Name: Mariam Mostafa Amin Mostafa

Key Components of Physical Security:

Physical security can be described as a group of layers of defense developed to deter, detect, delay, and respond to unauthorized access or physical threats here are some examples of key components of physical security.

1. Perimeter Security:

Examples: Fencing, walls, gates, bollards.

Function: This acts as the first line of defense in demarcation.
Avoids unauthorized entries and intrusion of vehicles into secured areas.
Serves as a physical barrier to intruders or a vehicle used in a ramming attack.

Risk Mitigation: Lessens the possibility of casual trespass and delays the determined intruder in order to give time for security teams to respond.

---

2. Access Control:

Examples: Key cards, biometric systems, PIN codes, physical locks.

Function: Regulates who can enter specific areas based on roles or permissions.
Tracks entries and exits for accountability.
Can integrate multi-factor authentication for higher security.

Risk Mitigation: Prevents unauthorized individuals from accessing restricted areas, reducing the chances of theft, sabotage, or espionage.

---

3. Surveillance Systems

Examples: CCTV cameras, IP cameras, motion sensors, drones.

Function: Monitors activities in real-time, creating visibility across the premises.
Records evidence for post-incident analysis or admissibility in a court of law. Provides some crime prevention through the perceived risk of recording them.

Risk Mitigation: Situational awareness, early detection of suspicious behavior, investigation assistance

---

4. Environmental Design

Examples: Strategic lighting, landscaping, clear sightlines, controlled vegetation.

Function: Reduces hiding spots for intruders with enhanced visibility.
Creates a safer environment for employees and visitors at any time of night.
Application of Crime Prevention Through Environmental Design-a philosophy that aims to prevent crime through the natural design of the environment.

Risk Mitigation: Minimizes the prospect of clandestine activities, hence enhancing the perception of safety and security.

---

5. Intrusion Detection Systems:

Examples: Infrared sensors, pressure sensors, glass-break detectors.

Function: Detectors of attempts at unauthorized entry or physical breaches.
Creates an alarm or notification to alert security personnel.

The configuration is able to interface with surveillance/access control to affect an automated response.

Risk Mitigation: Allows early warnings of breaches to minimize potential damage or theft.

---

6. Security Personnel:

Examples: Guards, patrol teams, K-9 units.

Function: Act as a visible deterrent to potential intruders.
Conduct physical checks and respond to alarms or suspicious activities.
Provide rapid intervention in case of incidents.

Risk Mitigation: Adds a human factor to security measures, covering the lapses where automated systems might fail.

---

7. Alarm Systems:

Examples: Fire alarms, panic buttons, emergency alert systems.

Function: Alert occupants and the security team when there is any emergency like intrusions, fire, or hazardous leaks.
Can trigger lockdowns or evacuation protocols.

Risk Mitigation: Improves the response time and minimizes the impact caused by any emergencies.

---

8. Physical Barriers:

Examples: Turnstiles, security doors, reinforcement of windows.

Function: Limits movements in facilities to authorized paths.
Strengthens entry points against forcible accesses.

Risk Mitigation: Delays intruders and gives very important response time to the security teams.

---

9. Secure Storage:

Examples: Safes, vaults, locked cabinets.

Function: Protects sensitive documents, equipment, or materials from unauthorized access or theft.

Risk Mitigation: Prevents data breaches, theft of equipment, or its damage by sabotage.

---

10. Redundancy and Backup Systems:

Examples: Backup power supplies, redundant communication lines.

Function: Ensures critical systems remain operational during outages or disruptions.
Reduces vulnerability during emergencies like natural disasters.

Risk Mitigation: Maintains security infrastructure functionality, preventing system downtime exploitation.