13.1.2 Physical Security Facts

Physical security is the measures taken to protect corporate assets from threats, such as theft or damage. Important aspects of physical security include:

- Restricting physical access to facilities and computer systems.
- Preventing interruptions of computer services caused by problems such as loss of power or fire.
- Preventing unauthorized disclosure of information.
- Disposing of sensitive material.
- Protecting the interior and exterior of your facility.

Control Characteristics

The table below lists several physical control measures and their characteristics.

Control Measure	Characteristics
Perimeter Barriers	For a secure facility, the first physical security measure is to secure the building perimeter and restrict access to only secure entry points. Methods for securing the perimeter provide multiple functions: - Fences provide an environmental barrier that prevents easy access to the facility. - Barricades prevent vehicles from approaching the facility. - Signs inform individuals that they are entering a secured area. - Lighting deters casual intruders, helps guards to see intruders, and is necessary for most cameras to monitor an area. To be effective, lights should be placed to eliminate shadows or dark spots. - Security guards offer the best protection for perimeter security because they can actively respond to a variety of threat situations. Security guards can also reference an *access list* that explicitly lists who can enter a secure facility. However, guards are expensive, require training, and can be unreliable or inconsistent.
Closed-Circuit Television (CCTV)	Closed-circuit television can be used as both a preventative tool (when monitoring live events) or as an investigative tool (when events are recorded for later playback). When CCTV is used in a preventative way, you must have a guard or other person available who monitors one or more cameras. The cameras effectively expand the area that can be monitored by the guard. Video surveillance can detect security breaches, but only guards can prevent and react to security breaches. When choosing a CCTV camera, consider the following features. - Camera specifications: - The *resolution* is rated in the number of lines included in the image. In general, the higher the resolution number, the sharper the image (e.g., 500 resolution). - The focal length measures the magnification power of a lens. The focal length controls the distance that the camera can see, as well as how much detail can be seen at a specific range. A higher focal length lets you see more detail at a greater distance (e.g., 50 mm). - LUX is a measure of the sensitivity to light. The lower the number, the less light needed for a clear image (e.g., .05 LUX). - Cameras models: - Pan-tilt-zoom (PTZ) cameras allow you to manually control the camera and zoom in on specific areas. Some PTZ cameras have an automatic mode that moves the camera between several preset locations. - Bullet cameras have a built-in lenses and are long and round in shape. Most bullet cameras can be used indoors or outdoors. - C-mount cameras have interchangeable lenses and are typically rectangle in shape with the lens on the end. Most c-mount cameras require a special housing to be used outdoors. - Dome cameras are protected with a plastic or glass dome. These cameras are more vandal-resistant than other cameras. - Camera lenses: - Varifocal lenses allow you to zoom the camera in on a location. - Fixed lenses have a set focal length and are unable to zoom.
Doors	Doors can enhance security if they are properly implemented. There are many types of doors, but three are commonly used for security purposes. - A *mantrap* is a specialized entrance with two doors that creates a security buffer zone between two areas. - Once a person enters into the space between the doors, both doors are locked. - To enter the facility, authentication must be provided. This may include visual identification and identification credentials. - Mantraps should permit only a single person to enter, and authentication must be provided by each person. - If authentication is not provided, the intruder is kept in the mantrap until authorities arrive.

	▪ A *turnstile* is a barrier that permits entry in only one direction. ▪ Physical turnstiles are often used to control entry for large events such as concerts or sporting events. ▪ Optical turnstiles use sensors and alarms to control entry. ▪ Turnstiles are often used to permit easy exit from a secure area. Entry is controlled through a mantrap or other system that requires authentication for entry. ▪ A *double-entry door* has two doors that are locked from the outside but have crash bars on the inside that allow easy exit. Double-entry doors are typically used only for emergency exits, and alarms sound when the doors are opened. Regular doors are susceptible to social engineering attacks such as *piggybacking* and *tailgating*. Piggybacking and tailgating are when an attacker enters a secured building by following an authorized employee through a secure door and does not provide identification. Piggybacking usually implies consent from the authorized employee, whereas tailgating implies no consent from the authorized employee. Tailgating tactics include: ▪ Simply following the authorized individual, making it appear that the authorized person is escorting the person who is tailgating. ▪ Joining a group of people, making it appear as if the unauthorized person belongs with the crowd. ▪ Preying on the kindness of the authorized person by coming up with an excuse for a lack of credentials and a need for admission. Problem points that are conducive to tailgating include: ▪ An unmonitored entry point. ▪ High-volume entry points where an unauthorized person may enter undetected.
Door Locks	Door locks allow access only to those with the proper key. Lock types include: ▪ Pick-resistant locks with restricted key duplication are the most secure key lock. It is important to note that all traditional key locks are vulnerable to lock picking. ▪ Keypad locks require knowledge of a code and reduce the threat of lost keys and cards. Clean keypads frequently to remove indications of buttons used. ▪ Electronic systems often use key cards (or ID badges) instead of keys to allow access. ▪ Dumb cards contain limited information. ▪ Smart cards have the ability to encrypt access information. Smart cards can be contact or contactless. Contactless smart cards use the 13.56 MHz frequency to communicate with proximity readers. ▪ Proximity cards, also known as RFID (radio frequency identification) cards, are a subset of smart cards that use the 125 kHz frequency to communicate with proximity readers. Proximity cards differ from smart cards because they are designed to communicate only the card's identity. A smart card can communicate much more information. ▪ Biometric locks increase security by using fingerprints or iris scans. They reduce the threat of lost keys or cards.
Physical Access Logs	Physical access logs are implemented by facility guards and require everyone gaining access to the facility to sign in.
Physical Access Controls	Physical access controls can be implemented inside the facility. ▪ Physical controls may include key fobs, swipe cards, or badges. ▪ To control access to sensitive areas within the facility, require a card swipe or reader. ▪ Some systems can track personnel movement within a facility and proactively lock or unlock doors based on the access token device. ▪ An *anti-passback system* prevents a card holder from passing their card back to someone else. ▪ Physical controls are often implemented with sensors and alarms to detect unauthorized access. ▪ *Photoelectric* sensors detect motion and are better suited to detecting a perimeter breach than interior motion detection. ▪ Wave pattern, heat sensing, and ultrasonic sensors are all better suited for interior motion detection than perimeter breach detection.
Asset Control	You can secure company equipment using asset tracking tags with tamper detection. *Asset tracking tags* contain company information, such as name, address, and a serial number. They identify company assets if found and may include a tracking device that allows them to be found and retrieved, if necessary. *Tamper detection* triggers a notification, in real time, if tags are removed or tampered with.

Layered Defense

When designing physical security, implement a *layered defense* system. A layered defense system implements controls at each layer to ensure that defeating one level of security does not allow an attacker subsequent access. Using multiple types of security controls within the same layer further enhances security. Tips for implementing a multi-layered defense system include:

- Protect entry points with a card access system (or some other type of control) as well as a security camera.

- Use a reception area to prevent the public, visitors, or contractors from entering secure areas of the building without an escort.
- Use the card access or other system to block access to elevators and stairwells. This will prevent someone who successfully tailgates from gaining further access.
- Use a different access system to secure offices or other sensitive area such as key locks, keypad locks, or biometric controls.
- Implement security within offices and data centers by locking storage areas and using computer passwords.
- Use cable locks on mobile computer devices, such as laptops and tablets. Cable locks secure mobile devices to stationary objects (such as desks or walls) and help prevent theft.
- Employ a hardware checkout policy to ensure that hardware containing sensitive data does not leave the organization's premises without approval. Before hardware is removed from the premise, the device's serial number, make, and model number should be recorded.

TestOut Corporation All rights reserved.