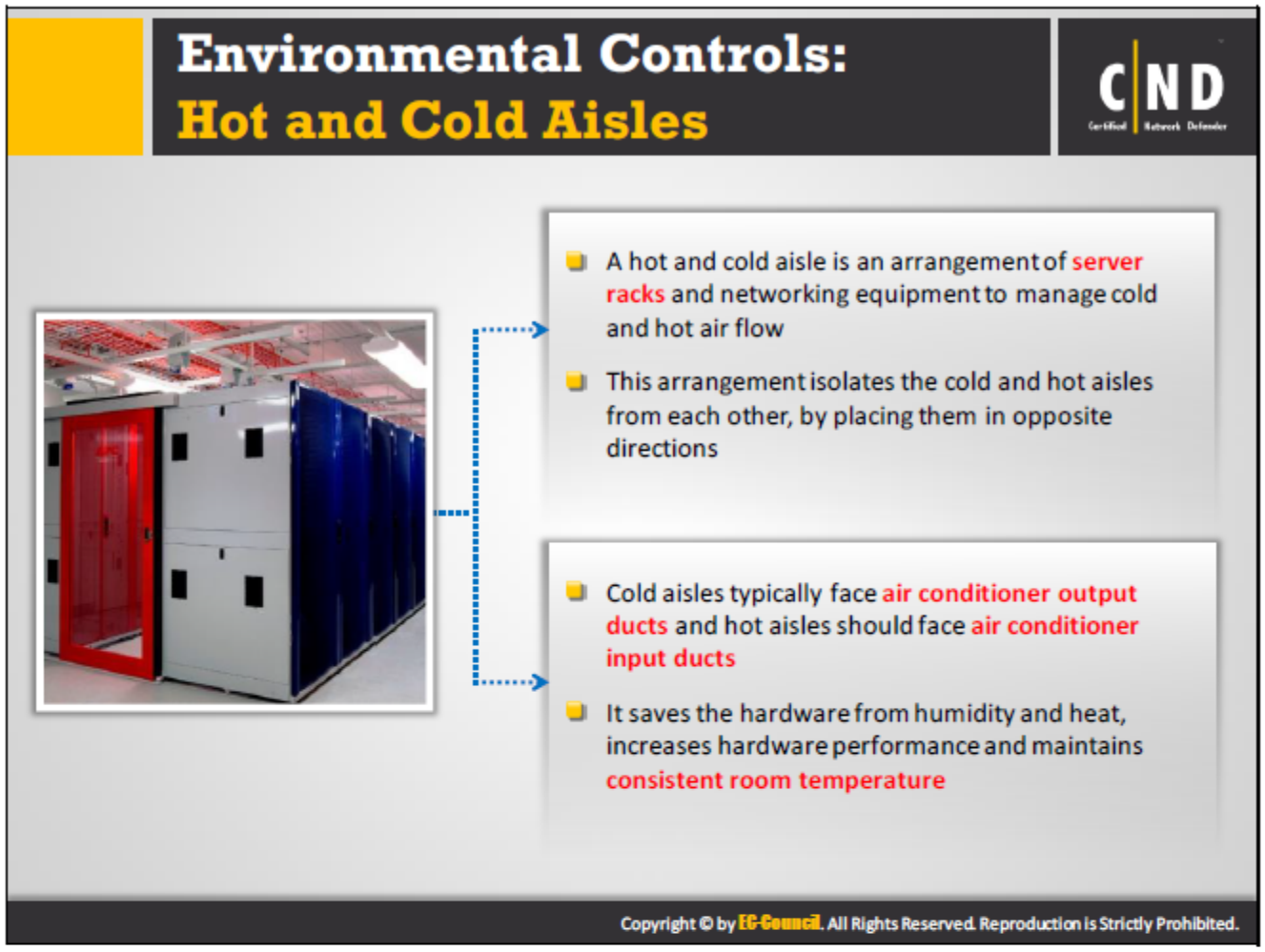
- **Hybrid Heat Split System:** This is an advanced version of a split system having better energy effectiveness. Here, the heat pump provides an electrically fueled HVAC instead of gas furnace heat. A typical hybrid heat split system includes:
  - Heat Pump: Cool/heat the refrigerant.
  - Furnaces/Evaporator Coil: Converts refrigerant and circulates the air.
  - Duct: Allow air flow throughout the building.
  - Control or Thermostat: An interface to control the system.
  - Air quality fittings like air cleaners, air purifiers etc.
- **Duct – Free Split Heating and Air Conditioning System:** Most commonly used in locations where the traditional split systems cannot be used. A typical duct-free split system includes:
  - An air conditioner in order to cool the refrigerant.
  - Fan Coil: Converts the refrigerant and circulates the air.
  - Refrigerant tubing and wires: Connects outdoor unit to the fan coil.
  - Control or Thermostat: An interface to control the system.
  - Air quality fittings like air cleaners, air purifiers etc.
- **Packaged Heating and Air-Conditioning System:** Most appropriate air conditioning system used mainly in locations where the space required for fixing all the components of a split system is available. Packaged units can be used in spaces that range from an entire building to one room units. Packaged heating and air-conditioning system includes:
  - Packaged Products: A heat pump or an air conditioner combined with a fan coil or an evaporator coil in a single unit.
  - Control or Thermostat: An interface to control the system.
  - Air quality fittings like air cleaners, air purifiers etc.



Electromagnetic radiation emitted from different electronic devices interferes with surrounding devices and causes a problem with their functions. EMI shielding is the practice of coating the electronic equipment with metals so the electromagnetic waves do not interfere with other devices or block the field 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 externally applied electric charge 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 way the shielded material has no outside effects or disturbances on it.

As organizations use heavy equipment, electronic hardware interference will become a problem and EMI shielding will be needed for all devices in these types of environments. Many industries, such as telecommunication, hospitals, etc. prefers to use EMI shielding.



It is a systematic arrangement of equipment to maintain air flow and to save energy. Many organizations follow hot and cold aisle alignment, mostly used in server rooms, data centers, etc. where heavy electronic equipment comes into use.

In the rack of heavy equipment or servers they are arranged so the front of them faces the cold air coming from the air conditioners. The backs of the equipment face the back of the next rack of equipment. This goes on for all the equipment in the room. This arrangement pushes the hot air coming from the back of the equipment to one end of the room. The cooling conditions are kept so that the hot air coming out of the equipment is sucked out and does not mix with the cool air inside the room. Place the cooling system below the room or above the room depending on the convenience.

Cold Aisle: Advantages and Disadvantages

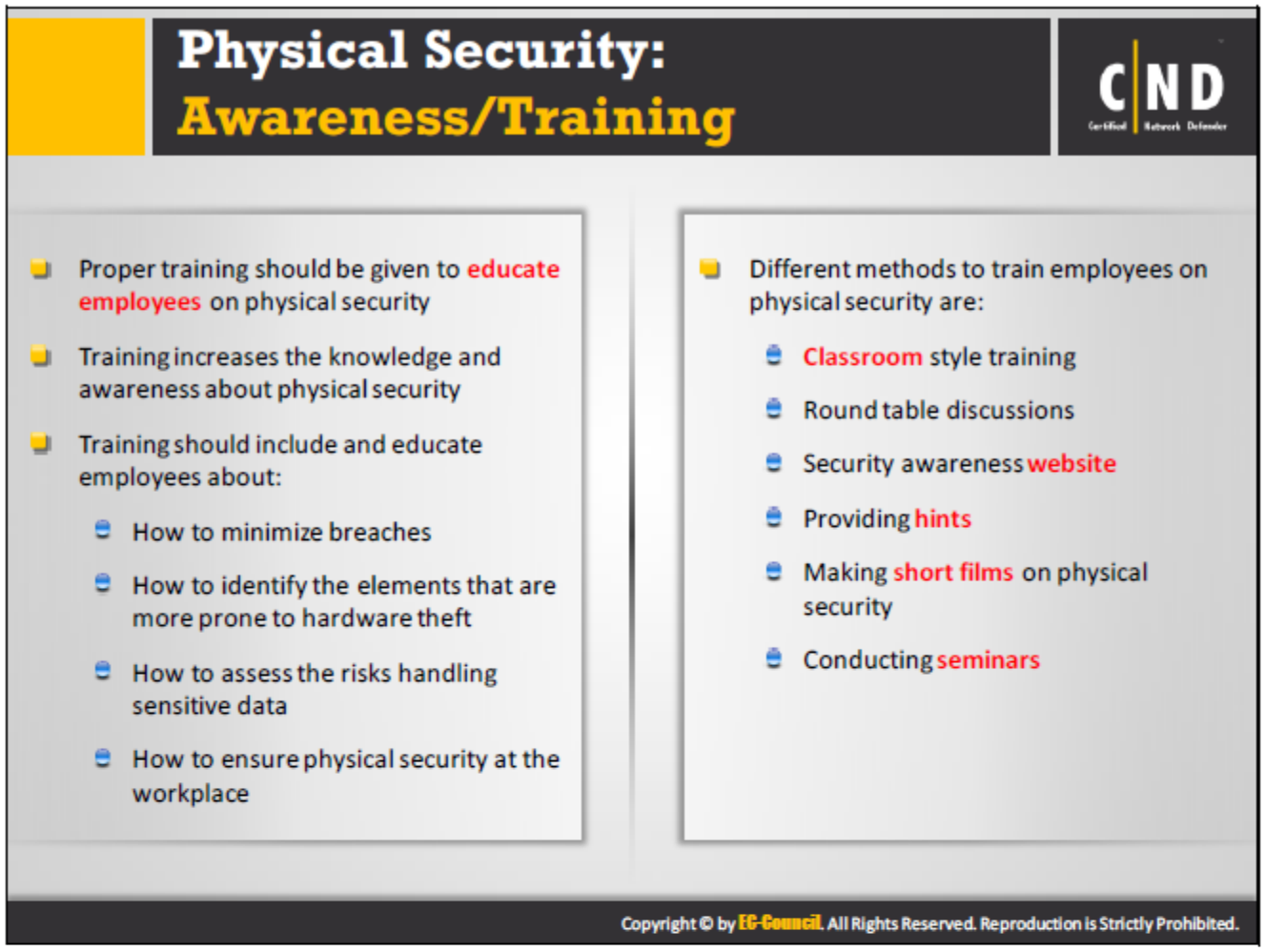
- **Advantages:**
  - Easy to implement as it does not require any supplementary architecture to give out air.
  - Requires doors only at the end.
  - Less expensive.
  - Can easily fit into an existing data center with issues like power, network distribution etc.

- Can be used with a raised floor supply space.
- Controls the air supply to match with the severe airflow.

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

Hot Aisle: Advantages and Disadvantages

- **Advantages:**
  - Leakage from the raised floor openings are passed over to the cold space.
  - 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 an additional space for the flow of air from the hot aisle to the cooling unit.
  - Very expensive.
  - Hot aisles it uncomfortable for technicians during maintenance work.



Well trained and skilled personnel can minimize the risk of a physical security threat to a great extent. The organization should provide proper physical security awareness training to all of their employees.

The training or awareness program should include:

- Provide methods to reduce attacks.
- Examine all the devices and the chances of a data attack.
- Teach the risks of carrying sensitive information.
- Teach the importance of having security personnel.

An organization can use various methods to conduct physical security training awareness programs:

- **Classroom Training**

  Classroom training provides an interactive lecture based session. The benefits of having classroom training are:

  - All doubts regarding the topic may be cleared.
  - Can provide web based and live training sessions.
  - Can be made more interactive by imposing role plays and simulation games.

The duration of the classroom training can vary. It depends upon the technique used in implementing the classroom session.

- **Round Table Sessions:** Round table sessions may be conducted to train employees regarding the need for physical security. These sessions may be held weekly or monthly.
- **Security Awareness Website:** Creating a security awareness website enables the employees to login and learn for themselves regarding physical security measures. Several videos, pictures and examples should be included in the website stating the importance of physical security. Several topics may be covered through the website training as there is no time constraint.
- **Providing Hints:** Hints regarding changing passwords or password security may be provided through hints.
- **Making Short Films on Physical Security:** Teaching using examples can help employees understand more about the importance of physical security. Filming instances describing the need for physical security, chance of risks and methods to prevent them.
- **Conducting Seminars:** Several seminars on each topic for physical security may be conducted. Seminars may include examples, discussions and debates regarding the topic.

Physical Security Checklists

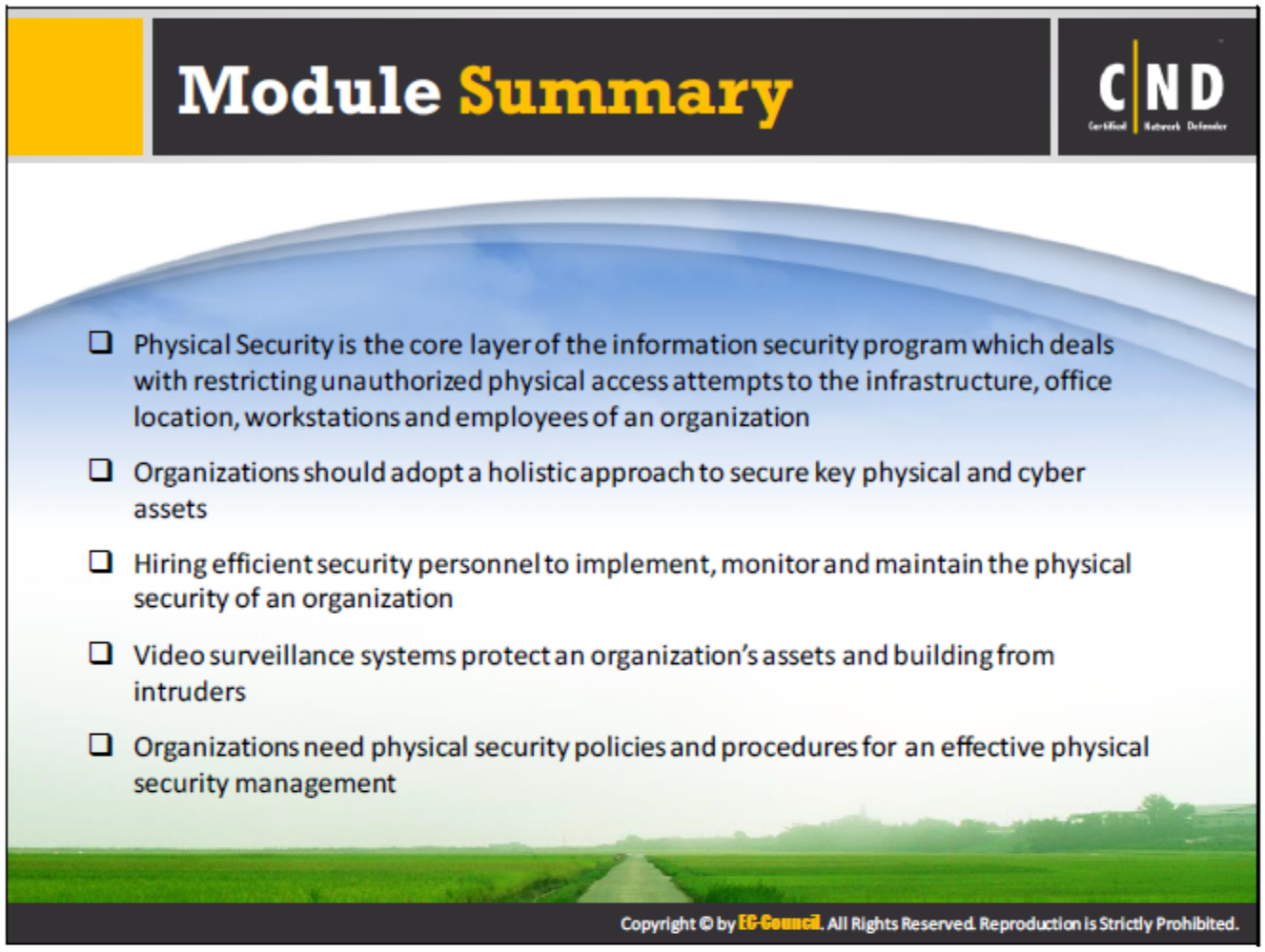
1	Ensure that proper access control methods are implemented to prevent unauthorized access
2	Ensure that sensitive areas are monitored with proper lighting
3	Ensure an alarm system is installed for all types of threats such as fire, smoke, electricity, water, etc. and is working properly
4	Ensure an 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
7	Ensure the security personnel is hired from a trusted agency
8	Ensure surveillance cameras are working properly and monitored regularly
9	Ensure proper procedures are implemented for detecting and reporting physical security incidents
10	Ensure employee contact information is maintained for use during emergencies

Physical security can be built in layers, or follow a Defense-in-Depth strategy to implement physical security for the organization. The organization should consider implementing all the physical security controls and measures to ensure a Defense-in-Depth physical security for their organization.

The following checklist will help an organization ensure they are implementing proper security controls and measures:

- **Follow copyright rules and licensing restrictions:** The organization should enforce copyright rules and licensing restrictions in order to prevent outsiders or insiders from creating illegal copyrighted copies of the software.
- **Store all removable and important items in the locker when not in use:** Employees should ensure to lock all sensitive information and important devices in a locker. Do not leave any important information unattended as it may catch the eye of an attacker.
- **Keep the sensitive areas under surveillance:** The organization should ensure security for sensitive areas like server rooms, etc. CCTV surveillance and guards may be enforced in order to maintain security in the sensitive areas. The organization should enforce 24x7 surveillance for the sensitive areas.
- **Always advise employees to swipe the card at the entrance:** Swiping ID cards at the entrance helps the organization to audit the login details of the employees in case of an incident.

- **Do not keep any combustible material in the workplace area:** Always keep any sort of combustible materials away from the workplace area. This ensures the safety of the employees, the information stored and the devices stored inside the workplace area.
- **Always ensure company satisfaction:** Employ security measures that guarantee 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. Preventing attackers from entering the workstations and server rooms, authenticating each person using ID cards or biometric ensures better security of the location. Other security measures include ensuring locking cabinets, doors and windows, proper surveillance using CCTV, proper lighting etc.
- **Do not disconnect consoles from ports:** Disconnecting cables or consoles from ports will lead to a disconnection for the user. You should make sure the cables are all connected to the ports and are working properly.
- **Use of alarms and sensors during fire, smoke etc.:** The organization should ensure proper use of sensors and alarms in order to detect fire or smoke on the premises. An organization may include sensors for devices in order to detect if anyone tries to take those devices out of the organization.
- **Prevent damage to hardware and software:** Any damage to the hardware or software results in damage of the information systems in the organization. Damage to the hardware will lead to the damage of the electronic and mechanical systems used in data processing. Damage to software leads to the damage in the programs and instructions used for data development.
- **Do not leave any devices or important data in the parking areas or cars:** Any unattended devices or data may attract attackers and may 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. Employ security cameras in sensitive areas and log the who is accessing those areas.
- **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 phone. Attackers may gain access to your mobile devices and then acquire all of its sensitive information.



In this module, we have discussed the importance of physical security, and its role in the organization's information security program. This module introduced you to the various physical security controls and security measures that organizations should consider while implementing physical security. It will help the organization implement their Defense-in-Depth strategy for physical security.

In the next module, we will discuss security of an individual host on the network. We will make discuss various security measures required to harden security of a host which may include workstations, routers, switches, servers, etc.