Apply Secure Principles to Site and Facility Design

**Secure Facility Plan**

**A secure facility plan outlines the security needs of your organization and emphasizes methods or mechanisms to employ to provide security. Such a plan is developed through a process known as *critical path analysis***.

**When critical path analysis is performed properly, a complete picture of the interdependencies and interactions necessary to sustain the organization is produced. Once** that analysis is complete, its results serve as a list of items to secure. The first step in designing a secure IT infrastructure is providing security for the basic requirements of the organization and its computers. These basic requirements include electricity, environmental controls (in other words, a building, air conditioning, heating, humidity control, and so on), and water/ sewage.

While examining for critical paths, it is also important to evaluate completed or potential technology convergence. **Technology convergence is the tendency for various technologies, solutions, utilities, and systems to evolve and merge over time. Often this results in** multiple systems performing similar or redundant tasks or one system taking over the feature and abilities of another. While in some instances this can result in improved efficiency and cost savings, it can also represent a single point of failure and become a more valuable target for hackers and intruders. For example, if voice, video, fax, and data traffic all share a single connection path rather than individual paths, a single act of sabotage to the main connection is all that is required for intruders or thieves to sever external communications.

**Site Selection**

Site selection should be based on the security needs of the organization. Cost, location, and size are important, but addressing the requirements of security should always take precedence. When choosing a site on which to build a facility or selecting a preexisting structure, be sure to examine every aspect of its location carefully. Securing assets depends largely on site security, which involves numerous considerations and situational elements. Site location and construction play a crucial role in the overall site selection process. Susceptibility to riots, looting, break-ins, and vandalism or location within a high-crime area are obviously all poor choices but cannot always be dictated or controlled. Environmental threats such as fault lines, tornado/hurricane regions, and close proximity to other natural disasters present significant issues for the site selection process as well because you can’t always avoid such threats.

**Visibility**

Visibility is important. What is the surrounding terrain? Would it be easy to approach the facility by vehicle or on foot without being seen? The makeup of the surrounding area is also important. Is it in or near a residential, business, or industrial area? What is the local crime rate? Where are the closest emergency services located (fi re, medical, police)? What unique hazards may be found in the vicinity (chemical plants, homeless shelters, universities, construction sites, and so on)?

**Natural Disasters**

Another concern is the potential impact that natural disasters could make in the area. Is it prone to earthquakes, mudslides, sinkholes, fi res, floods, hurricanes, tornadoes, falling rocks, snow, rainfall, ice, humidity, heat, extreme cold, and so on? You must prepare for natural disasters and equip your IT environment to either survive an event or be replaced easily.

**Facility Design**

Important issues to consider include combustibility, fi re rating, construction materials, load rating, placement, and control of items such as walls, doors, ceilings, flooring, HVAC, power, water, sewage, gas, and so on. Forced intrusion, emergency access, resistance to entry, direction of entries and exits, use of alarms, and conductivity are other important aspects to evaluate. Every element within a facility should be evaluated in terms of how it could be used for and against the protection of the IT infrastructure and personnel

There’s also a well-established school **of thought on “secure architecture” that’s often-called crime prevention through environmental design (CPTED). The guiding idea is to structure the physical environment and surroundings to influence individual decisions that potential offenders make before committing any** **criminal acts**. The International CPTED Association is an excellent source for information

**Administrative physical security controls include facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures. Technical physical security controls include access controls; intrusion detection; alarms; closed-circuit television (CCTV); monitoring; heating, ventilating, and air conditioning (HVAC); power supplies; and fi re detection and suppression. Physical controls for physical secuity include fencing, lighting, locks, construction materials, mantraps, dogs, and guards.**

**When designing physical security for an environment, focus on the functional order in which controls should be used. The order is as follows:**

**1. Deterrence**

**2. Denial**

**3. Detection**

**4. Delay**

**Security controls should be deployed so that initial attempts to access physical assets are deterred (boundary restrictions accomplish this). If deterrence fails, then direct access to physical assets should be denied (for example, locked vault doors). If denial fails, your system needs to detect intrusion (for example, using motion sensors), and the intruder should be delayed sufficiently in their access attempts to enable authorities to respond (for example, a cable lock on the asset). It’s important to remember this order when deploying physical security controls: first deterrence, then denial, then detection, then delay.**

**hardware should be scheduled for replacement and/or repair. The schedule for such operations should be based on the mean time to failure (MTTF) and mean time to repair (MTTR) estimates established for each device or on prevailing best organizational practices for managing the hardware life cycle. MTTF is the expected typical functional lifetime of the device given a specific operating environment. MTTR is the average length of time required to perform a repair on the device. A device can often undergo numerous repairs before a catastrophic failure is expected. Be sure to schedule all devices to be replaced before their MTTF expires. An additional measurement is that of the mean time between failures (MTBF). This is an estimation of the time between the first and any subsequent failures. If the MTTF and MTBF values are**

**the same or fairly similar, manufacturers often only list the MTTF to represent both values. When a device is sent out for repairs, you need to have an alternate solution or a backup device to fill in for the duration of the repair time. Often, waiting until a minor failure occurs before a repair is performed is satisfactory, but waiting until a complete failure occurs before replacement is an unacceptable security practice.**

**Wiring Closets**

Wiring closets used to be a small closet where the telecommunications cables were organized for the building using punch-down blocks. Today, a wiring closet is still used for organizational purposes, but it serves as an important infrastructure purpose as well. A modern wiring closet is where the networking cables for a whole building or just a floor are connected to other essential equipment, such as patch panels, switches, routers, LAN extenders, and backbone channels. A more technical name for wiring closet is *premises wire distribution room* . It is fairly common to have one or more racks of interconnection devices stationed in a wiring closet.

**Wiring closet security is extremely important. Most of the security for a wiring closet focuses on preventing physical unauthorized access. If an unauthorized intruder gains access to the area, they may be able to steal equipment, pull or cut cables, or even plant a listening device.**

**Server Rooms**

**Server rooms, datacenters, communications rooms, wiring closets, server vaults, and IT closets are enclosed, restricted, and protected rooms where your mission-critical servers and network devices are housed. Centralized server rooms need not be human compatible. In fact, the more human incompatible a server room is, the more protection it will offer against casual and determined attacks. Human incompatibility can be accomplished by including Halotron, PyroGen, or other halon-substitute oxygen-displacement fi re detection and extinguishing systems, low temperatures, little or no lighting, and equipment stacked with little room to maneuver. Server rooms should be designed to support**

**optimal operation of the IT infrastructure and to block unauthorized human access or intervention.**

**Media Storage Facilities**

Media that is reused, such as thumb drives, flash memory cards, or portable hard drives, should be protected against theft and data remnant recovery. Data remnants are the remaining data elements left on a storage device after a standard deletion or formatting process. Such a process clears out the directory structure and marks clusters as available for use but leaves the original data in the clusters. A simple un-deletion utility or data recovery scanner can often recover access to these fi les. Restricting access to media and using secure wiping solutions can reduce this risk.

Installation media needs to be protected against theft and malware planting. This will ensure that when a new installation needs to be performed, the media is available and safe for use.

Here are some means of implementing secure media storage facilities:

■ Store media in a locked cabinet or safe.

■ Have a librarian or custodian who manages access to the locked media cabinet.

■ Use a check-in/check-out process to track who retrieves, uses, and returns media from storage

■ For reusable media, when the device is returned, run a secure drive sanitization or zeroization (a procedure that erases data by replacing it with meaningless data such as zeroes) process to remove all data remnants.

**For more security-intensive organizations, it may be necessary to place a security notification label on media to indicate its use classification or employ RFID/NFC asset tracking tags on media. It also might be important to use a storage cabinet that is more like a safe than an office supply shelf.**

**Evidence Storage**

Evidence storage is quickly becoming a necessity for all businesses, not just law enforcement– related organizations. As cybercrime events continue to increase, it is important to retain logs, audit trails, and other records of digital events

**Smartcards**

**Smartcards are credit-card-sized IDs, badges, or security passes with an embedded magnetic strip, bar code, or integrated circuit chip. They contain information about the authorized bearer that can be used for identification and/or authentication purposes. Some** smartcards can even process information or store reasonable amounts of data in a memory chip. A smartcard may be known by several phrases or terms:

■ An identity token containing integrated circuits (ICs)

■ A processor IC card

■ An IC card with an ISO 7816 interface

**Memory cards are machine-readable ID cards with a magnetic strip. Like a credit card, debit card, or ATM card, memory cards can retain a small amount of data but are unable to process data like a smartcard. Memory cards often function** as a type of two-factor control: the card is “something you have” and its PIN is “something you know.” However, memory cards are easy to copy or duplicate and are insufficient for authentication purposes in a secure environment.

**Proximity Readers**

In addition to smart/dumb cards, proximity readers can be used to control physical access. A proximity reader can be a passive device, a field-powered device, or a transponder. The proximity device is worn or held by the authorized bearer. When it passes a proximity reader, the reader is able to determine who the bearer is and whether they have authorized access. A passive device reflects or otherwise alters the electromagnetic field generated by the reader. This alteration is detected by the reader. The passive device has no active electronics; it is just a small magnet with specific properties (like antitheft devices commonly found on DVDs). A field-powered device has electronics that activate when the device enters the electromagnetic field that the reader generates. Such devices actually generate electricity from an EM field to power themselves (such as card readers that require only that the access card be waved within inches of the reader to unlock doors). A transponder device is self-powered and transmits a signal received by the reader. This can occur consistently or only at the press of a button (like a garage door opener or car alarm key fob).

**Physical intrusion detection systems, also called *burglar* alarms If communication lines are cut, an alarm may not function and security personnel and emergency services will not be notified. Thus, a reliable detection and alarm system incorporates a heartbeat sensor for line supervision. A heartbeat sensor is a mechanism by which the communication pathway is either constantly or periodically checked with a test signal. If the receiving station detects a failed heartbeat signal, the alarm triggers automatically**.

**Piggybacking is following someone through a secured gate or doorway without being identified or authorized personally**

**With the right equipment, unauthorized users can intercept electromagnetic or radio frequency signals (collectively known as emanations)**

**The types of countermeasures and safeguards used to protect against emanation attacks are known as TEMPEST countermeasures.**

**TEMPEST countermeasures include Faraday cages, white noise, and control zones.**

**Faraday** Cage A Faraday cage is a box, mobile room, or entire building designed with an external metal skin, often a wire mesh that fully surrounds an area on all sides (in other words, front, back, left, right, top, and bottom). This metal skin acts as an EMI absorbing capacitor (which is why it’s named after Michael Faraday, a pioneer in the field of electromagnetism) that prevents electromagnetic signals (emanations) from exiting or entering the area that the cage encloses. Faraday cages are quite effective at blocking EM signals. In fact, inside an active Faraday cage, mobile phones do not work, and you can’t pick up broadcast radio or television stations.

**White Noise** White noise simply means broadcasting false traffic at all times to mask and hide the presence of real emanations. White noise can consist of a real signal from another source that is not confidential, a constant signal at a specific frequency, a randomly variable signal (such as the white noise heard between radio stations or television stations), or even a jam signal that causes interception equipment to fail. White noise is most effective when created around the perimeter of an area so that it is broadcast outward to protect the internal area where emanations may be needed for normal operations.

**Control Zone** A third type of TEMPEST countermeasure, a control zone , is simply the implementation of either a Faraday cage or white noise generation or both to protect a specific area in an environment; the rest of the environment is not affected. A control zone can be a room, a floor, or an entire building. Control zones are those areas where emanation signals are supported and used by necessary equipment, such as wireless networking, mobile phones, radios, and televisions. Outside the control zones, emanation interception is blocked or prevented through the use of various TEMPEST countermeasures

**Fault A momentary loss of power**

**Blackout A complete loss of power**

**Sag Momentary low voltage**

**Brownout Prolonged low voltage**

**Spike Momentary high voltage**

**Surge Prolonged high voltage**

**Inrush An initial surge of power usually associated with connecting to a power source, whether primary or alternate/secondary**

**Noise A steady interfering power disturbance or fluctuation**

**Transient A short duration of line noise disturbance**

**Clean Nonfluctuating pure power**

**Ground The wire in an electrical circuit that is grounded**

There are two types of electromagnetic interference (EMI): **common mode and traverse mode.** **Common mode noise is generated by a difference in power between the hot and ground wires of a power source** or operating electrical equipment. **Traverse mode noise is generated by a difference in power between the hot and neutral wires of a power source or operating** electrical equipment.

**Radio frequency interference (RFI) is another source of noise and interference that can affect many of the same systems as EMI. A wide range of common electrical appliances generate RFI, including fluorescent lights, electrical cables, electric space heaters, computers, elevators, motors, and electric magnets,**

**Rooms intended primarily to house computers should generally be kept at 60 to 75 degrees Fahrenheit (15 to 23 degrees Celsius). However, there are some extreme environments that run their equipment as low as 50 degrees Fahrenheit and others that run above 90 degrees Fahrenheit. Humidity in a computer room should be maintained between 40 and 60 percent. Too much humidity can cause corrosion. Too little humidity causes static electricity**

**Static voltage Possible damage**

40 Destruction of sensitive circuits and other electronic components

1,000 Scrambling of monitor displays

1,500 Destruction of data stored on hard drives

2,000 Abrupt system shutdown

4,000 Printer jam or component damage

17,000 Permanent circuit damage

**Water suppresses the temperature.**

**■ Soda acid and other dry powders suppress the fuel supply.**

**■ CO 2 suppresses the oxygen supply.**

**■ Halon substitutes and other nonflammable gases interfere with the chemistry of combustion and/or suppress the oxygen supply.**

Stage 1: The Incipient Stage At this stage, there is only air ionization but no smoke.

Stage 2: The Smoke Stage In Stage 2, smoke is visible from the point of ignition.

Stage 3: The Flame Stage This is when a flame can be seen with the naked eye.

Stage 4: The Heat Stage At Stage 4, the fi re is considerably further down the timescale to the point where there is an intense heat buildup and everything in the area burns.

Personnel should be trained in the location and use of fi re extinguishers. Other items to include in fi re or general emergency-response training include cardiopulmonary resuscitation (CPR), emergency shutdown procedures, and a pre-established rendezvous location or safety verification mechanism

Various types of fences are effective against different types of intruders:

■ Fences 3 to 4 feet high deter casual trespassers.

■ Fences 6 to 7 feet high are too hard to climb easily and deter most intruders, except determined ones.

■ Fences 8 or more feet high with three strands of barbed wire deter even determined intruders

**A turnstile is a form of gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction.**

**A mantrap is a double set of doors that is often protected by a guard**

**A lock is a crude form of an identification and authorization mechanism. If you possess the correct key or combination, you are considered authorized and permitted entry. Key-based locks are the most common and inexpensive forms of physical access control devices. These are often known as preset locks . These types of locks are subject to picking, which is often categorized under a class of lock mechanism attacks called shimming.**

Some programmable locks can be configured with multiple valid access combinations or may include digital or electronic controls employing keypads, smartcards, or cipher devices. For instance, an electronic access control (EAC) lock incorporates three elements: an electromagnet to keep the door closed, a credential reader to authenticate subjects and to disable the electromagnet, and a sensor to reengage the electromagnet when the door is closed

An **infrared motion** detector monitors for significant or meaningful changes **in the infrared lighting pattern** of a monitored area.

A **heat-based motion** detector monitors for significant or meaningful **changes in the heat levels** and patterns in a monitored area.

A **wave pattern** motion detector transmits **a consistent low ultrasonic or high microwave frequency signal into a monitored area and monitors for sig**nificant or meaningful changes or disturbances in the reflected pattern.

A **capacitance motion** detector senses changes in the **electrical or magnetic field** surrounding a monitored object.

A **photoelectric motion** detector senses changes in visible light levels for the monitored area. Photoelectric motion detectors are usually deployed in **internal rooms that have no windows and are kept dark**.

A **passive audio motion** detector listens for abnormal sounds in the monitored area.

**Deterrent Alarms** Alarms that trigger deterrents may engage additional locks, shut doors, and so on. The goal of such an alarm is to make further intrusion or attack more difficult.

**Repellant Alarms** Alarms that trigger repellants usually sound an audio siren or bell and turn on lights. These kinds of alarms are used to discourage intruders or attackers from continuing their malicious or trespassing activities and force them off the premises.

**Notification** Alarms that trigger notification are often silent from the intruder/ attacker perspective but record data about the incident and notify administrators, security guards, and law enforcement. A recording of an incident can take the form of log fi les and/ or CCTV tapes. The purpose of a silent alarm is to bring authorized security personnel to the location of the intrusion or attack in hopes of catching the person(s) committing the unwanted or unauthorized acts.

**Local Alarm System** Local alarm systems must broadcast an audible (up to 120 decibel [db]) alarm signal that can be easily heard up to 400 feet away. Additionally, they must be protected from tampering and disablement, usually by security guards. For a local alarm system to be effective, there must be a security team or guards positioned nearby who can respond when the alarm is triggered.

**Central Station System** The alarm is usually silent locally, but offsite monitoring agents are notified so they can respond to the security breach. Most residential security systems are of this type. Most central station systems are well-known or national security companies, such as Brinks and ADT. A proprietary system is similar to a central station system, but the host organization has its own onsite security staff waiting to respond to security breaches.

**Auxiliary Station** Auxiliary alarm systems can be added to either local or centralized alarm systems. When the security perimeter is breached, emergency services are notified to respond to the incident and arrive at the location. This could include fi re, police, and medical services. Two or more of these types of intrusion and alarm systems can be incorporated in a single solution….