Physical security can be defined as the protection and concern regarding information-related assets storage devices, hard drives, computers, organizations' machines, and laptops and servers. The protection is mainly taken care of real-world threats and crimes such as unauthorized access, natural disasters like fire and flood, a human-made disaster like theft, etc. This type of security requires physical controls such as locks, protective barriers, in-penetrable walls and doors, uninterrupted power supply, and or security personnel for protecting private and sensitive data stored in servers.

Information Security vs. Physical Security

Both the term has a conceptual difference. Information security generally deals with protecting information from unauthorized access, disclosure, illegal use, or modification of information, recording, copying, or destroying information. Information security is based on a logical domain, whereas physical security is based on the physical domain.

Objectives of Physical Security

- Understand the needs for physical security.
- Identify threats to information security that are connected to physical security.
- Describe the key physical security considerations for selecting a facility site.
- Identify physical security monitoring components.
- Understand the importance of fire safety programs.
- Describe the components of fire detection and response.

Factors on Which Physical Security Vulnerabilities Depend

Any hack may result in success, despite the security if the attacker gets access to the organization's building or data center looking for a physical security vulnerability. In small companies and organizations, this problem may be less. But other factors on which physical security vulnerabilities depend may be as follows:

1. How many workplaces, buildings, or sites in the organization?
2. Size of the building of the organization?
3. How many employees work in the organization?
4. How many entry and exit points are there in a building?

5. Placement of data centers and other confidential information.

Attack Points to Compromise Physical Security

Hackers think like real masterminds and find exploits in buildings for physical unauthorized access. From the attacker's point of view, the tactics to compromise physical security are:

- Are the doors propped open? If so, that can be an attack vector.
- Check whether the gap at the bottom of critical doors allows someone to uses any device to trip a sensor inside the security room.
- Check whether it would be easy or not to open the door by breaking the lock forcefully.
- Are any doors or windows made of glass, especially the server room's doors or other confidential areas?
- Are the door ceilings with tiles that can be pushed up?
- Are power supply and protection equipment is faulty?
- Obtain network access by a hacker, and then hackers can send malicious emails as logged in users.

Layers of Physical Security

Physical security depends on the layer defense model like that of information security. Layers are implemented at the perimeter and moving toward an asset. These layers are:

1. Deterring.
2. Delaying.
3. Detection.
4. Assessment.
5. Response.

Crime Prevention Through Environmental Design (CPTED)

It is a discipline that outlines how the proper design of a real scenario can mitigate crime and hacking by directly affecting human behavior. This concept was developed in the 1960s and is still used mainly to prevent social engineering. It has three main strategies, namely:

1. Natural Access Control.
2. Natural Surveillance.

3. Territorial reinforcement.

Risk Assessment

Both physical intruders and cybercriminals have the same motive as money, social agenda, etc. Also, intruders try to seek opportunities to exploit by any means. So these three terms - motive, opportunity, and means are listed together to make a formula whose calculation is resulted in the total risk i.e.

$$\text{Risk} = \frac{\text{Controls((Means+Motive)*Opportunity)} * \text{Business Impact}}{\text{Controls}}$$

Countermeasures and Protection Techniques

Physical security has the fact that security controls are often reactive. Other experts need to be involved during the design, assessment, and retrofitting stages from a security perspective. Other than that, the security measures that must be taken are:

1. Strong doors and locks.
2. Lights and security cameras, especially around entry and exit points.
3. Windowless walls around data centers'.
4. Fences (with barbed wire or razor wire).
5. Closed-circuit televisions (CCTVs) or IP-based network cameras need to be used and monitored in real-time.
6. An intrusion detection system must be applied to detect unauthorized entries and to alert a responsible entry.
7. Know the different types of IDS systems, such as electromechanical and volumetric.
8. Security personnel and guards must be used to protect data against physical theft or damage.
9. The organization should serve a simple form of biometric access system (such as facial or fingerprint scanning access).
10. Ties physical security with information access control such as ID card and name badge.
11. Different types of lock systems must apply, such as manual locks, programmable locks (controlled by computers), electronic locks, biometric locks (facial scan and retina scans).
12. Alarm and alarm systems should have to be installed in the building infrastructure to notify if an event occurs, such as fire detection, intrusion detection, theft, environmental disturbances, or interruption in services.