Physical Security

Introduction

- Physical security addresses design, implementation, and maintenance of countermeasures that protect physical resources of an organization.
- Most controls can be circumvented if an attacker gains physical access.
- Physical security is as important as logical security.
- Major sources of physical loss are Natural calamities, Human interference etc.,.
- Physical Security controls are achieved with High Walls, defense fencing, User access control systems, video surveillance systems, locks and keys, mantraps, alarms systems, Security lighting etc.

Effective physical security measures

Closed Circuit Television (CCTV): CCTV is a surveillance tool that provides an added set of eyes. Now a days CCTV surveillance systems can be easily integrated with monitoring devices, alarm systems and access control devices. Which helps to identify and interrupt security breaches before they occur.

Intrusion detection Alarms: It detects unauthorized entry into the building and also notifies Police/Fire department in case of any emergency. Alarm sensors are placed inside, outside or around the perimeter of building, when a sensor detects unauthorized entry it triggers alarm.

Security Lighting: Lighting and security go hand in hand. Installation of improved lighting inside and outside of the building reduces the risk of attacks.

Access control systems: It restricts unauthorized entry through doors/gates. There are different types of access control systems such as Key card, Key fob, biometric (finger print, retina scan) etc.

Objectives of physical security

- The main tasks of physical security include

  - Monitoring, surveillance, intrusion detection, barrier and detour.

  - Utilities management (electrical, AC, etc.).

  - Fire detection/suppression.

  - Data loss prevention & secure remote computing.

  - Laptop/mobile device inventory, management, and security.