Securing the Foundation

A Comprehensive Overview of Physical Security Strategies and Measures

CISSP Study Guide - II

Introduction to Physical Security

- Concerned with protecting organizational assets and personnel.
- Addresses both internal and external threats.
- Encompasses geographical, man-made, political, and natural threats.
- Requires a multifaceted approach involving threat mitigation techniques and physical security measures.

Threat Mitigation Techniques

1. **Internal Measures**: Protect sensitive areas within the facility, e.g., server room secured by card swipe locks.

2. **External Measures**: Secure the perimeter to prevent unauthorized access, e.g., electric fences.

3. Consider risks from man-made and political threats alongside natural disasters like hurricanes, tornadoes, earthquakes, and floods.

Natural Threats & Mitigation

- Assess required investments based on natural disaster risks in the area.
- **Implement measures such as:**

> - Raised flooring systems to counteract flood risks.
> - Uninterruptible Power Supplies (UPS) for mission-critical systems.
> - Onsite generators for sustained power outages.
> - Proper humidity control (40% - 60%) to prevent equipment damage.

Man-Made & Political Threats

Guard against explosions, fire, vandalism, and theft by restricting physical access.

Prepare for politically motivated threats like strikes, riots, civil disobedience, and terrorist acts with emergency planning and evacuation drills.

Site and Facility Design Principles

- Utilize a **Layered Defense Model** with multiple reinforcing security concepts.
- Integrate **Crime Prevention Through Environmental Design (CPTED)** with:

  - Natural Access Control
  - Natural Surveillance
  - Territorial Reinforcement

Physical Security Plan Objectives

1. **Deter Criminal Activity**: Implement a layout and policies that dissuade unlawful acts.

2. **Delay Intruders**: Use barriers to slow unauthorized entry.

3. **Detect Intruders**: Enable systems for recognizing unauthorized presence.

4. **Assess Situation and Respond**: Assign personnel for immediate action during security events.

Facility Selection & Computer Room Security

- Choose a facility based on visibility, surrounding environment, accessibility, and construction.
- **Secure computer and equipment rooms by:**

> - Locating in the building's center and limiting entrances.
> - Installing fire detection/suppression systems and raised floors.
> - Employing separate power supplies and solid doors.

Perimeter Security Features

Fences: Deter casual to determined intruders with varying heights and additional features like razor wire.

Gates: Categorized for residential, commercial, industrial, and restricted access.

Intrusion Detection: Utilize IR sensors, electromechanical, photoelectric, acoustical systems, and CCTV for comprehensive monitoring.

Interior Security Measures

1. Secure various door types according to their usage with bullet-resistant materials and electronic or mechanical locking mechanisms.

2. **Mantraps**: Control access between two entry points to secure areas.

3. **Glass Entries**: Choose from standard, tempered, acrylic, or laminated glass based on security requirements.

Protection Against Fire and Power Issues

Equip areas with smoke, heat, and flame detection systems.

Choose from wet pipe, dry pipe, preaction, or deluge systems for fire suppression depending on the room's sensitivity to water.

Mitigate power surges, brownouts, faults, blackouts, and sags with conditioners and UPS systems.

Prevent static electricity and ensure the safety of equipment and personnel.

HVAC, Equipment, and Personnel Security

- Outline HVAC specifications to protect against environmental threats.
- Establish proper procedures for equipment security, including tamper protection, encryption, inventory control, and physical device security.
- Prioritize human resource safety with a comprehensive Occupant Emergency Plan (OEP).

Information Security Buzz

Discover more at our InfoSec Knowledge Hub