Unit 3

Physical Security Management

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ *Discuss the various different types of physical security systems and safeguards*
- ✓ *Understand the main components of a physical security system*
- ✓ *Make effective use of lighting to maximise the effectiveness of a security system*

Unit 3

Physical Security Management

Physical Security Management Systems

The physical security of an organization is made up of all physical (or tangible) devices and methods used to safeguard the organization from loss or damage. Physical security can be approached in a variety of ways and is afforded different priority from one organisation to the next. Most effective when combined with psychological deterrents, physical deterrents (as the name suggests) establish physical barriers between the business and potential harm.

Some of the most important components of a physical security system include the following among others:

1. Intruder detection and alarm systems
2. Security doors and secure entrances
3. All types of surveillance systems
4. Human security patrols of the premises
5. Security lighting and automated lighting
6. Fire alarms and smoke detection systems
7. All types of access control systems
8. Watch towers and surveillance posts
9. Fences and perimeter boundaries
10. Shutters and window bars

Establishing the security requirements of the business means carefully considering its assets and the extent to which they require protection. It's rare to come across a business that includes *all* of the above in its physical security management system. Instead, most pick and choose the components that best suit their requirements and objectives.

Technology is playing an increasingly important role in all aspects of security, but the importance of manpower in the traditional sense has never been greater. Technologically-advanced security systems and deterrents can make a big difference, but do not have the same logic or decision-making capacity as a human security specialist. Hence, the two should always be used hand in hand.

Perimeter Security System

A perimeter security system is one that protects the business at its boundary. Hence, it is also the organization's first line of defence against unauthorized access. If a perimeter security system is adequate, it significantly lightens the load on all other components within the organization's security system. Quite simply, if you can prevent intruders from accessing your premises in the first place, the rest is inconsequential.

The first defined boundary of the premises is the perimeter wall. This not only defines the boundary of the organisation, it also acts as the first line of defence for any organisation from any unauthorised intrusion.

The importance of a perimeter wall can be summarised in four simple points:

- A perimeter wall clearly marks the boundaries of the property
- It provides a physical deterrent to prevent unauthorized entry
- A physical boundary also creates a legal liability against criminals
- Where unauthorized entry does occur, it is delayed significantly

The security of an organization can be bolstered by both natural and manmade barriers, which typically work best when used in unison with one another.

Natural Barriers

Some businesses benefit from natural barriers - i.e. geographical features that make it more difficult for intruders to gain access. Examples of which include expanses of water, marsh land, cliffs, mountains and so on. Though it's important to remember that while natural barriers can improve security, there is no such thing as an *impenetrable* natural barrier.

Manmade Barriers

As the name suggests, manmade barriers are those that are designed, manufactured and put in place by human beings. Perimeter walls and fencing can be constructed using a wide variety of materials, though in all instances should be sufficiently robust as to prevent (or at least deter) unauthorised intrusion. For obvious reasons, it's also important to ensure that boundary walls and fencing are of a sufficient height - 8 feet or higher is the typical recommendation.

Again, it's important to remember that the perimeter boundary wall is the first obstacle would-be intruders will encounter. If it poses a big enough challenge to their successful entry, your organization will not be considered an attractive target.

It may be written off entirely as a non-viable target, if the deterrent is sufficient.

Perimeter Lighting

One of the most effective ways of boosting the effectiveness of a perimeter wall or fence is to ensure it is adequately illuminated. Visibility is the enemy of the intruder, meaning anything you can do to *literally* shine light on their activities is something you should be doing. Illumination can make it much easier to see, stop and identify criminals - it can also be a great way of preventing them from attempting to gain entry in the first place.

Fences

If it is not economically or logistically feasible to construct a perimeter wall, a fence could offer an effective yet affordable alternative option. Some of the most advanced fence and gating systems on the market provide exceptionally robust protection, often at an exponentially lower cost than a traditional boundary wall.

There are various different types of fences available, each with their own unique advantages and intended applications. Some of the most commonly used types of fences in physical security systems being as follows:

1. Chain link fence - A commonly used type of fence in security, which is composed primarily of wire mesh at least 8 gauge or heavier.

2. Barbed Wire Fence - Made from a variety of different materials in various specifications, though in all instances with sharp 'barbs' that can cause injury to deter unauthorized access.

3. Concertina Coil Fencing - A high-security variant of the barbed wire fence, which is made using coils of barbed wire stretched out as the required.

4. CGI (Corrugated Galvanised Iron) Sheet Fence - Comprises a series of galvanised iron sheets which are also corrugated for additional durability.

What represents the ideal option pure business will be determined by its location, your available budget, the size of the boundary you wish to secure, the level of security required and so on. In all instances, however, fences share a series of similar advantages and disadvantages, when compared to traditional perimeter walls:

Advantages

- Significantly less expensive
- Quicker and easier to erect
- More flexible configuration options

- Clear visibility through the fence
- Easy to repair and replace components

Disadvantages

- Allow outsiders to see in
- Not as durable or robust

Security Gates

Both with boundary walls and fences, security gates will be necessary to allow persons, vehicles and materials to pass through. The idea being that with a security gate, only those who are *authorized* to gain access to your premises are able to enter. The importance of selecting adequately strong and reliable gates cannot be overstated, as low-quality gates represent points of weakness in boundary defences in their own right.

A few points to consider when selecting security gates for a business:

- As it will be the primary entrance and exit point for clients and visitors, it need to look the part and deliver the right first impression
- Sufficient parking should be provided both inside and outside the gate, in order to accommodate employees and visitors alike
- The gate and barrier system should have a failsafe option where it can be operated manually, in case the automated/electronic system fails
- Always ensure that your gates are illuminated adequately at all times, in order to deter would-be intruders
- As gates are often targeted as potential points of entry, they should be covered by CCTV, manned patrols and anything else team deemed necessary
- Carefully consider how many gates may be needed in your boundary wall to allow the free flow of those who are authorized to enter your premises
- Emergency situations should also be taken into account, in order to ensure employees and visitors are not 'stuck' inside in the event of an emergency
- Where possible, it can be beneficial to set up a gate for employees and a separate gate for visitors to your business
- Consider the additional security measures available to prevent vehicles from making forced entries, such as speed bumps, barriers and so on

When choosing and installing gating systems, think from the perspective of a potential intruder. If you can think of a way of potentially compromising the security of your gate, so can they.

Security Lighting Systems

Lighting plays one of the most important roles of all in a wider security system. Good lighting is a uniquely effective deterrent when it comes to protecting both property and people from potential harm. To bring adequate lighting into your security system is to reduce the likelihood of falling victim to a criminal attack for two reasons:

1. Firstly, premises that are properly illuminated deter criminals due to the higher levels of visibility, and the higher subsequent risk of being spotted. Not to mention, identified if caught on camera in an adequately illuminated space.

2. Secondly, lighting provides security personnel with the opportunity to spot suspicious individuals/activities and deal with them accordingly. If there is nowhere for criminals to *literally* hide in the dark, they're much easier to spot.

In addition, it's also true to say that lighting ensures maximum attention is drawn to the rest of your physical security setup. Your perimeter walls or fences, your CCTV cameras, barbed wire, window bars - all sending a strong message to potential intruders.

Ensuring your premises are adequately illuminated is about more than simply installing dozens of random lights in equally random locations. The following objectives should be carefully considered at all steps of the security lighting planning and installation process:

- To provide a clear view of anyone on or in close proximity to your premises
- To ensure there are no 'blind spots' in which criminals could hide
- To provide clear facial identification when used in conjunction with CCTV
- To enable other security provisions on the premises to operate properly
- To draw attention to your security provisions and deter would-be criminals
- To make it impossible to enter your premises 'secretly' day or night
- To provide employees and visitors with a sense of comfort and safety

The specific lighting fixtures, devices and bulbs needed to provide adequate illumination, will vary enormously from one business to the next. It depends entirely on the size, nature and the layout of your business, along with potential entry points for intruders.

In all instances, however, it's important to remember that more isn't always better where security lighting is concerned. Avoiding glare is important to enable your CCTV cameras and security personnel to do their job properly. In addition, you'll also want to carefully consider the energy consumption and

heat output of the different types of security lights available.

Common Security Lighting Mistakes

Setting up a security lighting system doesn't have to be a daunting task, but is nonetheless surprisingly easy to make a mess of. Ineffective security lighting can be just as detrimental as *no* security lighting at all.

Hence, it is important to be mindful of the following common security lighting mistakes, in order to ensure you don't make them yourself:

- Illumination where it is not necessary
- Excessive illumination
- Poor quality lighting fixtures and bulbs
- Unshielded light fixtures
- Excessive glare
- Misaligned like features
- Failing to consider directional light

For example, an unshielded lighting fixture of low quality that beams directly into a CCTV camera will render it completely useless during hours of darkness. Likewise, excessive illumination where it is not necessary can be expensive for the business and uncomfortable for those patrolling or working in the area.

Security Lighting Techniques

Along with simple illumination of any given space, security lighting can be used to achieve a variety of objectives:

- To indicate that an alarm system has been activated
- To disable the visual capabilities of an intruder with glare
- To alert security personnel to movement in a specific area
- To provide emergency elimination in the event of a power cut

Irrespective of how advanced your security lighting system is, it is still essential to conduct a thorough inspection to identify shaded areas, dark corners and blind spots. Installing additional lighting to cover these problem areas is known as 'topping up' and forms an important part of the security lighting system installation.

Alarm Systems

An effective alarm system is more of a psychological deterrent than a physical security measure. The reason being that an alarm system is only effective when it is used alongside other measures to detect intrusion, delay the efforts of criminals and enable an appropriate response.

Alarm systems can be installed to cover one or more areas of an organisation's premises, or to secure it in its entirety. Likewise, alarm systems can also be multi-layered, incorporating such components as door and window alarms, motion detectors and so on.

In short, alarm systems are designed to provide an audible and/or visual alert in the instance that unusual or suspicious activity is detected in any given space. An alarm system may be configured to send a direct alert to a relevant security office or police department, or to simply trigger an audible alarm and flashing lights to draw attention to the incident.

Patrolling

Even with all the most sophisticated security systems and devices in the world, nothing is considered more effective as a physical or psychological deterrent than a manned patrol. This is where one or more individuals physically patrol the area in question, either on foot or using vehicles where required.

The presence of one or more patrol guards alone can completely eliminate the appeal of any given property as a potential target for attack.

Objectives of Patrolling

Patrolling can be used to achieve a variety of security objectives, including but not limited to the following:

1. To watch for signs of unusual or suspicious activity
2. To deter criminals from attempted attacks/intrusions in the first place
3. To make note of damage to any physical security safeguards
4. To ensure all security devices and components are functioning properly
5. To continuously identify potential security vulnerabilities
6. To ensure that workers and visitors are behaving appropriately on-site
7. To ensure that all windows, doors, gates etc. are securely closed and locked
8. To keep an eye on areas that may be susceptible to fire or other damage

9. To create a sense of safety and reassurance for workers, clients and visitors

10. To help others better-understand their security obligations

Foot Patrols

It is generally agreed that foot patrols are the most effective of all patrols, as they provide the security personnel in question with the opportunity to observe their surroundings much more slowly and in greater detail. In addition, patrolling premises on foot enables security personnel to communicate and interact with workers, customers, visitors and so on.

When patrolling on foot, security personnel can access areas of the property that would be inaccessible by way of any vehicle. In addition, patrolling premises on foot is something that can be achieved in absolute silence, making it much easier to catch potential perpetrators unaware.

Mobile Patrols

As the name suggests, mobile patrols are conducted using some kind of vehicle. These days, an extensive range of vehicles and transportations devices are used by security personnel - examples of which include Segway scooters, bicycles, golf buggies, motorbikes and various types of cars/vans.

For obvious reasons, the bonus of a mobile patrol is the way in which it can cover a much broader area at once. Access to vehicles also makes it much easier to tend to emergencies or chase down criminals quicker.

The downside to mobile patrols being that it's much easier to overlook suspicious behaviour or potential security shortfalls, when driving past them at speed.

Typical Duties While on Patrol

The exact duties that will be carried out by security personnel on patrol will differ significantly from one organisation to the next. Nevertheless, the vast majority of patrolling security personnel will be expected to take responsibility for the following:

- Checking perimeter walls and fencing for potential damage
- Ensuring security devices (such as cameras and alarms) are working
- Checking the security of locks, seals and potential points of entry
- Taking notes of vehicles parked in close proximity to the business
- Carefully monitoring the actions and activities of suspicious persons
- Making sure nobody is in a place they shouldn't be at any time
- Identifying hazards or potential threats to health and safety

- Investigating and reporting all types of abnormalities
- Reporting all potential security issues to senior management
- Contacting the emergency services where necessary

Tips for Making Patrols More Effective

1. Always ensure that patrols are carried out at random times, with no patterns that could be identified or exploited
2. Don't use vehicles where manned patrols are possible, as the latter tends to be more precise and therefore effective
3. Provide security personnel with access to the modern technology, such as communication devices, night vision equipment and so on
4. Strength in numbers works well with manned patrols, so try to ensure there's help on hand if your patrolling personnel need it
5. Place heavy emphasis on patrolling key areas, but never overlook other areas where criminals could gain access to the premises
6. Produce a detailed checklist of security checks that should be conducted on a daily basis, which all security personnel must follow
7. Ensure security personnel regularly meet with senior management to discuss any potential issues or ideas for improvements
8. Vary the route of your patrols continuously to prevent the risk of pattern exploitation, though ensure all areas of the business are covered each time

Visitor Management Best Practice Guidelines

A visible security presence can be reassuring for visitors, though can in some instances also be disconcerting. The heavier your security presence and general security infrastructure, the more uneasy visitors to your premises are likely to feel.

This is where a few visitor management best practice guidelines for security personnel can help, including but not limited to the following:

- Always ensure every visitor is greeted with a smile
- Make clear your genuine desire to help them
- Question their reasons for visiting politely and professionally

- Ask questions politely and answer the visitor's questions
- Be patient and attentive - never cold and indifferent
- If you can't help them, direct them to someone who can
- Note their details or get them to sign in if necessary
- Help them get to their destination if unsure where to go
- Treat every visitor with the same kindness and respect

As previously touched upon, it's important for security personnel to understand that they are often responsible for delivering guests' first impressions of the entire organisation.

Hence, there are certain unfortunate (yet surprisingly common) behaviours that should be avoided at all costs:

- Sleeping on the job
- Poor grooming or personal hygiene
- Treating guests and enquiries with disdain
- Using inappropriate language
- Coming across as cold and uncaring
- Treating visitors with suspicion
- Being impatient or indifferent
- Not taking visitors' questions and concerns seriously

Keys

For centuries, keys have represented the first and often only line of defence for important assets and property. In some instances, locks and keys are the only things that stand between criminals and their targets. Keys are available in a wide variety of different shapes, sizes and types these days, though nonetheless serve the same basic purpose they always have.

Consequently, it is essential to have a good key control system in place. This not only ensures adequate protection for the organization and its property, but also enhances accountability in the event that something goes wrong.

The Different Types of Keys

It's worth building a familiarity of some of the different types of keys and related terminology used in security, such as the following:

- Operating keys are the standard keys used to open and close locks
- Duplicate keys are copies made of original keys, either handed out to personnel who need them or kept in storage in case the originals are lost or damaged
- Master keys are specially designed to open an extensive range of locks using a single key. As such, they must be handled and stored with extreme care
- Control keys are used to remove lock cylinders to change the locks when using an interchangeable cylinder system

Lock and Key Accountability

A lock and key system of any kind is only effective when those overseeing it conduct themselves and their activities with responsibility and professionalism. Accountability is essential in all aspects of security, ensuring everyone involved understands their responsibilities and obligations.

For example:

- Each time a key lost, it undermines or even compromises the safety of a key system. This should be clearly communicated to all key holders across the board
- Keys should only ever be allocated to those who are responsible enough to look after them and cannot perform their duties without them
- Detailed, accurate and up to date records should be kept on the keys that have been issued, who they have been issued to, when they were issued, the locks they can open and so on
- If a single key to a sensitive or important lock is lost, the lock should be changed immediately, and all previous keys discarded or destroyed
- Key storage containers around the facility should be secured with robust locking systems and their responsibility allocated to suitable personnel
- Duplicate keys should only be issued upon the approval of senior management or authorized security personnel

Protection of Keys

There are also certain good practice guidelines that should be followed to ensure keys are sufficiently protected, which include the following examples among others:

- Under no circumstances should keytags or markings be used that give an indication of which locks any given key corresponds with
- Disciplinary measure should be enforced in the event that keys are carelessly left on desks, dropped on the floor or handed to individuals who are not authorized to use them
- Periodic audits and spot checks should be carried out to ensure that every key is accounted for and is being held by an appropriate individual
- Any damage or deterioration to any keys or locks should be treated as urgent and addressed accordingly
- Under no circumstances should important keys be allowed to leave the business premises, unless they are specifically required by the individual carrying them

Control Room and Security Management

Many organizations are now choosing to operate without a centralised security control room. However, control rooms still play a role of importance for millions of large and small businesses worldwide.

In a typical security control room, operatives will monitor computer screens and CCTV images, while communicating with other security operatives and patrolling guards remotely. This is also where the administrative side of an organization's security framework and general policies will be overseen.

Typical duties handled in the security control room may include the following:

- Real-time monitoring of the premises
- Coordination of patrols and on-site activities
- Delegation of duties and deployment of security staff
- Logging and storage of events and related data
- Monitoring of security equipment functionality
- Reporting of unusual or suspicious activities
- Liaising with police and other external parties

- Consulting on security issues with senior management
- Issuing keys and key holder responsibilities

Importantly, security personnel (and senior security managers) may also play a direct role in the training and coaching of other members of the workforce. It's widely acknowledged that it is only when every employee contributes to the cause that an organization's security framework can be truly effective.

As such, security personnel may be required to assist with the development and provision of training materials, discuss security issues directly with employees and highlight potential problem in existing security practices.

Further Reading:

- ✓ ***Boothman,***