Physical Security Quick Study Guide

Jerry Scott
For CISSP 2013
Your Physical Workspace

General Goals: 1) People Safety First, get HVAC on, 2) Set up a Layered Defense in Depth system

Your Building Controls

- Mantrap and Turnstiles at Entrance
- Login Sheets, Badges, Elevator Passes, Office Keys
- CCTV, Doors, Locks, Windows
- Special Controls on Server Rooms
- Fire Extinguishers, Sprinklers, Alarms

Your Office Environment

- Special Keys and Badges
- Motion Sensors
- CCTV
- Shredder
- Media Destruction

Physical Security Quick Study Guide  Jerry Scott

**Threats to Physical Security:** Natural or Environmental, Utilities, Circumstantial, and Human or Man Made. Circumstantial is a human or made threat that you have no control over.

**Threat Sources:** External activists, Staff, Intelligence agents/ Governments, Petty Criminals

<table>
<thead>
<tr>
<th>Threat</th>
<th>Control</th>
<th>Threat</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>Locks, Special doors and Windows</td>
<td>Espionage</td>
<td>Background Checks</td>
</tr>
<tr>
<td>Dumpster diving</td>
<td>Proper disposal efforts</td>
<td>Social Engineering</td>
<td>Training and Awareness</td>
</tr>
<tr>
<td>Shoulder surfing</td>
<td>Screen Filters</td>
<td>HVAC Access</td>
<td>Monitors/Sensors</td>
</tr>
</tbody>
</table>

**Location Issues:** Layout, Design, Age and Condition of Facilities, Access to Emergency services, such as fire, Security, Location visibility and Controlled Access, Public Transportation issues

**Location Countermeasures/Controls:** Physical, Environmental, and Technical

**Basic Control** is to build in Defense in Depth.
CPTED Principle #1 Natural Surveillance "See and be seen" is the overall goal when it comes to CPTED and natural surveillance. A person is less likely to commit a crime if they think someone will see them do it. Lighting and landscape play an important role in Crime Prevention Through Environmental Design.

CPTED Principle #2 Natural Access Control Natural Access Control is more than a high block wall topped with barbed wire. CPTED utilizes the use of walkways, fences, lighting, signage and landscape to clearly guide people and vehicles to and from the proper entrances. The goal is not necessarily to keep intruders out, but to direct the flow of people while decreasing the opportunity for crime.

CPTED Principle #3 Territorial Reinforcement Creating or extending a "sphere of influence" by utilizing physical designs such as pavement treatments, landscaping and signage that enable users of an area to develop a sense of proprietorship over it is the goal of this CPTED principle. Public areas are clearly distinguished from private ones. Potential trespassers perceive this control and are thereby discouraged.

CPTED Principle #4 Maintenance The "Broken Window Theory" suggests that one "broken window" or nuisance, if allowed to exist, will lead to others and ultimately to the decline of an entire neighborhood. Neglected and poorly maintained properties are breeding grounds for criminal activity. We will work with you to develop a formal CPTED based maintenance plan to help you preserve your property value and make it a safer place.
Perimeter Security

First Line of Defense. **Barriers** could be natural or structural. **Controlled access points** are gates and fences, which form a primary wall, and **bollards**, which may be removable.

**Fence Heights:** 1 Meter or 3-4 feet will deter casual trespassers, 2 M or 6-7 feet is too high to climb easily, 2.5 M will delay the determined intruder. In high security areas, a barbed wire top guard should be 2-3 feet. **Fences may be restricted** by local regulations, but should be inspected to ensure they are still properly working to deter intruders. **No parking should be allowed near fences.**

**Perimeter and Space Detection Systems** Lots of forms. Photoelectric, ultrasonic, microwave, passive infrared, pressure sensitive, sounds and vibration, electrical circuits, and motion sensors.

**CCTV systems** are used inside and outside buildings. **CCTV systems must be able to detect, recognize, and identify people.** Pan and tilt cameras allow CCTV systems to be more versatile. Virtual CCTV systems are dummy units meant to deter. Make sure your CCTV systems can survey all that you need them to, and are of the proper size, height, and depth, and that there is sufficient lighting and contrast so that images are recognizable. Care must be taken to make sure that stored CCTV footage is available when needed.

**Guards add a human deterrent to surveillance,** but they can be bribed. Guards often work for third party security firms, so proper guard training must be done. Guard stations provide a deterrent, but can also be a mixed blessing, especially if they are easily compromised. Turnstiles and Mantraps are effective barriers to quick entry by trespassers.
Building and Inside Security

**Doors**

Doors play a key role in building security, isolating a building from its exterior and within the building, isolating specific areas. Doors should be properly lighted and can be controlled by contact devices, even sometimes remotely controlled. In designing doors, remember that protection of human life is important. Doors should be solid core, and not hollow core. They should not open out except as required by building codes. Exterior door locks should provide both daytime for when a room is occupied and 24 hour locks, such as deadbolts. Door frames should be permanently fixed to the adjoining wall studs, and doors should be fixed to building frames with a minimum of 3 hinges. Emergency exit doors should be clearly marked and equipped with panic bars to permit rapid access. You should decide which doors are to be monitored and that they can provide entry and exit in case of a power failure.

**Access and Visitor Logs** – Any visitor entering a secure area should be escorted. Visitor cars should be given window tags. Visitor logs allow visitors to sign in and out and should require authentication before a visitor is added to the list. Emergency personnel will often use visitor logs to try to find missing people in emergencies, or when a building is being shut down at the end of a work day. Temporary badges are useful for visitors and can be helpful on reissuing badges to visitors who come back frequently.

**Locks**

3 kinds, Keyed (something you have), Combinations (Something you know), and Biometric, something you are. Keyed locks have a body, strike, strike plate, a key, and a cylinder. Managing lock keys is important, as you need to know who has access to the keys, who has the keys, what type of lock inventory is available. You also need to secure unused locks and remove default settings from locks.

**Lock terms:** Fail-Soft – the lock in unlocked; Fail-Secure – the lock is locked, and Fail-Safe In an emergency, the lock will allow people to exit as opposed to keeping the building secure. Lock Attacks – Lock Picking and Lock Bumping. If you use electronic cards to enter, you need to guard card access. If you are using biometric methods, you need to ensure that the personal images, etc., needed for these methods are securely stored.
Windows, Internal IDS Systems, Lighting, and Secure Areas

Windows and Glass Types: In high security areas, windows should be meshed. Types of Glass: Plate glass – worst in terms of breakage and security, but cheapest; Tempered Glass – 5 to 7 times better than plate glass, but more expensive; Acrylic materials – better than laminate but also more expensive; Polycarbonate windows – strongest form of glass, also most expensive. Polycarbonate is used in high security areas. Sometimes solar film is useful to remove heat from the direct sun, and to obscure the outside view. Some solar films are helpful in preventing bomb blast damage. Wired glass is also helpful here, and can be placed on a window or window frame to detect breakage or window opening.

Internal IDS Systems – common tools are CCTV and Sensors and Monitors.

Common Lighting Types – continuous lighting, trip lighting, standby or backup lighting, emergency egress lighting, and infrared or night vision lighting.

Secure Operations areas: Equipment room – you need a perimeter enclosure, locks and other electronic controls for critical equipment rooms. You also need BCP policy and procedures for who enters what rooms, especially in emergency situations. Data Processing Facility – also usually enclosed with a perimeter. These rooms are often called server rooms, mainframe rooms or storage rooms. Sometimes people enter these secure rooms with small devices, such as I-Phones, digital cameras, or high capacity plug in USB disk drives. This can be a real security problem. Communications racks and devices must also be protected. Wireless devices must be carefully placed to avoid allowing outsiders to gain privileged information. Enterprise Network Access Control devices, such as Layer 2 Switches must be guarded as well, as hackers can easily cause lots of havoc by changing switch ports of different cables. For physical protection, cabling should be run in conduit.
Access to Special Places

Access to utility rooms and special work areas for system administrators and operators should be carefully guarded. To protect sensitive equipment, a proper inventory must be kept, with locks and tracing equipment. Sensitive data should be encrypted, and unused I/O ports on Layer 2 devices should be disabled. Some environmental threats are

<table>
<thead>
<tr>
<th>System</th>
<th>Threat</th>
<th>System</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electric Power</td>
<td>Power Loss</td>
<td>HVAC</td>
<td>Overheating</td>
</tr>
<tr>
<td>Water/Plumbing</td>
<td>Flooding/Dripping</td>
<td>Gas</td>
<td>Explosion</td>
</tr>
<tr>
<td>Refrigeration</td>
<td>Leaking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fire Protection:** Prevention, Detection, Suppression. A Fire needs three legs to burn – Fuel, Heat, and Oxygen. Fire prevention efforts try to remove one of the three legs. Water reduces Heat, Purple K is a dry powder the fire dept. uses to bind with solid objects, and CO2 can displace oxygen, but CO2 can be lethal. There are five categories of fires: Class A, common combustibles such as wood, paper, etc., Class B, flammable and combustible liquids, Class C, Electrical equipment, and Class D, metals. Remember CLEM, C for class A and combustibles, L for Class B and Liquids, E for Class C and Electrical, and M for Class D and Metals. Class K fires are kitchen fires.

**Flooding Area Coverage** Water may damage lots of equipment, while Halon/CO2/Argon can be lethal. Halon systems are problematic and a 1985 agreement, called the Montreal agreement, said that no new Halon systems would be installed but buildings with existing systems could use them, but had to get replacements from authorized dealers.
Electrical Power and Infrastructure Problems

**Power Problems: Terms** -- Complete Loss, Blackout, or a Fault, a momentary loss. **Power degradation terms**: Brownout, Sag or DIP, Surge, Transients, In-Rush current, and Electrostatic discharge. **Power Interference** – EMI and RFI. **Power Grounding Issues**.

**Protecting Power** – **UPS** – only stay up for a few minutes, used to power down machines normally; **Line Conditioners** – goal is to provide clean power; **Generators** – come on quickly or automatically when power fails. UPS holds power until generator can come on.

**Power Controls** – **Emergency Power Off Switch**, **Power Line Monitors** – most power companies charge you for the maximum load in small increments, such as 15 minutes. If you turn on all your machines at the same time, this will be a power spike and many power companies will charge you 7 by 24 for that amount of power. **Rule** – turn on machines serially. **Total Load Monitors** help you know your power uses so you can know the best sequence to start different machines.

**HVAC Issues** HVAC controls should be separate from those for the building at large. HVAC considerations: **Location** – independence of the data center air conditioning from the rest of the building; **Positive Pressure** is applying more pressure to constantly ensure that air is being forced from the environmentally controlled area (quality, humidity, temperature) to one that is not as environmentally controlled. You must also maintain building temperature, Humidity Levels, and Air Quality and have documented maintenance procedures.

**Other Infrastructure Threats** – **Vermin** – can be a health hazard; **Electromagnetic fields** – can affect data transfer lines (EMI), and **Excess Vibration** – can happen from many sources; if it does move equipment racks to safer locations.