Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 10 of the official CISSP study guide. Here are the top things that you need to know from this chapter on physical security requirements.

Understand why there is no security without physical security. Without control over the physical environment, no amount of administrative or technical or logical access controls can provide adequate security. If a malicious person can gain physical access to your facility or equipment, they can do just about anything they want from destruction to disclosure and alteration.

Understand a security facility plan. A security facility plan outlines your organization's security needs and emphasizes methods or mechanisms to provide security. Such a plan is developed through risk assessment and critical path analysis.

Know about technology convergence. Technology convergence is the tendency for various technologies, solutions, utilities, and systems to evolve and merge over time. Though this can result in improved efficiency and cost savings in some instances, it can also represent a single point of failure and become a more valuable target for malicious actors and intruders.

Understand site selection. Site selection should be based on the security needs of the organization. Cost, location and size are important, but addressing the requirements of security should always take precedence. The key elements in selecting a site are visibility, composition of the surrounding area and accessibility. Know the key elements in designing a facility for construction. A key element in designing a facility for construction is understanding the level of security needed by your organization and planning for it before construction begins. Know the functional order of controls. These are deter, deny, detect, delay, determine and decide.

Understand equipment failure. No matter the quality of the equipment your organization chooses to purchase and install, eventually it will fail. Preparing for equipment failure may include purchasing replacement parts, storing equipment or having an SLA with a vendor. Know how to design and configure secure work areas. There should not be equal access to all locations in a facility. Areas that contain assets of higher value or importance should have restricted access. Valuable and confidential assets should be located in the heart or center of protection provided by a facility.

Understand the security concerns of a wiring closet. A wiring closet is where networking cables for an entire building or a floor are connected to other essential equipment such as patch panels, switches, routers, land extenders and backbone channels. Most of the wiring closet security focuses on preventing unauthorized access. If an unauthorized intruder gains access to the area, they maybe able to steal equipment, pull or cut cables or even plant a listening device.

Know about proximity devices and readers. A proximity device can be a passive device, a field powered device or a transponder. When it passes near a proximity reader, the reader device is able to determine who the bearer is and whether they have authorized access.

Understand intrusion detection systems. Intrusion detection systems IDSs or burglar alarms are automated or manual systems designed to detect an attempted intrusion, breach or attack, the use of an unauthorized entry point or the occurrence of some specific event at an unauthorized or abnormal time.

Know about cameras. Video surveillance, video monitoring, closed circuit television and security cameras are all means to deter unwanted activity and create a digital record of the occurrence of events. Cameras can be overt or hidden, can record locally or to a cloud storage service, may offer pan-tilt and zoom, may operate in visible or infrared light, maybe triggered by movement and may

support time lapse recording, tracking, facial recognition, gait analysis, object detection or infrared or color filtered recording.

Understand security needs for media storage. Media storage facilities should be designed to store blank media, reusable media and installation media securely. Concerns include theft, corruption and data remnant recovery. Media storage facility protections include using locked cabinets or safes, using a media library or custodian, implementing a check-in and checkout process and using media sanitization.

Understand the concerns of evidence storage. Evidence storage is used to retain logs, drive images, virtual machine snapshots and other datasets for recovery, internal investigations and forensic investigations. Protections include dedicated and isolated storage facilities, offline storage, activity tracking, hash management, access restrictions and encryption. Know the common threats to physical access controls. No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent abuse, impersonation, masquerading, tailgating and piggybacking.

Understand how to control your environment. In addition to power considerations, maintaining the environment involves control over the HVAC mechanisms. Rooms containing primarily computers should be kept at 59 to 89.6 degrees Fahrenheit. Humidity in a computer room should be maintained between 20 and 80%. Too much humidity can cause corrosion, too little humidity causes static electricity.

Understand the need to manage water leakage and flooding. Your environmental safety policy and procedures should address water leakage and flooding. Water and electricity, don't mix. Locate server rooms and critical computer equipment away from any water source or transport pipes whenever possible.

Understand the importance of fire detection and suppression. Protecting personnel from harm should always be the most important goal of any security or protection system. In addition to protecting people, fire detection and suppression are designed to keep damage caused by fire, smoke, heat and suppression materials to a minimum, especially in regard to the IT infrastructure.

Know about physical perimeter security controls. You can control access to a facility with fences, gates, turnstiles, access control vestibules, bollards and barricades.

Know about security guards and guard dogs. Guards can be posted around a perimeter or inside to monitor access points or watch detection and surveillance monitors. Guards are able to adapt and react to various conditions or situations and can learn and recognize attack and intrusion activities and patterns, adjust to a changing environment and make decisions and judgment calls. An alternative to security guards, guard dogs can often be deployed as a perimeter security control and are an extremely effective detection and deterrent control.

Understand how to handle visitors in a secure facility. If a facility employs restricted areas to control physical security, then a mechanism to handle visitors is required. Often, an escort is assigned to visitors and their access and activities are monitored closely. Failing to track outsiders actions when granted access to a protected area can result in malicious activity against the most protected assets.

Understand internal security controls. There are many physical security mechanisms for internal control, including locks, badges, protective distribution systems, motion detectors, intrusion alarms and secondary verification mechanisms. Know the KPIs of physical security. Physical security's key performance indicators should be determined, monitored, recorded and evaluated. KPIs are metrics or

measurements of the operation or failure of various aspects of physical security. Those are the study essentials that you'll need to know for Chapter 10, physical security requirements.

From:
https://trident365.com/ - **三叉戟**

Permanent link:
https://trident365.com/doku.php?id=projects:cissp:chapter10

Last update: **2025/05/18 17:16**