4.1.3 Physical Security Facts

Physical security is the protection of corporate assets from threats such as theft or damage. There are three factors to keep in mind with physical security:

- *Prevention* is making the location less tempting to break into.
- *Detection* is identifying what was broken into, what is missing, and the extent of the damage.
- *Recovery* is the review of the physical security procedures, repairing any damage, and hardening the physical security of the company against future problems.

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

The table below lists physical control measures and their characteristics:

Control Measure	Characteristics

Perimeter Barriers	The first measure in physically securing a building is to secure theperimeter and restrict access to only secure entry points. Methods for securing the perimeter are explained in the following list:
	- Fences provide an environmental barrier that prevents easy access to the facility.
	  - 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, and 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 *access list*, 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)	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:
	- A *bullet* camera, which has a built-in lens and is long and round in shape. Most bullet cameras can be used indoors or outdoors.
	- A *c-mount* camera, which has interchangeable lenses and is typically rectangle in shape with the lens on the end. Most c-mount cameras require a special housing to be used outdoors.
	- A *dome* camera, which 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, which lets you dynamically move the camera and zoom in on specific areas (cameras without PTZ capabilities are manually set looking toward a specific direction). *Automatic* PTZ mode automatically moves the camera between several preset locations; *manual* PTZ lets an operator remotely control the position of the camera.
	When selecting cameras, be aware of the following characteristics:
	- 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.
	  - 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 *fixed* lens camera has a set focal length. A *varifocal* camera lens lets you adjust the focus (zoom).
	- A 70 degree view angle is the largest view angle possible without distorting the image.
	- The *resolution* 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.
	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 only detect security breaches: Guards can prevent and react to security breaches.

Doors	Doors can enhance security if they are properly implemented. Specific door types include:
	▪ A *mantrap*, which is a specialized entrance with two doors that create 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. 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 *turnstile*, which is a barrier that permits entry in only one direction.
	  ▪ 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 *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*, or tailgating, where an unauthorized person asks an authorized person to hold the door. Mantraps and turnstiles that permit only a single person and require individual authentication are effective deterrents to piggybacking.

Door Locks	Door locks only allow access to people with the proper key. Lock types are explained in the following list:
	▪ *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 (shimming).
	▪ *Keypad locks* require knowledge of a code and reduce the threat from 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 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.
	▪ *Biometric locks* increase security by using fingerprints or iris scans. They reduce the threat from lost keys or cards.

Physical Access Logs	Physical access logs are implemented by the guards of a facility 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.
	▪ Physical controls may include biometric factors such as fingerprint scanners, retinal scanners, iris scanners, voice recognition and facial recognition.
	  ▪ The false acceptance rate (FAR) is likelihood that an unauthorized user will incorrectly be given access.
	  ▪ The false recognition rate (FRR) is the likelihood that an authorized user will incorrectly be rejected and not be given access.
	  ▪ Both the FAR and FRR are influenced by the biometric scanners threshold settings. The crossover error rate (CER) is the rate when 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 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 along with sensors and alarms to detect unauthorized access.
	  ▪ *Photoelectric* sensors detect motion and are best suited to detect a perimeter breach rather 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	As you implement physical security, be sure to keep the safety of employees and visitors in mind. Consider the importance of the following actions: ▪ 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	

Cable Distribution	A protected distribution system (PDS) encases network cabling within a *carrier*. This enables data to be securely transferred directly between two high-security areas through an area of lower security. Three different types of PDS are most frequently implemented: ▪ In a *hardened carrier PDS*, 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 *alarmed carrier PDS*, the welds and/or glue used to secure a hardened carrier are replaced with an electronic alarm system that can detect attempts to compromise the carrier and access the protected cable within it. ▪ In a *continuously viewed carrier PDS*, security guards continuously monitor the carrier to detect any intrusion attempt by attackers.

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.

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:

- 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.

Perform physical security inspections quarterly. Violations should be addressed in a formal manner, with warnings and penalties imposed.

TestOut Corporation All rights reserved.