3.2.4 Physical Security Attack Facts

Planning, preparation, and prevention for physical security threats must be taken into consideration to protect an organization's data and systems. The National Institute of Standards and Technology (NIST) has a special publication, NIST SP 800-53, that details security controls and assessment procedures to protect the integrity of information systems.

This lesson covers the following topics:

- Environmental threats
- Threats to assets and property
- Facility breaches
- Physical attacks

Environmental Threats

The following table describes some of the environmental threats an organization may encounter.

Threat	Description
Flood	Flooding can occur for a variety of reasons, including heavy rains, overflowing rivers, broken dams, urban drainage basins, storm surges, broken pipes, and lack of vegetation.
Fire	Fires are a common environmental threat. There are many controls available that, if properly implemented, help reduce fire damage and diminish their threat to physical security.
Hurricane and tornado	Hurricanes and tornadoes are intense weather events that can be extremely destructive. They often disrupt services, such as electricity and communications networks, and prevent facility access.
Tsunami	Tsunamis are caused by underwater earthquakes, volcanic eruptions, or other events that results in the displacement of large volumes of water. Tsunami waves can be tens of feet high and cause an immense amount of destruction.
Earthquake	Earthquakes result from the seismic shift of tectonic plates moving along fault lines. Shaking ground, ruptured ground, and landslides can destroy buildings, cause dams to collapse, and ignite ruptured gas lines.
Other natural disasters	Other natural disasters include wind storms, electrical storms, blizzards, and other types of extreme weather.

Threats to Assets and Property

Threats to assets and property can be posed by those external to the organization as well as insiders. The table below describes some of these threats.

Threat	Description
Theft	Theft of an organization's assets can be very detrimental. For example if an employee's laptop is stolen, it’s not only inconvenient for the employee but also any plans, projects, and other sensitive data that might be on that laptop could be leaked or used against the organization. The more important the position of the employee within the organization, the more serious the theft is.
Vandalism	Vandalism is damaging, defacing, or destroying someone else's property. Vandalism can be done by resentful employees or ex-employees; someone with a political agenda or vendetta against the organization; or for other reasons.
Destruction	Destruction is similar to vandalism, but it aims to completely destroy the organization’s assets. This kind of malicious act could result in significant loss for the organization.

Facility Breaches

The following table describes a few techniques an attacker can use to gain access to a facility.

Technique	Description
Bump keys	A bump key is cut to the number nine position, which is the lowest possible cut. When the bump key goes inside the lock, the hacker puts a little bit of pressure on the back of the key by either bumping or tapping it. Doing this makes the pins jump inside of the cylinder, creating a temporary shear line that allows enough time for the intruder to quickly turn the lock.
Lock	Lock picking involves manipulating the lock’s components to open it without a key. A attacker only needs a tension wrench and a

picking	pick. A tension wrench is a small, L-shaped tool available in several thicknesses and sizes. A pick is a small, angled, and pointed tool.
Scrubbing	One of the most common ways to pick a lock is called scrubbing. This method involves holding the lock with the tension wrench while quickly scraping the pins with the pick. Some of the pins are placed in a mechanical bind and become stuck in the unlocked position. With practice, an attacker can do this very easily. When all the pins stick, the lock is disengaged.
Lock shim	Another technique uses lock shims. This tool is, basically, a thin, stiff piece of metal that can be inserted into the latch of the padlock.
Badge cloning	Many employee ID badges use an RFID chip to access their office and other parts of their organization's building. However, this kind of chip can be easily copied to another card. To do this, all an attacker needs is a high-frequency antenna to capture a card's frequency, a card read/write device, a legitimate card, and a blank card. The attacker gets close enough to the legitimate card to read it. Once the card information is read, the attacker can easily clone it.

Physical Attacks

The table below describes some physical attacks:

Attack	Description
Cold boot attack	In the cold boot attack, the attacker enters the facility and extracts data remanence from RAM that might still be available before the system is completely powered off.
BIOS access attack	BIOS attacks have been around for a long time, but should not be overlooked. This attack usually involves changing the boot order on a PC so that the hacker can gain access to the computer by bypassing the installed operating system.