Topic 3

Physical Security

Dr Diarmuid Ó Briain

Version: 2.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

This page is intentionally blank

1 Objectives

By the end of this topic, you will be able to:

- Compose a secure facility plan
- Integrate physical access controls into a secure facility plan
- Formulate a plan for physical security controls as part of a secure facility plan
- Incorporate environmental and safety concerns into a secure facility plan.

2 Introduction

Physical security controls are essential for protecting sensitive facilities and assets from unauthorised access, theft, vandalism, and other physical threats. These controls can be divided into two main categories:

- Perimeter security
- Interior security.

Perimeter security is the first line of defence for a secure facility. It includes physical barriers such as fences, walls, and gates, as well as intrusion detection devices such as motion sensors, cameras, and alarms. Interior security is the second line of defence for a secure facility. It includes physical barriers such as doors, locks, and turnstiles, as well as intrusion detection devices such as motion sensors, cameras, and alarms.

In addition to physical security controls, it is also important to consider the environment and safety of a secure facility. This includes having a backup power generator, a fire suppression system, a flood detection system, and flood protection measures (if necessary).

3 Site and Facility Design

3.1 Location

The location of a facility is often decided on purely technical considerations; however, it is essential that security and environmental and safety concerns are also on the list of things that determine the final siting. Consider:

- Emergency Services
- Hazards and threats
- Agency to services.

3.2 Threats

Consider the site and facility design threat landscape. Devise a risk assessment and put controls in place to deal with each:

- Fire
- Water and flooding
- Storms
- Vandalism
- Sabotage
- Explosions
- Building failure, collapse
- Utility failure and continuity
- Equipment failures
- Access
- Strikes.

3.3 Secure Facility Plan

The planning process should begin by involving all stakeholders and posing two fundamental questions:

- What is the threat, what is the organisation securing against?
- What levels of security are necessary and the organisation is willing to provide?

Once these questions are answered a list of possible threats should be drawn up.

The plan itself is developed using critical path analysis. With this process the company applications are systematically related with all the possible threats to it. A Database Server will require, hardware, software, power, temperature control. This leads to a critical look at the dependencies for this server, what if the electricity goes down, what if the hardware overheats.

3.4 Physical Security Controls

Physical security controls can be grouped into the following three groups:

- **Physical**
  - Walls
  - Fences
  - Gates
  - Locks
  - Lighting
  - Guards
  - Guard dogs
- **Technical**
  - Intrusion detection systems
  - Alarms
  - CCTV
  - Fire detection
  - Fire Suppression
- **Administrative**
  - Site Management
  - Personnel Access Controls
  - Security Training
  - Procedures in the event of security breaches

3.4.1 Server Rooms

Server rooms should be enclosed, restricted and protected rooms where mission critical equipment should be maintained in a temperature and humidity controlled environment. Halon type oxygen displacement fire detection and extinguishing systems should be available. Human access should be severely restricted to prevent unauthorised access as well as casual human access by employees who have no business there.

3.4.2 Work Areas

In as much as is possible work areas should be designed to prevent shoulder surfing. Shoulder surfing is the act of gathering information by watching someone's monitor and keyboard. The level of access an employee has should determine the work area they have. If they have high levels of access it is important that the proximity of their work area to lower level access employees does not allow for unauthorised access.

4 Physical Access Controls

4.1 Fence

Figure 1: Security Gate with bollards

This is usually the first line of defence. The following guidelines should be considered when establishing such a fence.

- 1 metre Deter casual trespassers
- 2 metres Hard to climb easily
- 2.5 metres Delay determined intruders.

Another consideration is the planning laws in your locality. These may impact the type or look of the fence you plan.

A grass or gravel clearway along a fence should be considered to deter vehicles from parking near the fence. Bollards are a good method to deter such vehicles.

4.2 Access points

These points can be a weakness in the first layer of defence. By their nature gates provide access through the fence and therefore should be afforded the appropriate management.

4.3 Intrusion detection devices

- Photoelectric beams
- Ultrasonic
- Passive infrared
- Microwave
- Pressure sensitive pads

The use of intrusion detection systems can be mixed. They can either trigger audio or silent alarms or perhaps drown the area in light. One consideration however is the triggering of alarms by non intruders i.e. animals and birds.

Figure 2: Motion detector

4.4 Light

This is an very important consideration in your security plan. If it is dark it makes it easier for the intruder to access undetected. We also need to light areas to allow escape from the building in emergencies. Here are some of the lights that are typically encountered in an plant:

- **Continuous Lighting**
  - Fixed lights should be installed 2.5 metres above ground. The light on the ground from the lights should be at least 2 lumens.
- **Motion sensitive/trip lighting**
  - Sensor activated light can be both a good security deterrent and a cost effective alternative to continuous lighting.
- **Standby lighting**
  - Lights that come on in the event of power failure.
- **Exit lighting**
  - Lights to indicate the exit points.

4.5 Closed Circuit Television (CCTV)

Figure 3: CCTV

CCTV is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. CCTV equipment may be used to observe parts of a process from a central control room; when, for example, the environment is not suitable for humans.

CCTV systems may operate continuously or only as required to monitor a particular event.

A more advanced form of CCTV, utilising Digital Video Recorders (DVR) or Network Video Recorders (NVR), provides recording for possibly many years, with a variety of quality and performance options and extra features like motion-detection and email alerts.

Points to consider when installing CCTV systems:

1. The ability to **detect** an object
2. The ability to **recognise** a detected object
3. The ability to **identify** object details.

4.6 Security Guards

A security guard is a privately and formally employed person who is paid to protect property, assets, and people. Security officers are uniformed and act to protect property by maintaining a highly overt and visible presence to deter inappropriate access, observing for signs of crime, fire or disorder; then taking action and reporting any incidents to their client and emergency services as appropriate.

Generally the Security Guard will practice the *detect, deter, observe and report* methodology and call on the Gardaí or police when a situation is getting beyond their control.

Security officer's primary duty is the prevention and deterrence of crime. Security personnel enforce company rules and can act to protect lives and property. In fact, they frequently have a contractual obligation to provide these actions.

Security personnel may also perform access control at building entrances and vehicle gates, meaning, they ensure that employees and visitors display proper passes or identification before entering the facility. Security officers are often called upon to respond to minor emergencies (lost persons, lockouts, dead vehicle batteries, etc.) and to assist in serious emergencies by guiding emergency responders to the scene of the incident, helping to redirect foot traffic to safe locations, and by documenting what happened on an incident report.

4.7 Access Logs

Company: **Date:**

Name	Company	Name of person visiting	Security Guard	Time in	Time out

Figure 4: Access Log

Access logs should be maintained either in paper form though more commonly in electronic form to record the comings and goings on non employees.

5 Perimeter Security

5.1 Doors

1. Panels and glass should be protected against being kicked in or knocked out
2. Install metal lining on exterior wooden doors to resist drilling or sawing
3. Secure double doors with heavy duty, multiple-point, long flush bolts. Make sure the frame is as strong as the door
4. All exterior doors should be constructed of steel, aluminium alloy, or solid-core hardwood, with minimum 1.5mm steel on side and rear doors
5. Door frames should be securely fixed to the walls
6. Glass doors should have burglar-resistant glass installed
7. Doors should be secured with a minimum of 3 hinges
8. Doors should be clearly lit
9. Emergency doors should be clearly marked
10. Doors should provide entry and exit in the event of emergencies like power failure
11. Doors should have the same fire rating as the walls.

5.2 Locks

Exterior swinging doors should have a minimum 25mm deadbolt lock, 25mm throw bolt with a hardened insert, and free turning steel or brass tapered-cylinder guard. Steel strike plates should be used on aluminium door frames. All outside hinges should have non-removable hinge pins.

5.2.1 Electronic/Electrical Locks

An electronic or electric lock is a locking device which operates by means of electric current. Electric locks are sometimes stand-alone with an electronic control assembly mounted directly to the lock. More often electric locks are connected to an access control system. The advantages of an electric lock connected to an access control system include:

- Key control, where keys can be added and removed without re-keying the lock cylinder
- Fine access control, where time and place are factors
- Transaction logging, where activity is recorded

5.2.2 Authentication methods

Electronic locks offer a variety of means of authentication some are described below:

Numerical codes, passwords and passphrases

Perhaps the most prevalent form of electronic lock is that using a numerical code for authentication. The correct code must be entered in order for the lock to deactivate. Such locks typically provide a keypad. Combination lengths are usually between 4 and 6 digits long.

Security tokens

Another means of authenticating users is to require them to scan or swipe a security token such as a smart card or similar, or to interact a token with the lock.

Biometrics

As biometrics become more and more prominent as a recognised means of positive identification, their use in security systems increases. Some new electronic locks take advantage of technologies such as fingerprint scanning, retinal scanning and iris scanning, and voiceprint identification to authenticate users.

5.2.3 Padlocks

The most common assaults on padlocks are made with bolt cutters or crowbars. Quality padlocks should have the following features:

- Laminated or solid body case
- Hardened steel shackle with a minimum diameter of 8mm
- A double locking mechanism providing *heel and toe* locking, and at least 5-pin tumblers in the cylinder.

5.3 Turnstiles

A turnstile, also called a baffle gate, is a form of gate which allows one person to pass at a time. It can also be made so as to enforce one-way traffic of people, and in addition, it can restrict passage only to people who insert a security pass, or similar. Thus a turnstile can be used to restrict access to authorised people, for example in the lobby of an office building.

Figure 5: Turnstyle

From a security standpoint, they lead patrons to enter single-file, so security personnel have a clear view of each patron. This enables security to efficiently isolate potential trouble or to confiscate any prohibited materials. Thus, turnstiles are a tool which leads to a more safe and secure atmosphere throughout a site.

5.4 Mantrap

A mantrap refers to a small space having two sets of interlocking doors such that the first set of doors must close before the second set opens. ID may be required for each door, and possibly different measures for each door. For example, a key may open the first door, but a personal identification number entered on a number pad opens the second. Other methods of opening doors include proximity cards or biometric devices such as fingerprint readers or iris recognition scans.

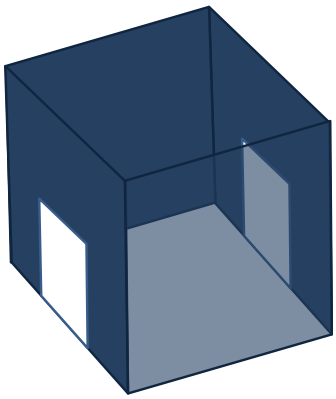

Figure 6: Mantrap

Mantraps may be configured so that when an alarm is activated, all doors lock and trap the suspect between the doors in the *dead-space* or lock just one door to deny access to a secure space.

5.5 Windows

Windows should offer light, ventilation, and visibility, but not easy access. Locks should be designed so they cannot be reached and opened by breaking the glass. First floor windows should be protected with burglar-resistant glass, bars, grilles, grates, or heavy-duty wire screening to provide optimum window security.

5.5.1 Plate Glass

This is the most common type of glass found in windows. It is easy to get and cut for openings and for replacement. One problem is it tends to shatter in shards when broken or subject to an explosion. This presents a safety hazard.

5.5.2 Tempered Glass

This form of glass has been processed by controlled thermal or chemical treatments to increase its strength compared with normal glass. Tempered glass is made by processes which create balanced internal stresses which give the glass strength. It will usually shatter into small fragments instead of sharp shards when broken, making it less likely to cause severe injury and deep lacerations.

5.5.3 Polycarbonate Glass

This is not really glass but thermoplastic polymer moulded to look like glass. Fabrication is done with fine tooth saws. Polycarbonate is the toughest glazing available for windows. It very difficult to cut with a knife, but it is easily scratched, damaging the appearance.

6 Environment and Safety

6.1 Power

The maintenance of a secure and sustained power source is essential for technology businesses, data centres and technical laboratories.

6.1.1 Power problem terms

- **Fault** – This is a momentary loss of power
- **Blackout** – Complete loss of power
- **Sag** – Lowering of the power supply voltage
- **Brownout** – Prolonged period of low voltage
- **Spike** – Momentary increase in voltage
- **Surge** – Prolonged period of high voltage
- **Noise** – A continuous power fluctuation
- **Transient** – A short period of noise
- **Ground** – Electrical earth
- **Clean** – Continuous non fluctuating power
- **Inrush** – Surge of voltage given initially after a device is connected to a power source.

6.1.2 Uninterruptible Power Supply (UPS)

A UPS or sometimes called a battery backup, is an electrical device that provides emergency power when the input power source, typically the mains, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide instantaneous or near-instantaneous protection from input power interruptions by means of one or more attached batteries and associated electronic circuitry. The on-battery runtime of most uninterruptible power sources is relatively short 5 – 15 minutes being typical for smaller units but sufficient to allow time to bring an auxiliary power source on line, or to properly shut down the protected equipment.

6.1.3 Electrical/Electronic Noise

In electronics and communication systems, noise is a random fluctuation or variation of an electromagnetic analogue signal such as a voltage or a current. Electronic noise is a characteristic of all electronic circuits. Depending on the circuit, the noise generated by electronic devices can vary greatly. Noise can be produced by several different effects. Thermal noise and shot noise are inherent to all devices. The other types depend mostly on manufacturing quality and semiconductor defects.

6.2 Water and Fire

6.2.1 Development of a Fire

A fire develops typically in four stages, and fire detectors are designed to detect some characteristic effect of one or more of these stages:

- **Incipient stage**
  - No visible smoke, no flame and very little heat
  - A significant amount of invisible (but sometimes detectable by smell) combustion particles may be created
  - This stage usually develops slowly.
- **Smouldering/smoke stage**
  - Smoke, but no flame and little heat.
- **Flame stage**
  - Visible flame, more heat, often less or no smoke, particularly with flammable liquids and gas fires.
- **Heat stage**
  - Large amounts of heat, flame, smoke and toxic gases are produced.
  - The transition from the previous stage can be very fast.

6.2.2 Fire triangle

The fire triangle is a simple model for understanding the ingredients necessary for most fires.

The triangle illustrates the rule that in order to ignite and burn, a fire requires three elements: heat, fuel, and an oxidising agent (usually oxygen). The fire is prevented or extinguished by removing any one of them. A fire naturally occurs when the elements are combined in the right mixture.

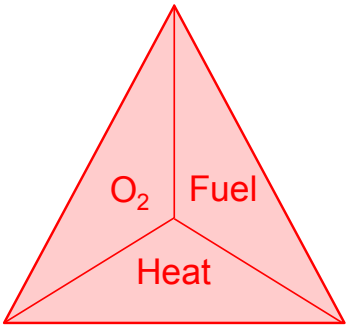

Figure 7: Fire triangle

Without sufficient heat, a fire cannot begin, and it cannot continue. Without fuel, a fire will stop. Without sufficient oxygen, a fire cannot begin, and it cannot continue.

6.2.3 Fire Classes

European	American	Fuel/Heat source	Agents
Class A	Class A	Ordinary combustibles	Water
Class B	Class B	Flammable liquids	CO_2, Foam
Class C		Flammable gases	Dry chemical, Gas
Class D	Class D	Combustible metals	Dry Powders
Class E	Class C	Electrical equipment	CO_2, Foam, Gas
Class F	Class K	Cooking oil or fat	Wet chemical

Figure 8: Fire Classes

Fires are identified according to one or more fire classes. Each class designates the fuel involved in the fire, and thus the most appropriate extinguishing agent. The classifications allow selection of extinguishing agents along lines of effectiveness at putting the type of fire out, as well as avoiding unwanted side effects.

6.2.4 Fire management in OT

With all the electronics in utilities and manufacturing OT, fire is a real risk. Typically water is used in fire control but used on electronic equipment will result in further damage to the equipment. For this reason Halon 1301 Gas was used in such environments. Unlike water, Halon 1301 didn't damage equipment however it did damage the ozone layer. The Montreal Protocol of 1987, limited the production of Halon 1301 to roles like aircraft emergency equipment where another alternative did not exist.

Halon 1301 was replaced by a number of extinguishing agents like Argon and Inergen when protecting data centres. They fall into two broad categories:

- **Halocarbon gases**
  - These work by removing heat from the fire
  - The room must be evacuated before the release of these agents
  - Lower storage space requirement compared to inert gasses
  - Fast fire suppression time (10sec)
  - Must be very near point of use (max 30m)
  - More expensive than inert gasses.

- **Inert gases**
  - These suppress fires by lowering the oxygen concentration in the room below the level needed to sustain combustion
  - Perform more effectively in rooms that aren't well sealed
  - More gas required than Halocarbon gasses to suppress an area
  - These can be piped long distances (100 – 200m) to a room and still retain their effectiveness.

6.2.5 Pre-action Sprinklers

Pre-action sprinkler systems also are an option. The best choice for a particular facility will depend on the system's overall cost, the way in which the system will be used and the space available to house the extinguishing substance. The pipes in pre-action sprinkler systems do not hold water which reduces the risk of leaks that could damage computer or telecommunications equipment.

Instead, a valve within the system is located outside the data centre and keeps water from entering. In order for water to get past the valve, a smoke detector has to let the system know that a fire is occurring; at that point, water moves into the pipes. However, the fire has to grow to a certain temperature before the valve will open and water can discharge into the room. Given that these two events have to occur before water will flow through the pipes that are located within the data centre, the risk of an accidental leak is greatly reduced.

6.3 Water threat

Water damage is a threat in itself. Information systems and paper records can be badly damaged should they get wet particularly if saturated. Data centres and laboratories should be considered for water detection sensors that can trigger an alarm. Such rooms having raised floors to allow time for a water threat to be reacted to are common (though these are also used for conduits to carry room power and network cabling. Water threats are another reason to place such rooms above ground level.

6.4 Heating, Ventilating, and Air Conditioning

Heating, Ventilating, and Air Conditioning (HVAC) is the technology of indoor environmental comfort plus temperature and humidity control in data centres and laboratories. HVAC is particularly important in the design of medium to large industrial and office buildings such as skyscrapers and in marine environments such as aquariums, where safe and healthy building conditions are regulated with temperature and humidity, as well as *fresh air* from outdoors.

6.4.1 Positive Pressure

By applying greater air pressure in the room or building than is outside which ensures that should there be any leakage it will be out and thus prevent any unwanted air in. Monitoring of air pressure in a controlled room is a method that can be applied to the alarm system. Should the pressure change suddenly it is an indication of the possibility of unauthorised access.

7 Summary

Physical security is a critical component of any security programme. By understanding the different types of threats and implementing appropriate physical security controls, organisations can protect their people and property from physical harm. It is important to note that the specific physical security measures that are needed will vary depending on the specific needs of the organisation or facility being protected. For example, a high-security facility may require more stringent physical security measures than a low-security facility. Additionally, it is important to keep physical security measures up to date with the latest technologies and threats. For example, organisations may want to consider using newer technologies such as facial recognition and Artificial Intelligence (AI) to improve their physical security posture.

Finally, it is important to remember that physical security is not just about technology. It is also about people and processes. Organisations need to train their employees on physical security procedures and make sure that these procedures are followed.

This page intentionally left blank