

3.2.2 Physical Security Facts

Physical security is the protection of corporate assets (including property, facilities, equipment, and personnel) from damage, theft, or harm. Physical security inspections should be performed quarterly. Violations should be addressed in a formal manner, with warnings and penalties.

This lesson covers the following topics:

- Security factors
- Security aspects
- Physical controls
- Security sequence
- Layered defense

Security Factors

There are three factors to keep in mind with physical security:

- *Prevention* is taking safeguards to protect property, facilities, equipment, and personnel. The safeguards should deter an attack.
- *Detection* is identifying the extent of damage, theft, or harm.
- *Recovery* is the implementation of security procedures to minimize the impact of an attack and repair any damage in order to get the organization operational again. It also involves hardening the physical security of the organization against future problems.

Security Aspects

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 the facility.

Physical Controls

The following table lists physical control measures and characteristics.

Control Measure	Characteristics
Perimeter barriers	<p>The first measure in physically securing a building is to secure the perimeter and restrict access to only secure entry points. Methods for securing the perimeter include:</p> <ul style="list-style-type: none"> ▪ Fences to provide an environmental barrier that prevents easy access to the facility. <ul style="list-style-type: none"> ▪ A low fence (3-4 feet) acts as a deterrent to casual intrusion. ▪ A higher fence (6-7 feet) acts as a deterrent unless the trespasser has a specific intent to violate security. ▪ A fence 8 feet or higher topped with barbed wire is an effective deterrent. ▪ Barricades and bollards can be erected to prevent vehicles from approaching the facility. ▪ Signs should be posted to inform individuals that they are entering a secured area. ▪ Guard dogs are generally highly reliable, but are appropriate only for physical perimeter security. They can be expensive to keep and maintain. Their use might raise issues of liability and insurance. ▪ Lighting deters casual intruders, helps guards see intruders, and is necessary for most cameras to monitor the 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 <i>access list</i>, which explicitly lists who can enter a secure facility. However, guards are expensive, require training, and can be unreliable or inconsistent.
Closed-circuit television (CCTV)	<p>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). Camera types include the following:</p> <ul style="list-style-type: none"> ▪ A <i>bullet</i> camera has a built-in lens and is long and round in shape. Most bullet cameras can be used indoors or outdoors. ▪ A <i>c-mount</i> camera has interchangeable lenses and is typically rectangular in shape with the lens on the end. Most c-mount cameras require a special housing to be used outdoors. ▪ A <i>dome</i> camera is a camera protected with a plastic or glass dome. These cameras are more vandal-resistant than other cameras. ▪ A pan tilt zoom (PTZ) camera can dynamically move the camera and zoom in on specific areas. Cameras without PTZ capabilities are manually set looking toward a specific direction. <i>Automatic</i> PTZ mode automatically moves the camera between several preset locations; <i>manual</i> PTZ lets an operator remotely control the position of the camera. <p>When selecting cameras, be aware of the following characteristics:</p>

	<ul style="list-style-type: none"> ▪ The <i>focal length</i> 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. ▪ The focal length is expressed in millimeters (mm). A higher focal length lets you see more detail at a greater distance. ▪ Most cameras have a 4 mm lens with a range of 30-35 feet, allowing you to see facial features at that distance. ▪ A <i>fixed</i> lens camera has a set focal length. A <i>varifocal</i> camera lens lets you adjust the focus (zoom). ▪ A 70-degree view angle is the largest view angle possible without image distortion. ▪ The <i>resolution</i> is rated in the number of lines (such as 400) included in the image. In general, the higher the resolution, the sharper the image. ▪ LUX is a measure of the sensitivity to light. The lower the number, the less light is necessary for a clear image. ▪ Infrared cameras can record images in little or no light. Infrared cameras have a range of about 25 feet in no light and further in dimly-lit areas. <p>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. Cameras can detect only security breaches. Guards can prevent and react to security breaches.</p>
Doors	<p>Doors can enhance security if they are properly implemented. Specific door types include the following:</p> <ul style="list-style-type: none"> ▪ A <i>mantrap</i> is a specialized entrance with two doors that create a security buffer zone between two areas. <ul style="list-style-type: none"> ▪ Once a person enters into the space between the doors, both doors are locked. ▪ To enter the facility, authentication must be provided. Authentication may include visual identification and identification credentials. ▪ Mantraps should permit only a single person to enter, and each person must provide authentication. ▪ If authentication is not provided, the intruder is kept in the mantrap until authorities arrive. ▪ A <i>turnstile</i> is a barrier that permits entry in only one direction. <ul style="list-style-type: none"> ▪ Physical turnstiles are often used to control entry for large events such as concerts and 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 <i>double-entry door</i> 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. Alarms sound when double-entry doors are opened. <p>Regular doors are susceptible to social engineering attacks such as <i>piggybacking</i>, or <i>tailgating</i>, where an unauthorized person follows an authorized person through a door. Mantraps and turnstiles that permit only a single person to enter and require individual authentication are effective deterrents to piggybacking.</p>
Door locks	<p>Door locks allow access only to people with the proper key. Lock types are explained in the following list.</p> <ul style="list-style-type: none"> ▪ <i>Pick-resistant locks</i> 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 (shimming). ▪ <i>Keypad locks</i> require knowledge of a code and reduce the threat of lost keys and cards. Keypads should be cleaned frequently to remove indications of buttons used. ▪ Electronic systems often use <i>key cards</i> (or ID badges) instead of keys to allow access. <ul style="list-style-type: none"> ▪ <i>Dumb cards</i> contain limited information. ▪ <i>Smart cards</i> 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 <i>proximity readers</i>. ▪ <i>Proximity cards</i>, also known as radio frequency identification (RFID) 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. ▪ <i>Biometric locks</i> increase security by using fingerprints or iris scans. They reduce the threat of lost keys or cards.
Physical access logs	<p>Physical access logs are implemented by a facility's guards and require everyone gaining access to the facility to sign in up on entry.</p>
Physical access controls	<p>Physical access controls can be implemented inside the facility in the following ways.</p> <ul style="list-style-type: none"> ▪ Physical controls may include key fobs, swipe cards, or badges. ▪ Physical controls may include biometric factors such as fingerprint scanners, retinal scanners, iris scanners, voice recognition, and facial recognition. <ul style="list-style-type: none"> ▪ The <i>false acceptance rate</i> (FAR) refers to the likelihood that an unauthorized user will incorrectly be given access. ▪ The <i>false recognition rate</i> (FRR) refers to the likelihood that an authorized user will incorrectly be rejected and denied access. ▪ Both the FAR and FRR are influenced by the biometric scanners threshold settings. The <i>crossover error rate</i> (CER) is the rate at which the FAR becomes equal to the FRR after adjusting the threshold. The lower the CER, the better the biometric system. ▪ 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 each person's access token device. ▪ An <i>anti-passback system</i> prevents a card holder from passing a card back to someone else. ▪ Physical controls are often implemented along with sensors and alarms to detect unauthorized access. <ul style="list-style-type: none"> ▪ <i>Photoelectric</i> sensors detect motion and are better suited to detect 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.

Employee and visitor safety	<p>As you implement physical security, be sure to keep the safety of employees and visitors in mind. Consider the importance of the following actions:</p> <ul style="list-style-type: none"> ■ Implement adequate lighting in parking lots and around employee entrances. ■ Implement emergency lighting that runs on protected power and automatically switches on when the main power goes off. ■ Implement fail-open locking systems that allow employees to exit your facility quickly in the event of an emergency. ■ Devise escape plans that utilize the best escape routes for each area in your organization. Post these escape plans in prominent locations. ■ Conduct emergency drills to verify that the physical safety and security measures you have implemented function correctly.
Protected distribution system	<p>A <i>protected distribution system</i> (PDS) encases network cabling within a <i>carrier</i>. This enables data to be securely transferred directly between two high-security areas through an area of lower security. Three types of PDS are most frequently implemented:</p> <ul style="list-style-type: none"> ■ In a <i>hardened carrier PDS</i>, network cabling is run within metal conduit. All conduit connections are permanently welded or glued to prevent external access. To identify signs of tampering, regular visual inspections of the carrier should be conducted. ■ In an <i>alarmed carrier PDS</i>, an electronic alarm system replaces the welds and/or glue used to secure a hardened carrier. The electronic alarm system can detect attempts to compromise the carrier and access the protected cable within it. ■ In a <i>continuously viewed carrier PDS</i>, security guards continuously monitor the carrier to detect any intrusion attempt by attackers.

Security Sequence

Physical security should deploy in the following sequence. If a step in the sequence fails, the next step should implement itself automatically.

1. Deter initial access attempts.
2. Deny direct physical access.
3. Detect the intrusion.
4. Delay the violator to allow for response.

Layered Defense

When designing physical security, implement a *layered defense* system. A layered defense system is one in which controls are implemented 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 the following:

- 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 such as key locks, keypad locks, or biometric controls to secure offices or other sensitive areas.
- Implement security within offices and data centers using locking storage areas and computer passwords.

TestOut Corporation All rights reserved.