5.1 Site Security

Objectives:

- Describe the use of physical security controls in planning and implementing site security
- Identify key features of environmental and fire suppression systems that impact security

Site Layout and Access

Physical Access controls depend on the same access control fundamentals as network or operating system security:

- Authentication – create access lists and identification mechanisms to allow approved persons through the barriers
- Authorisation – create barriers around a resource so that access can be controlled through defined access points
- Accounting – keep of record of when access points are used and detect security breaches

Physical security mechanisms are expensive, costs need to be balanced against risks.

Security Zones

Physical security can be thought of in terms of zones. Each zone should be separated by its own barrier. Access points through the barriers need to be controlled by one or more security mechanisms. Progression through each zone should be progressively more restricted.

The number of zones will depend on the size of the site and the type of operations that take place there, but you could categorise the following general issues:

- External – the areas outside the premises. It may be difficult to control these areas, with security mechanisms limited to surveillance
- Perimeter – for a single site, this will be the walls of the building itself. A large site with many buildings will have an outer perimeter and then inner perimeters for each building
- Public – these are areas of the building where guests are invited, deliveries accepted, and so on. Public zones are typically high traffic
- Restricted – these are areas where most of the employees work. Guest may be invited into these zones, if they are subject to the proper controls. Depending on the level of security, it may or may not be appropriate to control the movement of employees between restricted zones.
- Secure – these are areas where access is strictly limited because they contain critical systems or confidential data.

ID Badges

A photographic ID Badge showing name and access details. These can be combined with passcode, smart card or biometric information to authenticate at gateways.

Barriers and access points

A barrier is something that prevents access but usually are not completely effective. The purpose of a barrier is to channel people through access points. Each access point should have an authentication mechanism so that only authorised people are allowed through. Surveillance should also be used to ensure that attempts to breach the barrier are detected.

Site Layout and Signs

Really only effective with a new site as it can be difficult to change an existing site. Plan the site using the following principles:

- Locate secure zones as deep within the building as possible, avoid external walls, doors and windows
- Position public access areas so that guests do not pass near secure zones
- Minimise traffic that has to pass between zones
- Make high traffic areas visible so that covert use of networks and devices is hindered
- Do not position screens and input devices in secure zones facing windows, doors or pathways

Fencing

Protect the exterior with fencing. Security fencing needs to be transparent so guards can see through it to detect breaches. Fencing should be robust and should be anti-climb.

Gateways and locks

Locks are categorised as follows:

- Conventional – prevents door handle being operated without a key. Not resistant to lock picking
- Deadbolt – this is a bolt on the frame of the door, separate to handle mechanism
- Electronic – lock is operated by entering a PIN on an electronic keypad
- Token Based – a smart lock may be opened using a magnetic swipe card or a proximity reader to detect the presence of a wireless key fob or one time password or smart card.

A secure gateway will normally be self-closing and self-locking. With a simple door or fence as an entry mechanism it can be difficult to record who passes through and multiple people may pass at once. Unauthorised users will be able to “tailgate” to gain access behind an authorised user.

This can be avoided by introducing a turnstile or by using a mantrap. This is where one gateway leads to another in an enclosed space.

In addition, all entrances, fire exits and windows should be fitted with bars, locks or alarms to prevent intrusion.

Securing Devices

The most vulnerable part of the network infrastructure will be the communications room. Access should be controlled and surveillance should be in place.

Equipment within the communications room should be installed in lockable cabinets in order to add another layer of security. Another option is to install cable locks for use with portable devices such as laptop. Portable devices could also be encrypted in case of theft which would render them unreadable unless the encryption key was known.

Alarms

There are three main types of alarms:

- Circuit – this sounds when the circuit is opened or closed e.g. a door or window being opened. Suitable for use on the perimeter and on doors and windows.
- Motion – This is triggered by movement within the area that is being protected. These are use radio reflection or passive infrared
- Duress – this is triggered manually by staff if under threat.

Alarms can be linked to local law enforcement or third party security firms. Alarms can also be silent in order to avoid detection.

The main problem with alarms is the incidence of false alarms where the alarm has been triggered by mistake.

Surveillance

This is usually a second layer of security designed to improve the resilience of perimeter gateways. Surveillance may be focussed on perimeter areas or within a security zone.

Several different kinds of surveillance can be deployed:

- Guard Dogs – used more as detection and deterrence. Can be expensive as need experienced trainers and handlers.
- Security Guards – again effective detection and deterrence. But again is expensive. Guards need to be scrutinised and provided with effective training
- CCTV – still quite expensive but cheaper than having guards. Good for detection and deterrence. Should ensure that cameras work in all lighting conditions. The right camera should be used. Entry ways a fixed focal length camera would do but if you are monitoring a large area then a camera that supports Pan, Tilt and Zoom would be better.
- Lighting – this can act as a deterrent and can be linked to a motion detector.

- Physical Access List – log entry and exit of people. This could be automatic or as simple as signing in and out of a register.
- Staff – this is the cheapest form of surveillance and could be implemented within general staff duties. Staff should be trained to challenge visitors who are not authorised to be on the premises. Have proper procedures for authentication on entering buildings.

Environmental Controls

Environmental security means maintaining a climate that is not damaging to electronic systems or staff and ensuring a stable power supply.

Site Location

In terms of choosing a location of a new site, the following factors are important security considerations:

- Accessibility – A geographically remote site has advantages in terms of deterring and detecting intruders. It is much easier to detect suspicious activity in a quiet, remote environment than it is in a busy urban area. On the other hand, a remote location does carry risks. Infrastructure (electricity, heating, water, telecommunications, and transport links) may not be as reliable and require longer to repair.

- Natural Disaster Hazards – In many locations, flooding is the most commonly encountered natural disaster hazard. Rising sea levels mean that previously safe areas can become a subject to flood risks within just a few years. A common sense approach should be taken by ensuring computer equipment and cabling should be positioned above the ground floor and away from major plumbing. Other natural disasters can include earthquake, volcanoes and storms.

- Dust - This can damage computer systems as dust builds up on components. Dust should be kept in check through regular cleaning and filters should be in place if possible to help clean the air.

- Temperature and Humidity - Servers should be installed in a dedicated room or area. This could be isolated to help maintain the proper environment and to control security. Servers and communications equipment are often housed in purpose built buildings (data centre) Servers generate quite a bit of heat so the room has to be fan cooled from the front and warm air blows out through exhausts in the back which can cause the room to heat up quite considerably. A warm room raises the chances of equipment overheating which can cause system failure. The temperature in the server room should be consistent as temperature variations can cause condensation leading to corrosion or short circuiting. Heat causes components to expand and contract causing connectors over time to work free from their sockets. The environment should be thermostatically controlled and the temperature maintained around 20-22^{o}C with relative humidity around 50% using an HVAC system is possible.

Environmental Systems (HVAC)

Building control systems maintain an optimum working environment for different parts of the building. The acronym HVAC (Heating, Ventilation, and Air Conditioning) is used to describe these services. For office areas this means heating and cooling; for other areas different aspects of climate control, such as humidity may be important.

Locating computer equipment in the optimum environment and maintaining that environment will reduce the risk of failures and increase the operational life of equipment.

It is also important to establish and log a maintenance routine to maintain the life of systems.

HVAC

This ensures that adequate cooling and humidity and dust control within a room. All air flow into and out of the room is run through ducts, fans and filters and warmed or cooled to the correct temperature and humidity.

The room should also provide decent air flow around the server equipment. Air flow is provided by ensuring enough space around the server or rack. Obviously air conditioning vents should not be blocked by racks or equipment. Where possible, the space should not be exposed to direct sunlight.

The HVAC system should be inspected and maintained regularly. The system should be fitted with an alarm to alert staff of problems. High mission critical systems should be supported by a backup system in case of failure.

Hot and Cold Aisles

A datacentre or server room should be designed in such a way that air flow is maximised across the server or racks. If multiple racks are used, ensure that the warm air flow from servers and equipment will not affect other devices. It is better to implement a hot aisle/cold aisle system to prevent heat from affecting other equipment. This type of system prevents hot air leaks as the hot aisle is covered by blank panels or strip curtains and the air is then drawn in to a heat exchanger.

RFI / EMI

Radio Frequency Interference (RFI) is electromagnetic "noise". Noise in this context is anything that interferes with the signal you want to transmit (or receive). Typical man-made sources of electromagnetic noise include power lines, generators, transformers, magnets, fluorescent lights, fans, air- conditioning units, cordless phones, baby monitors, and microwave ovens.

The signal from one device also counts as interference when it disrupts another device - for example, if you use a cell phone in proximity to stereo N speakers you may be able to hear the interference. Similarly, the signals from two access points can interfere with one another in some circumstances.

RFI has the potential to disrupt wireless communications. Microwaves and cordless phones are a particular problem because they use the same general part of the spectrum as some wireless network standards (2.4 GHz).

When electromagnetic noise affects electronic equipment, it is often referred to I specifically as ElectroMagnetic Interference (EMI). To affect an electronic circuit, the source of EMI

would have to be quite close to the component. Examples include a fan positioned next to a monitor or a network cable running next to a fluorescent light.

If a troublesome EMI source is identified and cannot be relocated, the only option is to install some sort of EMI shielding. Wired network links can be implemented using the following media:

- Twisted-pair - this carries electrical signals over copper wire cable pairs. , Cabling is usually unshielded (UTP) but can be screened (ScTP / FTP [Foil Twisted Pair]) or shielded (STP) to further reduce interference and / or eavesdropping.

- Fiber optic - this carries light signals generated by a laser or LED. Fiber optic supports much higher bandwidth than copper cable over longer distances and is not susceptible to interference. It is more difficult to attach eavesdropping equipment on fiber.

- Coaxial - another type of copper cabling. Coax is obsolete in terms of network data cabling but is still used for Audio/Video applications (such as CCTV) and for the wiring within premises for cable TV/internet providers.

Fire Prevention and Suppression

Fire can be catastrophic for businesses and for people

Fire prevention mechanisms should be in place and flammable material should be kept away from possible ignition sources. Office spaces should be kept clear of flammable materials such as boxes and polystyrene. Most countries require businesses to commission a fire inspection annually during which an inspector will advise of any risks and check safety procedures and equipment. Regular checks should be performed on fire/smoke detectors and fire alarms to ensure that they are in working order.

Health and Safety legislation dictates the mechanisms that an organisation must have in place to detect and supress fires. Each building must have well marked fire exits and an emergency evacuation procedure which should be tested and practiced regularly.

Larger buildings need to be designed in such a way that fire cannot be allowed to spread quickly, by separating different areas with fire resistant walls and doors (which must be kept shut).

Fire Detection - Buildings also need to be fitted with automatic smoke and fire detection systems, as well as alarms that can be operated manually. There are several types of detector:

- Smoke detector – measures the integrity of an internal beam of light. The alarm will sound if the beam degrades e.g. if obscured by smoke.
- Ionization smoke detector – a radioactive source creates a regular movement of ionized particles, which can be disrupted by smoke
- Heat detector – these sound if heat rises to a certain point or if the rate of temperature increase exceeds the defined limit
- Flame detector – these use infrared sensors to detect flames, and are the most effective and expensive type

Fire Suppression systems work on the basis of the fire triangle. The fire triangle works on the assumption that a fire requires heat, oxygen and fuel to ignite and burn. Removing any one of these elements provides fire suppression and prevention.

In the UK fires are divided by class, according to the combustible material that the fuels fire

- Class A – ordinary combustible materials such as paper wood, cardboard and most plastics
- Class B – flammable or combustible liquids and solids such as oil, paint and alcohol
- Class C – flammable gas
- Class D – combustible metals such as those found in labs
- Class F – highly flammable materials such as cooking oils and fats.

Staff should be trained to use firefighting equipment and only when safe to do so. Offices should be supplied with adequate fire extinguishers which are of the correct class suitable to that particular working environment.

Extinguisher	Colour Code	Used Against	Prohibited against
Water	Red	Class A	Class B, C, D, F, Electrical
ABC Dry Powder	Blue	Class A, B, C, Electrical	Class D, F
Foam/AFFF	Cream	Class A, B	Class C, D , F , Electrical
CO^2	Black	Class B, Electrical	Class A, C, D, F

Apart from fire extinguishers, buildings can also be fitted with an overhead sprinkler system. This is a legal requirement is a building contains more than 100 people, if it is high rise, it contains overnight accommodation or if it is a public building.

Most sprinklers work automatically, are triggered by heat, and discharge water. This however can be problem in an area containing electrical equipment so an alternative may need to be used such as gasses that are non-toxic to humans e.g. CO2, Argon and Nitrogen. These gases deplete oxygen in the area and have a cooling effect.

Escape Plans, Routes and Drills

Every building requires to have a fire evacuation plan for use in an emergency. The plan instructs staff on how to leave the building safely and assemble at a designated point outside.

The plans assigns responsibility to fire marshals who ensure that the building has been empty and that everyone is accounted for.

Escape Routes from the building must be clearly signed and be kept clear. The plan should also set out procedures to follow should an escape route be blocked.

The escape plan should be tested by performing an evacuation drill periodically. This ensures that all staff are familiar with the plan and with escape routes and marshal point.