LEVEL 3 AWARD IN SECURITY MANAGEMENT REVISION NOTES

Provide a healthy, safe, secure and productive working Environments.

Introduction

In the modern workplace there is the potential for many accidents and incidents to take place which could have a detrimental effect upon staff and employees. Anyone who enters your premises and facilities as part of their legitimate business is required to be protected as far as is reasonably practicable from any potential hazards which it is within the business's ability to prevent.

Because business is required to protect people and to provide Health and Safety (H&S) cover in accordance with regulation, it is your responsibility to ensure that you comply with the regulations. The responsibility for protection rests not only with the organisation but with individuals within it — therefore it is not only in the interests of potential victims of incidents but also in the personal interests of you and your company (to avoid prosecution) that you understand the principles of H&S regulation and your contribution to it.

This unit provides background on H&S regulation and how it is applied in the workplace. It also details the responsibilities for H&S enforcement and will address the requirements of Control of Substances Hazardous to Health.

The Scope of Health and Safety

Many people shy away from H&S as they feel it imposes too many restrictions on routine working practices — some see it as an overly bureaucratic hindrance to business. It is true that recent years, because of tighter regulation, have seen an increase in the application of H&S in the workplace. The scope of H&S has necessarily widened in response to an increasing range of potential risks and to the increased incidence of litigation and claims for compensation because of accidents or corporate negligence. H&S therefore legislates to cover a wide range of potential incidents.

Those who may be at risk from such incidents will include but are not limited to:

Think about the reasons for

Health & Safety Regulations and why you think people might be afraid of them and who is at risks Make some brief notes in the space below.

The direct employees of the business or organisation - Those personnel who work as a routine within the company premises or who conduct its operations and processes. Also, those who operate the business's equipment, machinery, vehicles, aircraft and vessels.

Contractors and venture partners employed on your sites - Contractors may take many roles but the majority will be involved in construction and maintenance work. It is particularly important for such personnel to be fully cognisant and compliant with the specific H&S requirements at your business locations.

Visitors - Most businesses will have a range of visitors entering their facilities on a regular and routine basis.

Clients and customers for retail, hospitality and transportation businesses that pay to use your facilities, there will be a range of potential hazards with which they will be unfamiliar in addition to the required response to incidents taking place.

You should have identified a wide range of hazards which could affect people in the workplace. Depending upon the nature of the business the hazards could be extensive and cover a spread from minor to life-threatening. Any or all the following could be applicable to your workplace:

Risk of falling objects and structures.

Risk of exposure to hazardous materials. Risk to personnel from slipping, tripping or falling. Fire risks.

Explosive risks (either accidental or through malicious acts).

Traffic risks, including roads and vehicles including those inside buildings, such as forklift and delivery vehicles. Risks for dangerous machinery. Risks associated with travel such as in vehicles, trains and aircraft. Risks of drowning (public place, retail and hospitality/leisure facilities).

Risks associated with areas of public assembly (overcrowding/overloading).

Consider your own premises and the range of personnel who are involved in its routine activities. Identify them in accordance with the list on the left and the activities that they carry out. What is the range of potential hazards to which they may be exposed? Make some brief notes in the space below.

Risks caused by negligence or poor planning such as obstruction of exit routes or inadequate provision of protective clothing/equipment.

Risks caused by personnel (horseplay, noncompliance with safety requirements).

It can be seen by combining the list of potential 'victims' with the range of possible incidents that there is considerable scope for incidents and accidents to happen. It is important here not to underestimate the ability of human beings to circumvent or ignore regulations and measures which they feel do not apply to them or cause what they feel to be undue inconvenience. It must be reiterated here that it is the responsibility of the business, as far as is reasonably practicable, to anticipate and prevent any combination of the above risks from becoming a reality.

As a Supervisor, Security Officer, Manager and Business Employee you share that responsibility.

The Sources of Health and Safety Regulation

Within the UK, H&S regulation is led by the Health and Safety Commission (HSC) and its executive department, the Health and Safety Executive (HSE) on behalf of HM Government. The relatively recent additions to H&S legislation and regulation, and the associated increased emphasis on its importance in the workplace are due mainly to EU legislation and directives which are now affecting and influencing UK practices. However, it must be understood that the Government retains responsibility for enacting UK laws and regulations.

The detail of H&S regulation and legislation is quite complicated and is the business concern of the H&S department and those specialists directly responsible for their application and enforcement. However, you should understand the basics of such regulation and their provisions.

Look through The Health and Safety at Work Act 1974 and read Pages 8 to 12 'General Duties'. Consider your business and look at the definitions and duties in the

Act. List the areas which apply to your business and to your department. Cross reference (by page number) to where the duties can be found within the Act Make some brief notes in the space below.

The Health and Safety at Work etc. Act 1974, also referred to as HASAW or HSWA, is the primary piece of legislation covering occupational health and safety in the United Kingdom. The HSE is responsible for enforcing the Act and many other Acts and Statutory Instruments relevant to the working environment.

It is probably neither practical nor desirable for you to know the Act in any detail, but it is a valuable exercise to look at the document and ensure that you are clear about your responsibilities and those of the employer.

In addition, the Workplace (Health, Safety and Welfare) Regulations 1992 apply to most workplaces (except construction, onboard ships and underground mines).

Statutory Instruments and Regulations

These are enforced by the HSE and local authorities and cover a wide range of specific areas of business and industry, along with their associated risks and hazards.

For the security manager, it is again worthwhile looking at the regulations listed, some will definitely be applicable to your business and therefore there will be clear benefits in being familiar with the areas of concern.

All laws and regulations contained in these documents are relevant to almost all workplaces, regardless of the operations and functions of the organisation concerned. They enable the provision of protection and the preservation of safe working practices through the mandatory application of their content.

Penalties for Non-Compliance

Prosecution is the main means by which health and safety enforcing authorities hold those companies to account for alleged breaches of the health and safety law. The law provides few sentencing options for the courts, and conviction is usually a fine.

HSE Public Register of Enforcement Notice

The HSE Public Register of Enforcement Notice holds a database where notices will appear for a period of 5 years. HSE enforces health and safety legislation for some industry sectors in the UK excluding those enforced by Local Authorities.

Since April 2011 HSE has classified industries using SIC 2007.

HSE have been using a Standard Industrial Classification to group businesses by their activity since before the Health and Safety at Work Act. (They need to group industries to enable them to target businesses of a type in their inspections and programmes as well as to produce meaningful statistics).

The Provisions of Health and Safety

Regulation in the Workplace

H&S incident book for your organisation.

Alongside the HASAW/HSWA and associated legal directives, the statutory instruments and regulations require a clear response from the organisation or business which may be affected. The provisions of these documents are clear but can be summarised in straightforward terms as follows:

The laws and regulations place a duty upon you and your employer to protect people If you and your employer are found to be guilty of non-compliance or negligence you will face legal penalties

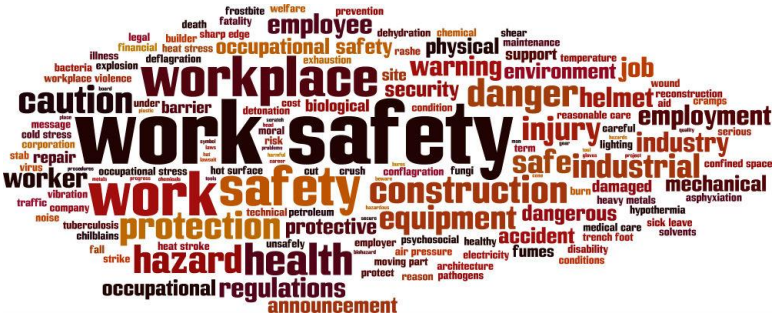
You and your employer need to ensure that there has been a complete and adequate assessment of the risks associated with the activities that you conduct and of the range of effects that they can have upon your staff, employees, contractors, clients and visitors.

Also, and crucially, every employee and individual have a responsibility to comply with the legislation and to ensure that their own actions, negligence or omissions do not cause hazards to other personnel. In the next section of this unit we will address how the security manager can assist in the practical application of H&S regulation through their own actions, by judicious cooperation with the H&S department and by the proper management and coordination of security officer (and system) operations.

The Practical Applications of Regulation

Legal requirements can often be difficult to understand, particularly when the terminology used can be confusing to the non-H&S specialist. Nevertheless, having recognised the fact that we are all responsible for compliance in the workplace, we now need to consider how the law and regulation can be properly and safely implemented. The application of H&S law can be difficult and can appear to stand in the way of some tasks, especially those which need be completed quickly, but you should consider the consequences if it all goes wrong, and you have not done enough or as much as you could reasonably be expected to.

In your organisation, how do you and your H&S representative help to make the workplace a safe working environment?



Under HSWA regulations, there is a range of responsibilities which must be followed to ensure that compliance, and thus safe working, is achieved.

Employers: The employer must ensure, as far as possible, that health, safety and welfare are maintained in the workplace. They must appoint a 'competent person' (normally your H&S officer/manager).

For businesses employing five or more people, there must also be an official record of risk assessments and a formal health and safety policy. You must ensure that your staff understand and comply with the policy.

All Employers, regardless of the business size, must ensure that they:

Make the workplace safe for all employees, contractors, clients and guests.

- Prevent risks to health within the workplace.
- Ensure that plant and machinery are safe to use and that safe working practices are established and followed. Also ensure that IT systems are properly configured for ergonomic use.
- Make sure that all materials are handled, stored and used safely.
- Provide adequate first aid facilities, properly maintained and in appropriate and accessible locations.

Inform employees about any potential hazards, chemicals and other substances used by the firm, and give information, instructions, training and supervision as needed.

- Provide emergency plans to deal with any incidents related to H&S.
- Make sure that ventilation, temperature, lighting, toilet, washing and rest facilities all meet HSAW requirements.

Check that the correct work equipment is provided and is properly used and regularly maintained.

- Prevent or control exposure to substances that may damage health.
- Take precautions against the risks caused by flammable or explosive hazards, electrical equipment, noise and radiation.

What are the typical areas in which employees violate H&S rules?

Avoid potentially dangerous work involving manual handling (and if it cannot be avoided, take precautions to reduce the risk of injury).

Provide health supervision as needed.

Provide protective clothing or equipment free of charge (if risks cannot be removed or adequately controlled by any other means).

Ensure that the correct warning signs are provided and maintained.

Report certain accidents, injuries, diseases and dangerous occurrences to either the HSE or the local authority, depending on the type of business.

(Adapted from: GOV.UK: Employing People

Health and Safety at Work:

Employees: have a duty to ensure that they:

Take reasonable care of their own H&S.

Are dressed appropriately when operating machinery.

Take reasonable care not to put other people (fellow employees and members of the public) at risk by what they do or don't do during their work.

Co-operate with the employer, making sure that they are trained and that they understand and follow the organisation's H&S policies. Do not interfere or misuse anything that has been provided for health, safety or welfare.

Report injuries, strains or illnesses that they suffer because of doing work.

Inform the employer if something happens that might affect their ability to work.

As we will see in Unit 2, risk assessment is at the core of efficient and cost-effective security operations. The role of risk assessment in H&S is little different in that, if it is done correctly, a series of planned actions and contingencies can be put in place.

Risk assessment is the process of looking at all the potential threats to life or well-being that can occur in the workplace and their potential effects on people, groups of people and the business. The importance of this process cannot be overestimated, and non-specialist personnel need to be aware of the process involved and required.

Hazard means anything that can cause harm (e.g. chemicals, electricity, working from ladders, etc.)

Risk is the chance, high or low, that someone will be harmed by the hazard.'

Source: 'An Introduction to Health and Safety' (HSE).

According to the HSE, there are 5 fundamental steps to making a H&S Risk Assessment which are progressive and designed to deal with any kind of risk which may affect a business or organisation. You should become familiar with this process and think about its applications in the workplace.

These steps are:

1. Identify the hazards - Sensibly, the first stage is to look at the hazards in the workplace. There are various methods that can be used to do this and will include a visual inspection, questioning of specialist personnel involved in, for example, hazardous work, and even the distribution of questionnaires to relevant personnel. The HSE website also provides guidance on

the types of hazard which may be encountered. If specialist equipment is being used, any hazards associated with its use must be assessed. Identification of hazards should look at anything and everything that could become a risk and thus can be a long process. However, attention to detail is essential here as an omission could mean that a vital hazard is overlooked. It is also important to bear in mind that hazards from neighbouring sites may have

Using the 5 steps, draw up a Risk Assessment that could be used in your department, an impact upon your facilities (for example, a nearby chemical or nuclear facility).

2. Identify who may be harmed and how Hazards, if not prevented, become risks to people and fundamental to H&S is the identification of those who may be vulnerable. We have already mentioned the range of people who could be harmed, and the following will influence their vulnerability:

Type of work performed

Work location

Knowledge or awareness of hazards and risks

Availability of personal protective equipment (PPE)

What actual harm the hazard can cause to human beings.

3. Evaluate the risks and determine the precautions to take Some of the risks discovered will be more serious than others and there will need to be some level of prioritisation to ensure that these are dealt with first. It is critical that life-threatening risks are adequately addressed and that the precautions which are selected to deal with the risks are targeted towards them. In H&S it is rarely, if at all, acceptable to accept the risk and continue operations without change. According to the HSE, you should also consider what you currently do in comparison with best practice and regulation. If you do not address the risks correctly then you could face penalties. In any case, your priorities for dealing with, or 'treating' the risks should be in this order:

Attempt to carry out the work in a less risky way. Although this is highly desirable, the inherent risks in some forms of work will preclude you from this course of action.

Prevent access to the hazard. Do not carry out work where your personnel may be exposed to the risks. Also, if visitors or other personnel who are not required to be in the location of the risk have access to hazard locations, remove the hazard or physically block access.

How can security officers contribute to protection of personnel in the workplace against H&S risks?

Organise work to reduce exposure to the hazard.

Issue personal protective equipment. Because some activities are inherently risky, it is incumbent upon the employer, who requires those activities to be carried out to provide the appropriate protective equipment.

4. Record and implement findings - You should ensure that any risks are properly recorded and that the measures for dealing with them are implemented.

5. Review and reassess - Both the nature of your business operations and the risks themselves could change over time (or suddenly). Therefore, you should remain aware of the potential effects of such changes to your organisation and ensure that apart from periodical, planned reviews, ad hoc changes may be necessary. The crucial second element of this process is ensuring that any changes are properly communicated throughout the organisation.

It is important here to consider that although in your security role you are unlikely to have main responsibility for H&S; your input will invariably be required to inform specialists in risk assessments.

More relevant for the security personnel will be the requirement to implement and enforce H&S within their own department and perhaps beyond. The advantage for the security department is that its officers have almost unparalleled access throughout the facilities on a 24-hour basis and therefore have the capability to detect and report upon H&S hazards and risks. In the next section, we will assess the ability of the security department to contribute to the H&S effort.

Requirements for Health and Safety Protection

Within work areas, structures, buildings and on various surfaces, there are some general requirements for H&S protection measures to be imposed:

Maintenance Facilities, machinery, equipment and vehicles must be properly and fully maintained in accordance with relevant operating instructions and regulations to ensure the safety and protection of all users and, in the case of vehicles, passengers.

Ventilation - All workplaces need to be adequately ventilated by drawing and circulating fresh, clean air from outside which has not been contaminated in any way.

Temperatures The environment (e.g. humidity and sources of heat) combines with personal factors such as the clothing worn, and the work activity carried out to influence a person's 'thermal comfort'. Appropriate temperature requirements are laid down by regulation and should be enforced in the workplace through the H&S policy.

Lighting - Light should allow people to work and move around safely. Supplementary lighting may be necessary at workstations and in potentially hazardous areas. This includes provision for emergency lighting which will be needed in the event of sudden or unforeseen power failure.

Cleanliness - All workplaces must be clean. Waste should be removed to appropriate receptacles.

Floors and traffic routes - There should be sufficient routes for people and vehicles to move safely and these need to be of appropriate height and width. Speed limits need to be put in place where necessary and barriers and other methods of access restriction placed in and around potentially hazardous sites such as pits, stairs or raised walkways. Floors should be strong and stable enough to support intended usage and should have no holes or gaps which may cause potential risk. Surfaces should be of an appropriate type to avoid slippage or skidding.

Falls - There must be fencing or coverings in place to prevent falls into dangerous areas or substances or from heights. In

How can you inform employees that H&S is everyone's responsibility?

addition, there must be provisions for harnesses or other restraints to prevent falls. Falling objects are dangerous — objects must be appropriately stacked, stored and secured to prevent falling and appropriate protective equipment and clothing provided to workers who operate in hazardous areas to anyone passing through such areas.

Transparent or translucent surfaces Windows and transparent or translucent surfaces in doors, walls and windows must be made of materials to protect against breakage. They should be marked if there is a risk of personnel meeting them.

Sanitary and washing facilities - Must be accessible, clean and well-lit. Hot and cold running water, soap and clean towels (or other means of cleaning and drying) must be provided. Showers, if required by the type of work, must be provided and male and female facilities clearly separated unless each facility is in a lockable, separate room usable only by one person at a time.

Drinking water - High-quality drinking water must be provided in an upward jet or with suitable cups. Where it cannot be obtained from a mains supply, water should be provided in refillable closed containers which should be recharged daily unless they are in water-cooler refillable containers.

Accommodation for clothing and changing facilities - There should be appropriate changing facilities for workers who need to change into special clothing and adequate, suitable and secure spaces should be provided for storage of personal clothing. Facilities should be close to workrooms, washing and eating facilities and provide privacy.

Facilities for rest and eating meals - There should be suitable and sufficient rest facilities and appropriate and adequate seating should be provided for all personnel including any specific requirements for the disabled. Suitable facilities, including tables, should be provided in areas set aside for eating and there should be a means to produce hot drinks along with, where necessary, means for employees to heat their own food.

All security staff must be able to assist in the enforcement of H&S. Security and H&S are both elements of asset protection and security's contribution should not be underestimated. Security's role in enforcing and assisting in the administration of effective H&S measures could include many and varied tasks.

Briefing Visitors

Visitors to premises and facilities will invariably be unfamiliar with the hazards and potential risks on a site or those involved with its operations. Security officers will normally be the first point of contact for such personnel and they are well placed to provide the necessary briefings and c instructions for compliance with H&S. There may also be a role for security here in issuing the necessary PPE.

Patrolling and Reporting

As previously mentioned the patrolling security officer has a significant role to play in the detection and reporting of H&S risks. Although detracting from main security role/function is to be avoided, it makes business sense to use their skills in providing further capability in this area. Security officers must be alert to such risks and they should at least be familiar with the hazards on site and how to react and respond to them. They should also have a process in place whereby they can report any incident or hazard to the correct agency and responsible person as it occurs or is detected. The assignment instructions must have an up to date contact list for not only H&S department staff but also specialist hazardous materials trained personnel (if required by the company operation). Details of emergency services must also be held.

It is important that officers are aware of any hazards that they may encounter during their duties and that they are protected against the risks from them

When on patrol, security officers should be alert to the following potential hazards:

Notes

Hazards at Ground Level - Many workplace injuries are caused by hazards at ground level, either through chemical or lubricant spillage and wet floors, uneven flooring surfaces, debris or trailing cables, excavations or pot-holes, or uncovered utilities such as manholes. These hazards will be exacerbated by poor lighting or obscuration.

Obstructions - Access routes, particularly emergency entrance and exits must be kept clear of debris or other accumulations such as rubbish. The security officer, on discovering such obstructions, must report them immediately and then, if it is safe to do so, should remove them to permit access to be resumed.

Stairs and Elevated Walkways - Stairs and elevated walkways can be particularly dangerous and patrolling officers should be briefed to check not only for unsafe steps and pedestrian areas but also for loose, damaged or unsecured banisters, balustrades or openings. If any are discovered, they should be instructed to remove the hazard if possible and to report the problem. If necessary, they should take steps to block access to potentially dangerous areas until rectification action can be taken.

Warehouse and Storage Sites - The main hazard to personnel in storage areas is that from improperly stacked or arranged packaging, boxes or products. If discovered, security officers should be prepared to cordon the area and report to a responsible person for the problem to be removed.

Production Areas- Any industrial or production areas could have a wide range of potential hazards from electrical, chemical, leakage or machinery-related hazards. There are also potential hazards which can arise from the unsafe or irresponsible behaviour of personnel operating in

the area. A security officer cannot be expected to have the specialist knowledge to recognise and deal with this wide range of threats but should be briefed and have procedures in security instructions which give guidance on the actions to be taken. Vehicle Movements - Security officers witness unsafe vehicle movements must be given clear instructions on the procedures for reporting and if necessary preventing vehicular movement in an area if he/she considers it to be causing a hazard.

The perception of most people considering H&S is that it is directly industrial and production facilities. Of this is not the case and it is important security personnel are aware of the potential hazards at any site, be that a retail airport, large public event or any other where people are expected to work or visit. a prudent step for the security manager to arrange a tour of the site for all security conducted by H&S staff, which provides degree of awareness of the extent of potential hazards.

The Implementation of Procedures and Processes

In addition to the threats and risks from various hazards previously detailed in this there are specific risks to personnel exposure to hazardous substances. Regulation and legislation to provide Control of Substances Hazardous to Health (COSHH) is administered through the HSC and HSE in compliance the COSHH Regulations 2002. The types of substances which may be hazardous are many and varied and, as with other H&S hazards, it will be useful for security staff to be familiar these types.

For each type of hazardous substance, the employer is required to conduct COSHH assessments which will identify hazards and effects and the actions required to counteract their effects or to deal with associated emergencies. These assessments will have controlled centrally by the officer/department but may require input from other departments (e.g. security) for substances in use.

In most of cases, such substances are likely to be used by specially trained and dedicated personnel particularly if involved in a specific manufacturing or industrial process. However, accidental exposure due to inadvertent leakage, spillage or release of substances cannot be ruled out. The types of substances which may be present in the workplace could include:

Chemicals.

Paints and coatings.

Hazardous metals.

Biological materials, pathogens or substances.

Pesticides.

Fertilisers.

Explosives or their components.

Cleaning materials.

Toxins and poisons.

Construction materials (e.g. glass fibres and asbestos).

Radioactive materials.

And under those broad headings, there are many different subsets of hazard which can affect personnel in the workplace. Any hazard through which short or long-term exposure can cause risks to health must be the subject of rigorous risk assessment and clear statements as to the protective measures to be put in place to avoid risk. Naturally, this will be the clear remit of the H&S department but, as before, the security officer may well be in a situation where they may be exposed to the hazards. Exposure to the hazards may be in any of the following forms (sometimes in combination):

Inhalation.

Ingestion (swallowing or drinking). Absorption through the skin.

It is therefore most important that security personnel are aware of the risks and the methods of protecting against them. Security officers must have clear instructions available to them on the actions that they should take if they or another employee are exposed to hazardous substances.

Personal Protective Equipment (PPE) must be available to provide respiratory and dermal (skin) protection to prevent exposure. There will also be a need for security personnel to be trained in the necessary cordon and first aid responses in the event of exposure of personnel if it is safe to do so.

You must consult with the H&S department on required and permissible actions in the event of personnel exposure to substances.

Your Responsibility to Your People

Apart from considering the general risks to employees within your organisation and the methods in which you can assist in enforcement, you should also remember your own direct responsibility towards your staff.

Security officers and staff can often be exposed to all the hazards that have been discussed in this unit, but also it is important to think about their routine tasks and duties which may engender risks. Consider the following:

Security personnel must be adequately trained and equipped for their duties. If required to work outside, they must be given weather-appropriate clothing. Do not assume that this is confined only to wet/cold weather as there will be implications from operating in hot weather. You may be required to provide sun protection clothing, sunglasses and even creams.

Security operatives who are required to patrol at night will need to be given adequate illumination, either as part of building structures or by issuing torches, or both.

The staffing and operation of control rooms is a potentially hazardous operation, particularly concerning the monitoring of CCTV and operation of IT. H&S and

workplace regulations cover these, and it is important to ensure that control rooms are set up to ensure that personnel are not exposed to injury.

Security managers are directly responsible for assessing and implementing protection measures and should consult fully with the H&S department on what needs to be done.

Reference and Guidance

The HSC and HSE website links are excellent sources of general information on general H&S matters. Another extremely useful reference is the 'Workplace Law Handbook', published annually, and the Workplace Law Network website, link: http://www.workplacelaw.net/

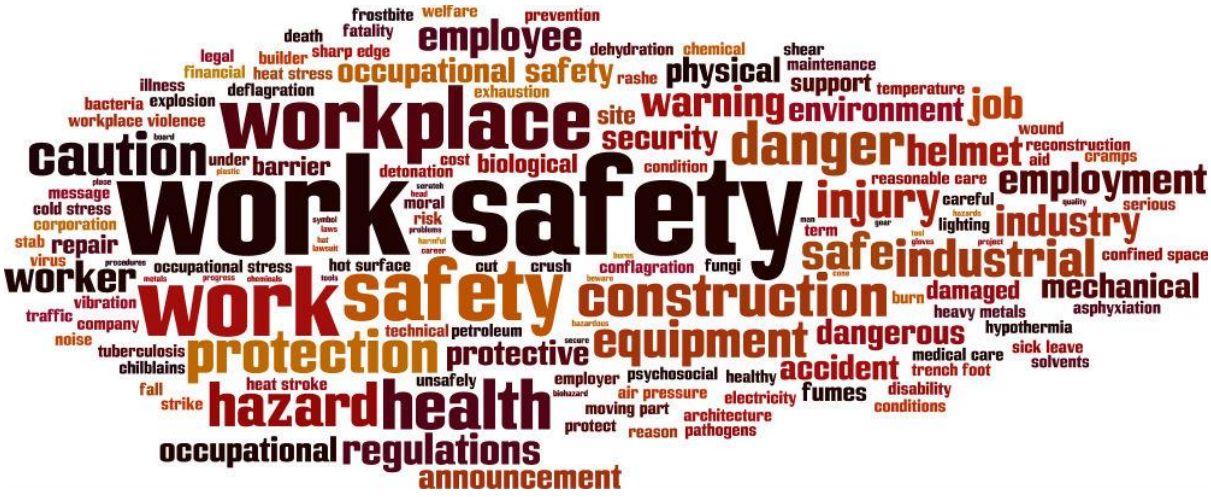
This provides background and easily understandable guidance on a range of H&S related issues such as:

Asbestos.

Biological Hazards.

Dangerous Substances. Construction Site H&S. COSHH.

Display Screen Equipment. H&S General.



PHYSICAL SECURITY OPERATIONS AND IMPLEMENTING SECURITY OPERATIONS

Introduction

The key purpose of security risk analysis is to provide the rationale for developing security measures that are above and beyond the baseline. This analysis process should be the basis for implementation of all measures including those for security of people, property, information and assets.

Risk

Risk Definition

Security risk can be defined simply as "the potential for loss". It is the product of three elements: Likelihood, Impact, and Vulnerability.

Vulnerability

The 3 components which must be considered, analysed, prioritised and managed in order that you can plan and implement appropriate protection measures are:

The Likelihood that a threat will become a reality is the first essential component and can be the most difficult to define, especially if it has never happened to the organisation before.

The impact of the threat becoming reality is easier to measure but needs to be considered carefully so that we neither apply over or under-protective measures.

The vulnerability of the organisation or its assets and the manageability of any threat to it will again provide an influence upon what you can put in place as appropriate security measures.

The Steps of Security Risk Analysis: Step 1 — Identify the Assets

The first step in the Security Risk Analysis process is to identify the assets. Most assets fall into one of three categories:

People

Property

Information

But there are intangibles, also, such as operational capability, relationships and knowhow.

The Steps of Security Risk Analysis: Step 2 Identify the Threats

Threat can be defined as "a potential source of harm". Many threats exist, and a threat doesn't become a risk to the enterprise until it can be assessed as having some measure of likelihood, some measure of impact, and the ability to exploit vulnerabilities.

There are many threat sources. In security threat sources are typically malevolent (deliberate) and may include a range of insider and outsider adversaries. Outsiders include those who may want to steal, harm the enterprise, force the enterprise to change policy, cause harm to employees or customers, extort etc.

The best way to analyse threats is to link that analysis to assets. Thus, in a threat assessment there are three fundamentally linked questions to answer:

What do you think are your organisation's primary assets?

The threat has never occurred in this sector or location and is unlikely to occur in the future.

Medium- The threat has occurred in this sector or location and has the potential to harm and cause pain

Events occur on a regular basis and are likely to reoccur in the future.

1. Who poses a threat?
2. What action might they carry out?
3. Against what asset?

Looking at the asset, action and adversary in this way can be referred to as the analysis of the "3

The Steps of Security Risk Analysis: Step 3 — Assess the Likelihood

Assessing the likelihood of a threat occurring is an imprecise science. In some sectors or businesses historical data will provide a good insight, especially where there is good incident reporting. At other times, it may be necessary to develop possible hostile scenarios and develop threat likelihood projects from that analysis.

Threats can be assessed as having a low, medium or high likelihood of occurrence.

The Steps of Security Risk Analysis: Step 4 — Estimate the Potential Impact

The next stage is to determine the potential impact if the threat materialises. Many organisations like to see impact expressed in monetary terms, but this is sometimes not possible, especially when dealing with injuries or fatalities. Impact includes not just asset loss, but denial (e.g. blockade), sabotage or destruction.

As with likelihood, impact can be estimated as low, medium or high.

Low- Loss or damage incurred would have negligible consequences or impact.

Medium- Moderate to serious consequences, leading to potential major financial loss, injuries or impairment of core functions and processes.

High- Grave consequences, such as large-scale loss of life, intolerable financial loss, injuries and impairment to core functions and processes.

Some oil companies break down impact using the PEAR system, allocating separate values for impact on people, environment, assets and reputation.

Potential losses can be categorised into two main types: direct and consequential. Direct loss refers to the immediate losses as the result of an event. For example, the direct loss of a vehicle may be

£l0,000 and such a loss can be offset and catered for by insurance.

Consequential loss is more difficult to predict with any degree of accuracy. For example, if a company has a spare vehicle, business disruption can be minimised. On the other hand, a small business which is critically dependent on a single vehicle for making deliveries to customers would have to hire or buy a replacement immediately or risk losing those customers.

As a rule of thumb, it is worth remembering that consequential losses are on average about ten times greater than direct losses.

Case Study

The following case gives an example of the impact of consequential losses:

MOLEYS Computer Services Ltd is a one-stop supplier of IT services to local businesses, employing a staff of 15. It supplies and installs computers and peripherals, provides web hosting services and back-up facilities for sensitive company data. The company is housed in a small multi-occupancy building on the outskirts of a town.

Last night a fire broke out in one of the computers. The fire service responded but by the time they had arrived the room in which the computer was housed was ablaze.

It took firefighters several hours to extinguish the fire. Initial estimates put the damage at £500K. The company does have insurance, but the offices have been extensively damaged and will be unusable for some time.

Consider the consequential losses resulting from an event such as this and the overall effect on the business:

Loss of operations (profit generating activities). Loss of profits.

Investigation costs.

Salaries for staff unable to work.

Loss of customers. Customers' losses.

Litigation.

Loss of credit worthiness.

Increase in insurance premiums.

Rehiring of staff.

Retraining of staff.

Cost of temporary accommodation and equipment.

Reconstruction of IT systems.

Reconstruction of infrastructure.

Restoration of communications.
Reputational damage.

Thus, an understanding of the potential impact of consequential loss is necessary to ensure that appropriate financial provision is made for security measures.

Failsafe controls are in place to deter, delay, detect and respond, providing a very low chance of an adversary success.

Low Reasonable controls are in place to deter, delay, detect and respond to the threat, but they are incomplete and not fully a lied.

Medium Basic controls are in place to deter, delay, detect and respond to the threat, but are relatively incomplete and can be easily exploited by an unsophisticated adversary

No controls in place to deter, delay, detect and respond, and therefore an adversary would easily have the capability to exploit and compromise the asset.

The following table provides a means to assess security vulnerabilities:

Risk Treatment

Having assessed and prioritised the risks we now need to consider dealing with them. This process is termed risk 'treatment' and is designed to mitigate or reduce the risks to an acceptable level. You should aim to drive risks down to a level termed 'As Low as Reasonably Practicable' or ALARP. This recognises the fact that there will always be a balance required between your wish to treat a risk as fully as possible and the cost and inconvenience of implementing protective measures. The point at which the costs and risks are balanced is the ALARP point, as illustrated overlay:

Failsafe

Under each heading for the 4

Reasonable Risk to ALARP T's, write an example of how your organisation uses that

Weak Low Moderate High method of risk mitigations

cost of security/inconvenience to business

Factors Which Can Limit Appropriate Risk Treatment

In an ideal world, the security manager would be able to follow the security risk analysis process and then apply the mitigation strategies freely. The application of mitigation procedures may need to be compromised if it has an adverse effect on organisational operations and outputs.

Businesses require open and unobstructed access to the marketplace and security managers need to ensure that they identify risk mitigation solutions that match equally the business operational requirements and culture and the prevailing threat climate. Other factors which may influence the choice of risk mitigation measures include:

Security Budget — Security measures should be able to demonstrate return on investment. Budgets are finite.

HSE Regulation Security measures should always take second place to safety considerations, which are often regulated by law.

The Law — There are laws governing surveillance, interviewing, human rights, data protection, arrest and much more. There are local regulations governing what defences you can put on tops of walls, the height of a fence etc. Ensure you are familiar with these and that you comply.

Customer Access Considerations — Perhaps you could reduce risk by building a 5-metre electrified fence around your premises, but what would customers think?

Your Location Think about your business travellers. How do you protect them from harm when they are overseas?

Security Risk Analysis Exercise — Hotel Mumzza

Introduction. The Hotel Mumzza is in UAE and is popular with foreign tourists and business groups. The latter, many of which are Western, regularly lodge their overseas business visitors at the hotel and use it as a conference venue.

Background Crime — UAE. There is little serious crime in UAE, although criminal gangs are known to use the state and its facilities to launder money. Theft, including theft of laptop computers and mobile phones happens, but the incidence is significantly lower than in European countries. Assault is very rare. The authorities are constantly concerned about the possibility of Al-Qaeda terrorists attacking Western targets. Al-Qaeda sympathisers are known to use UAE as a meeting point, but there is no history of any attack.

Background Crime — The Hotel Mumzza. The main problems in hotels, and the Hotel Mumzza is no exception, is theft. Theft is committed usually by staff against the hotel, staff against guests, guests against the hotel, guests against other guests or intruders against guests.

There have been several reported incidents of guest property (mainly cameras, mobile phones and money) having gone missing at the Hotel Mumzza in the past few months. Some of these have been assessed to be false insurance claims.

Recently, the head chef was dismissed for defrauding the hotel out of $150,000. He was operating a delivery scam in collusion with a supplier.

In the past five years, 18 of the 600 employees have been dismissed on suspicion of theft of guest property. Most of these have been from housekeeping, laundry, conference and banqueting or bar staff.

The Security Situation. Security at the hotel is not particularly good. There is a security manager and 6 security officers, but they are mainly involved in maintaining order in the hotel's 6 bars.

The hotel has a CCTV system monitoring the main entrance, lobby and several back-of-house areas. There is a total of 60 cameras, of which only 8 are linked to a recorder. The two monitors are not manned due to manpower constraints.

There are 23 entrances to the property, none of which are locked during the day and few of which are monitored by camera. There are several routes to guest floors, none of which pass by reception.

Guest rooms are secured by a card-key system, of which housekeeping, maintenance, guest relations, laundry and security staff all have masters. There is a safe in each room, but the master codes are assumed to be well-known amongst staff.

Conclusion

Successful security risk analysis will lead to successful, cost effective selection of mitigation and controls to deal with the threats to an organisation. The security risk analysis process should be applied to all the organisation's activities to avoid over or under-protection of assets and must also consider the potential external factors which can limit security activities.

Familiarity with risk analysis and the concept of direct and consequential loss are essential tools for effective security management and will allow the security manager to effectively plan and implement measures across the range of physical, personnel and information domains. The importance of risk be continual emphasised and revisited throughout this workbook.

PHYSICAL SECURITY OPERATIONS AND MANAGEMENT

Introduction

All buildings, facilities and areas used for organisational activity will need some form of access control. Every location and the actions conducted within and around that location require legitimate users to enter and exit whilst ensuring that adversaries are excluded. However, the risks from within an organisation can be worse than those from outside — so access needs to be controlled not only at external points but also within the workspace.

It is worth considering here that contractors, visitors and business partners, although entitled to some access to some areas, should be strictly controlled to ensure that they do not reach areas or assets which they do not need to. Access control is generally considered to consist of a system of badges and passes supported by locking systems; although they have an important part to play we must remember the value of sound procedures and employee awareness in controlling entry and movement.

Aims of Access Control

Well-implemented access control measures will be designed to ensure that the organisation can operate safely and securely and will have the following aims:

- To facilitate access for authorised people.
- To prevent access for unauthorised people.
- To prevent the unauthorised removal of property.
- To prevent the unauthorised introduction of property.

Facilitating Access for Authorised people

It is important to ensure that authorised people have access to appropriate areas of a site or building. Access must be as 'stress-free' as possible whilst maintaining appropriate levels of security to avoid unacceptable delays and congestion — the imposition of over-protective measures will serve only to alienate the workforce

Considering your own organisation, state the main methods by which you could implement access control by using procedures rather than physical security methods?

and engender a negative attitude to security personnel and procedures. There are several methods which can be used to facilitate access as follows:

Automated access management system - Such systems are in wide use and allow personnel to gain access without the intervention of security staff.

Multiple entrance and exit points on single gate - The use of one supervised gate with multiple access points will allow a larger, quicker throughput of personnel, thus reducing the inherent inconvenience of access control.

Target transaction times - Transaction time is that time taken for an individual to pass through an access control point and the security manager should aim for this time to be kept to a minimum level commensurate with the desired level of security.

Reliable technology with low failure rate Unreliable technology will increase transaction times, cause insecurities and alienate employees who need to use the system.

Written procedure for staff who have forgotten cards - Employees will forget cards and there needs to be a robust and reliable procedure in place to ensure that they and security staff know what to do in such an event (and the implications of it).

Written procedure and efficient and accountable system for visitor access Although visitors will have legitimate business and other reasons to be given access, this should not be uncontrolled, and a system should be established for visitors to go to only those areas that are necessary.

Well-trained, customer-focussed staff Customer care is essential for efficient access control for visitors and your own employees. This aspect of access control is also covered in Unit 3.3.

Preventing Access for Unauthorised people

Keeping unauthorised people out of a site or facility is often the main concern for the security department. Unauthorised access will engender many threats including theft, acts of violence or malicious damage. It is important that any measures put in place are thoroughly risk-driven and must be carefully thought out and implemented to ensure that the necessary level of protection is enabled. Various options to achieve this are as follows:

Monitoring the perimeter, especially weak points - Any site requiring access and exit will have potential areas of weakness at their perimeter. These must be closely monitored by security personnel either remotely using CCTV or in person by staffing gates and access points. Although this will be labour-intensive, it will offer the best chance of reducing compromise. Reducing entrance points to a minimum - In an ideal world, every site would have a maximum of 2 entrance points; the first as the main access/entrance and then a second as an alternate and emergency exit. Operational requirements and fire regulations will require many access points to be established. Don't forget windows!

Special attention to fire exits, especially when in use - Fire exits are often abused or left propped open by employees. These must be regularly checked to ensure that such abuse is minimised.

Safe activities to unsafe locations - This means that employees either congregate or operate in areas which are vulnerable.

An example is the locating of a smoking area close to or overlooking an access point — in this case employees will often challenge those who they do not recognise or who do not have the correct authorisation to enter. Strong form of identification checking an identification system is only as good as the staff who monitor and implement it and there must be procedures for checking identification which goes beyond the automatic access of 'authorised' personnel. Also, the system for checking visitor and contractor credentials must be robust. Staff awareness of walk-in thieves Despite best efforts to prevent access, walk-in thieves will find ways to circumvent systems - staff awareness is the key to prevent the situation developing by recognising potential intruders and, if necessary challenging them. At the very least, staff must be aware enough to report intrusions immediately upon discovery or detection.

Segregation of areas and compartmentalisation Not everyone within an organisation will be entitled access to all areas. Personnel should be restricted only to areas into which they 'need to go'. This principle, if properly enforced, is highly effective in reducing intrusion events.

Badge-based ID card system with 2factor identification - ID badges are effective when properly used and when more than one factor can be used to authenticate access privileges. The 2-factor system reduces the risk of forgery or badge misuse.

Efficient system for deleting former staff record and returning of cards.

Realistic card loss reporting and action system - If a card is lost the system must allow for prompt reporting and ensure that the lost card cannot be misused or used as a base for forgery.

Preventing Unauthorised Removal of Property

Remember - you are likely to experience more material loss from within your organisation than from outside - access control is also about ensuring that your property is not stolen.

Clear and well-understood policy - The policy for preventing removal of property must ensure that disciplinary or sanction procedures are in place and communicated clearly to all employees.

Material pass system - Any property or Notes asset which is to be legitimately removed from a site must be validated by and accompanied by a pass or document clearly authorising its movement and documenting its destination and the details of the person/persons entitled to carry it.

Cards for laptop "owners" - Similarly, those entitled to use company laptops and other equipment should have accompanying authorisation cards.

Random searching is an effective method of detecting the removal of property but must be employed carefully to avoid complaints and dissent. Searching is covered in detail in Unit 2.7.

Notice at entrance point - There should be clear signage at entrance points detailing the search and material pass systems and the potential sanctions for theft or unauthorised removal of items.

Asset marking - Assets may be overtly or covertly marked to ensure that they can be identified as the organisation's property Electronic, RF or GPS tagging Electronic tagging is becoming more common and will continue to do so in the future. Such tagging is effective in detecting

potential thefts and is used with great success in the retail environment, from where it will spread to other business sectors.

Preventing Unauthorised Introduction of Property

Property may need to be prevented from entering a site or facility for safety or security reasons. Whilst items such as cigarette lighters will be banned from high-risk sites such as petrochemical facilities the requirements for protection of information may involve the prohibition of recording devices such as MP3s, personal laptops, USB devices, cameras and mobile phones. The risks to organisations from allowing such devices to be introduced into the workplace are detailed in Unit 3.1. Measures to enforce exclusion of prohibited items may include:

- Clear and well-understood policy - A clearly set-out and explained policy should be put in place. This is critical to ensure that employees understand the reason for preventing access, which is essential when security may be perceived to be 'confiscating' personal property.

- Notice board with list of restricted items - To supplement the policy, the notice board must clearly and unequivocally detail the restrictions upon access.

- Random searching.

- Punishment of violators.

Methods of Facilitating Access by Authorised Personnel

Having established the aims of access control, we shall now consider the methods which can be used to implement appropriate security measures. When planning and enabling access by authorised personnel, you should consider the need to allow access for both vehicle-borne and pedestrian personnel.

Automated Access Management Systems

To ensure reduced transit times and to reasonably remove obstacles to entry for those personnel who may legitimately enter a site, automated access management systems are the most common option. These can be semiautomatic; that is operated by security personnel to allow entry once access has been authorised (such as a vehicle barrier or pedestrian turnstile). Alternatively, they can be operated fully automatically. The most common method of managing fully automatic entry is using access badges. Another option is to use biometric or pin technology to facilitate access. Once access is approved by the system, automated barriers will raise or open; if access is not approved the system will either lock or 'refuse' to function. These systems are discussed in more detail later in this unit.

Car Parking and Vehicular Access

The location and management of car parking facilities is an integral and important aspect of access management control. The requirement is to allow secure and trouble-free parking for employees and visitors whilst reducing access by all vehicles to the site.

The following points should be followed for parking and vehicular access:

For the most effective loss prevention, vehicle parking should be off-site and outside the main perimeter, with pedestrian access to the site only. In this way, individuals will have reduced opportunity to bring items into or out of the site. This system will also allow a stand-off distance between most vehicles and site buildings — which will be discussed in Unit 2.4.

Because deliveries and other vehicles will require access within the perimeter a tightly-controlled vehicle gate should be established. Access to this should be controlled by guards or card-operated for known users. In any case, visitors must be carefully controlled, and their credentials checked thoroughly before access is permitted. Car passes should be issued and be displayed in all vehicles. There may also be a requirement to issue zoned vehicle passes which will keep unauthorised vehicles out of restricted areas.

Vehicle registration numbers should be recorded in a visitor log for all vehicles accessing the site and employee cars should be recorded in a checkable database. Procedurally, it is essential that all employee and company vehicle details are updated whenever they are changed for any reason.

Access Management for Pedestrians and Building Access

Access management, once personnel are within the perimeter, is a matter of ensuring that entry to the building, and its sub-compartments is controlled. This layered process is a fundamental aspect of physical security and can be achieved by electronic systems, personal checking and the application of a security aware culture throughout the organisation. The design of an effective reception system (not necessarily staffed by security personnel) will be an essential component.

The aim is to ensure that first, authorised employees' identities are verified and that they have authority to enter a specific area. This may include but not be limited to the following:

When due to leave the company through resignation, dismissal or redundancy. Out of normal working hours or at weekends.

When they have no legitimate business in an area.

For 'unknown' personnel, the requirement is different in that we need to establish their identity and then ensure that they can legitimately enter the premises. This involves a more detailed check of the individual's credentials and more involvement by individuals within the

organisation. The security manager should consider the following measures to facilitate the process:

Regardless of the status of most individuals, they must check in to the site by signing a visitor's book and perhaps being issued with a photographic badge.

The organisation should send either an email or letter of invitation to the visitor detailing who they are to meet, where and when. If security requirements dictate, then the invitation should ask the visitor for vehicle details, a digital photograph or photographic identification.

All visitors should be met by the departmental host on arrival and escorted throughout the visit.

If the visitor is to be allowed access to the main building, employees should be warned in order that they are aware of the need for discretion and to protect sensitive information.

Consider allowing visitors only into dedicated meeting or conference facilities outside the main building.

Reception areas should be designed to control access to the main building. This can be achieved by locating comfortable seating, toilets and drink facilities in reception, thus giving visitors no excuse to enter the site without appropriate escort. Discreet surveillance cameras will be useful, and the reception should have clear signage to indicate security and safety requirements on site. The overall aim should be to ensure that security is as high as possible without undue intimidation of visitors.

Automatic Access Management

Returning to automated access management systems, this section of the unit will assess the operational requirements and technologies available for asset access and tracking within the facility.

Operational Requirements

The requirement for automated systems is to simplify access management and to reduce the need for excessive levels of security manpower whilst allowing employees, contractors and visitors the freedom to move around commensurate with their security status and clearance. Card reader access is the most common in use and should embody the following elements and properties:

List the advantages of using automatic access management

Validity - The system must be able to recognise known users with a very low margin of false rejection rates. Before any system is installed it must be clearly specified and tested to ensure that it meets this criterion.

Reliability - The system must demonstrate consistent performance with zero false acceptance rates.

Ease of use and speed of transaction from a user's perspective the system should be fast and simple. From a management perspective enrolment onto the system and card issue should be efficient, secure and quick. There is little point in installing a labour-saving system which requires extensive effort in terms of staff to administer and maintain.

Longevity - You should expect at least five years' life from all system components except the cards. There must be systems in place to ensure that personnel are aware of the need to replace damaged or worn cards.

Just as important as the physical and system properties is the need to have clear policies and procedures, properly enforced, for the use of cards. This should include such detail as:

When and where passes should be displayed, who has the authority to check the pass and the procedures for wearing (e.g. on the lapel or belt). It should also stipulate that cards are not to be left unattended such as on jackets hanging up or on desks.

Actions to be taken to retrieve and cancel cards belonging to employees leaving the organisation.

Card Layout and Contents

To be effective, the card should have certain physical properties that are designed to maximise their efficiency as security tools and to ensure that they are not prone to copying or forgery. The card should have the following design components:

Tamper resistance - Cards should be of a unique design which is imprinted into plastic. There are many card design companies operating in the market who can produce distinctive and complicated designs to your specification and requirements.

Strength - The card should be robust enough to withstand continuous use.

The card should have a clear colour photograph, at least 25mm square - The value of any photograph is reduced if the facial details are out of date. Therefore, they should be updated at no more than 3yearly intervals to reflect changes due to ageing, changes in hair (facial and on the head) and the wearing of spectacles. In any case, the wearer must be clearly identifiable from the photograph. To test the efficacy of your own system, check the passes worn by your company staff against their facial features.

Some passes may include height, weight and other vital statistics - Care should be taken not to offend individuals by requesting such information if not considered by management to be necessary.

Holography or 'smart card' - There may also be reading technology incorporated into the card to increase security and to store additional information.

Zones - The card should either be colour coded or give a clear written indication of the zones or areas which an individual can enter.

Rear of the card - Should carry no security information such as emergency actions, any H&S notices and restrictions.

A good example of the layout of a card and of the amount of detail which can be included is the UK photocard driving licence.

Using the Card

The card access process and its linkage to automatic systems needs to ensure that access is

Most organisations have a card/badge access system. Thinking of your own system, compare with the previous list of requirements and details and list the improvements or refinements, if any, that you could implement Remember to consider the possible inconvenience to users and the requirements for controlling access to sensitive areas,

rapid and that only authorised personnel can enter a facility. Also, it is useful to track individuals' movements once they are within the facility.

There are various options for using automated access management systems to track movement within a facility. Each option has its advantages and disadvantages:

The use of a card to enter a building and a push-button or switch to exit is most common in smaller organisations as it is relatively cheap. This system is limited in that personnel leaving the room or facility cannot be identified or tracked. Also, employees working inside can easily and undetectably open doors to allow unauthorised and unidentifiable access for others.

Using a card to both enter and exit a building is a better option as it can be used to track personnel quite well if properly networked. Precautions should be put in place to ensure that the card cannot be passed back through the barrier to be used by an unauthorised person.

Card entry and exit along with internal movement controls by card swipe is useful but the main threat to its effective use is abuse of the system by employees. Unless procedures are explained and enforced, and because of human nature, there will be many cases of employees allowing others into certain areas using their own card. This negates the usefulness of the system.

The system of card access and internal movement controls can be further strengthened by dual factor authentication; that is using a PIN to authenticate movement. Target transit

times and expense will be increased but the risk assessment will dictate whether installation of such a system is justified.

Card entry can be authenticated by a security guard at the point of entry. This is a labour-intensive method, but it can be effective in that personal recognition is a reliable way to verify ID. Some card access systems will also allow a guard to compare a database-stored photograph with the individual attempting to gain access. The potential setback with this system is that it Notes relies heavily on the level of training, diligence and integrity of the guard.

Electronic Access Control Systems

Electronic access control systems are the most common method for managing access. Although such systems can vary in terms of cost, reliability and quality, if properly planned, specified, installed and used, they have clear and obvious advantages over mechanical or manual systems operated by guards. Regardless of the keying method, all electronic access control systems have the same fundamental architecture, designed to delay, detect and allow a response should the system be breached. It is important to re-emphasise here that no access control system can be relied upon to keep intruders out and that without a credible response, any system can fail.

Electronic Access Technologies

All access badges and methods are not the same and there are various technologies available to operate electronic access control and management systems. Each system has its advantages and disadvantages and the decision to use a type will depend on factors such as cost and ease of use. The cost is not simply associated with a card or badge, but also with the technologies required to read the card and the requirement to maintain them. As a minimum requirement, card systems should be robust enough to withstand wear and tear caused by constant use — they should also be capable of rapid and prompt cancellation should they be lost or stolen.

The main types of card technology in wide and current use include:

• The 'simple' and common magnetic swipe card is an effective and relatively cheap access control method. It is best used with an authenticating PIN, but this can lead to delays in access. Although it is easy to use and can store substantial amounts of information it can be easy to copy — for example the magnetic swipe cards used by many hotels can be a rich source of information for

dishonest employees. The main setbacks with these cards (and their readers) are their susceptibility to malfunction, if the swipe strip is damaged or dirty. The proximity of magnetic media to the card (for example a mobile phone carried in the same pocket or handbag) can cause the information on the card to be corrupted or erased.

Wiegand cards provide a higher level of security and resilience than magnetic swipe cards. Their information is stored in a unique pattern of small magnetic wires embedded into the plastic card. The information in Wiegand cards cannot be updated once loaded in, but they can be used as proximity cards and are more effective than swipe cards in external locations.

Smart cards are plastic cards which store vast amounts of information on an embedded microchip. Smart cards fall into two main categories; those containing an active microprocessor and those containing a read-only memory microchip. Active microprocessor cards are, obviously, the more versatile as they have local read/write functionality. As access control cards, they often perform the dual function of access/Id. card and refillable stored value card, which can be used in company restaurants and vending machines. Increasingly, there is convergence between physical security and IT security access control, as the same card becomes the token for both types of transaction. Some smart cards work on contactless technology giving all the benefits of proximity cards. Others store biometric information, which can be read and compared with the holder's biometric attribute. This is especially useful where access is required to many different sites and by delivery drivers accessing sensitive areas. In the case of the latter even the cargo manifesto can be stored on the card.

Proximity card is a generic name for a contactless access control card. It can use a variety of active and passive Radio Frequency-based technologies, including Wiegand and Radio Frequency Identification more commonly referred to as RFID. This is the term for wireless noncontact systems that use radio frequency electromagnetic-fields embedded in the card to transfer data to the card reader and can incorporate embedded smartcard chips. Many proximity systems require a card to be positioned next to a reader, often while remaining in a wallet or handbag. Others offer a much greater range, such as for use with vehicles accessing car parks. Some companies issue employees with separate photo ID cards and unprinted proximity cards. This is not good practice since the proximity card could be easily used by an illegitimate user if in a stolen wallet or handbag. This problem is further exacerbated by the implication that proximity card holders do not use PIN numbers.

Biometric Technology

Biometrics — the measurement of a person's physical attributes against stored information or standards is the most rapidly evolving of access control technologies and is becoming more common across a wide variety of applications. At the time of writing, biometric technology can be used to identify and verify identity through measurement of the following physical attributes against stored data:

, Fingerprint.

- Eye pattern (retina and iris).
- Hand and finger geometry.
- Facial recognition.

- Voice recognition.
- Hand vein (vascular) recognition.

Biometrics are not fool proof systems yet and systems need to be carefully selected to ensure that they are of the required quality to avoid false acceptance or rejection of persons attempting

Biometric access control systems are widely used and increasing in popularity — what are the advantages and disadvantages of linking such systems to networks and databases for controlling access within the organisation? They can also require lengthy transit times due to the need to check details against databases. Also, criminals are reported to be able to fake fingerprints and are working on other methods to defeat biometric devices. Biometrics are still in the relatively early stages of development and we can be confident that their use will become far more widespread in the coming years.

Visitor Badges

Visitor badges may use some or all the above technologies, but it is important to consider these badges as temporary. If they are to contain access information, then it is most important that they are closely managed and authorised and cleared only for specific visitors for a specific time. Security staff must ensure that visitor badges are managed as follows:

All badges must be clearly numbered and accounted for.

It must be the responsibility of the host to recover the badge from the visitor and ensure its return.

The badge should confer no or very limited access privileges. To avoid unmonitored movement, badges must always be deactivated when not on issue. Emergency information on back of card. Colour coded for escorted or non-escorted — the best method is to always escort visitors!

Access Management Handling

Personnel

Earlier in this unit we discussed access management for pedestrians and building access. Once inside the building there will still be a need to control and monitor movement. Security need to ensure that access is only granted to those who have a need to be there and that means that access to some areas will be prohibited for most people. Because employees will often compromise security procedures to make their own lives easier, the best method of restricting access will be a combination of procedures and physical security measures. Disregarding these procedures poses the biggest threat to security and the physical measures must be thorough and well planned to avoid the undesirable issue of inconvenience.

Visitors

Every business receives visitors daily it is a fundamental part of business operations. However, visitors bring their problems, particularly if they have malicious intent. It is worth remembering here that thefts often take place because an opportunity is presented, and the act takes place on the spur of the moment. Access control will reduce the opportunity.

When dealing with visitors it is generally important to ensure that we avoid offending or intimidating them by overbearing or hostile security procedures. The aim should be to ensure that the visitor feels that they are not being constrained or suspected of potential hostile activity — remember that most visitors will have no malicious intent.

Security staff must ensure that visitors are processed efficiently and that no prohibited items are brought in. If security have been pre-notified of a visit (and they should be!), visitor details should be held at reception or the access point with a prepared access badge or other documentation. If the reception area is covered by CCTV it may be a worthwhile tool for allowing the host to verify the visitor's identity. Even if full details are held, security staff should ask the visitor for photographic identification and to state the reason for the visit and name of the host.

The visitor should be held at the reception point whilst the host is notified of their arrival and should not be allowed to enter the facility unaccompanied. At no stage should the visitor be allowed to move around inside the facility alone and it is the job of the security department to raise awareness within the organisation and to encourage a 'challenge culture' where unrecognised persons are immediately questioned about their activities. The host should be

responsible for the visitor throughout the visit and will be responsible for returning the visitor badge at the end of the visit. The badge must be cancelled immediately.

Before allowing entry to a site, if any goods or items are prohibited then the visitor should be encouraged to declare them and deposit them at reception. A notice should be located at the entrance in clear view of visitors and hosts reminded to inform guests before arrival. Security officers must ask visitors as standard procedure — an example of this type of activity being carried out as a routine is at airport check-in desks. Many people will feel uncomfortable about handing over their personal property and to make the security system work secure storage and receipts or tokens must be provided.

Contractors

Contractors work in a position of trust within many organisations and often have privileged access to many areas of operating and administrative sites and facilities. Security managers and

their staff must be extremely vigilant where contractors are concerned as they are a rich source of potential losses to the organisation. They have no real connection or loyalty to your organisation and may not feel that security rules and other regulations apply to them. It is important to ensure that their access to your facilities is balanced with an appropriate security regime. The following measures can be considered to ensure an appropriate level of security:

A separate access control point should be considered for contractors to ensure that appropriate control of entry and exit exists. A separate ID system. Daily token to be issued on production of photo ID and checked against list of contractor names.

Consider security wrist banding - these relatively cheap bands can be issued daily to contractors instead of badges.

Separate toilet facilities.

Separate off-site parking.

Fenced-off building site. Contractors will take every opportunity to smuggle items out of their working areas and into parking Notes areas. You must make it as difficult as possible for them to do this.

Conclusion

Access control is not simply a matter of keeping people out of a site. Those personnel who have legitimate reason to be on site can, if not adequately controlled and monitored, be responsible for huge material and information losses. It is the role of the security manager and their staff to design, plan and implement appropriate security measures to ensure that access and movement are managed to reduce the risks. As with all other physical security measures, security managers must - ensure that any measures put in place are risk-commensurate and cost effective.

Your greatest weapon, and conversely your greatest potential problem, is the lack of security awareness of staff and departmental managers which will do much to ensure that unauthorised access and movement are challenged and reported. There are many electronic and mechanical devices available to you to control and manage access both inside and outside buildings but without procedures and security awareness, these will be useless.

THE EFFECTIVENESS OF SECURITY MEASURES.

Introduction

perimeter may be natural or (manufactured), or a combination of to understand the limitations security perimeter. A typical for example, comprising a 2.4m fence with 450mm coiled razor provide a delay of no more than against a determined and skilled basic requirement of an effective

Place a clear boundary around your site and other premises. Use zones within your areas to safeguard assets of highest Transfer fear of detection to adversary but be aware that an adversary may not be put off. Deploy physical measures to slow adversary. Implement as many cost and risk security measures.

Detection is more effective when sterile zones either side of the Deploy appropriate measures such to notify response.

Adversary chooses weaker to difficulty of penetration.

Persons attempting entry or exit authorisation, and notify the police

A physical security structural both. It is important of a physical “security fence", high chain link wire topping May stop a 10 seconds intruder.

There are 8 perimeters:

1. Demarcate between
2. Delineate perimeter value.
3. Deter - potential determined
4. Delay - down an
5. Deny - commensurate 100% denial
6. Detect - there are fence. as PIDS
7. Deflect target due
8. Detain - without as appropriate.

Balancing Delay, Detection and Response

To be effective a perimeter must be able to deter, delay and detect any unauthorised intrusion. It must also be linked to a credible response. This is shown in the simple equation: Tp>Td+Tr (time of penetration must be greater than time of detection plus time of response). In practice this means that if the fence crossing time is assessed as 10 seconds a credible response must be able to stop the intrusion in less than 10 seconds. Ways to satisfy this equation include:

Strengthening (or electrifying) the fence to give a greater delay value. Improving detection capability and reliability.

Locating the response close to areas of vulnerability.

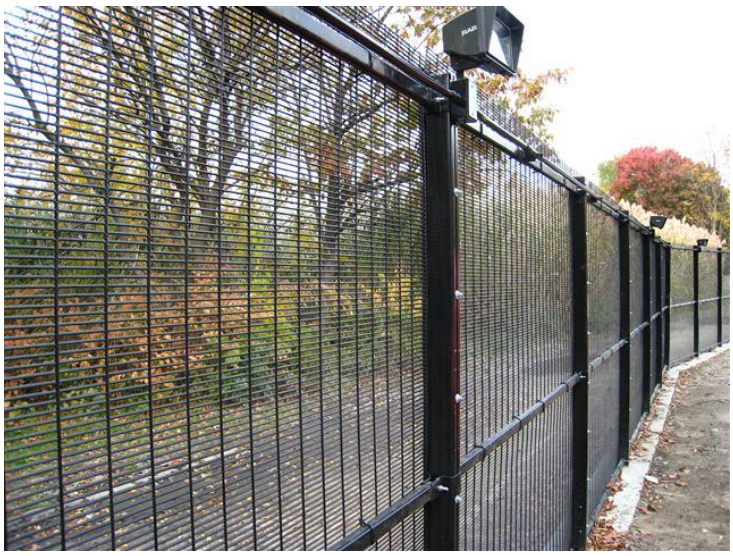
Providing the response with a fast means of transport.

Layering the Perimeter to Provide Defence in Depth

It is important to bear in mind that any security system is only as strong as its weakest element or point. Whenever security is applied to protect an asset it should take the form of layers. No single physical control can provide 100% protection.

The outer layer of protection for a facility often depends on the environment. For example, a corporate HQ in an urban setting may have just its building walls as the first obvious layer, whereas a manufacturing facility on an industrial site may be able to benefit from a perimeter wall

Thinking about your own workplace, what could you improve or upgrade to increase perimeter protection? There can be many layers of physical security surrounding a high-risk site. In this example they include: the fence itself; sterile zones outside and inside the fence; a monitored detection zone, which may extend beyond the perimeter; lighting; CCTV; perimeter intrusion detection systems; patrolling guards; hostile fence topping etc.



In all cases the type of layered security must be consistent with the assessed risk.

Fencing Options

Chain Link - The most common perimeter barrier is the fence. Fences come in many different styles, fabrics, sizes and qualities, the most common of which is the relatively cheap, and relatively insecure, chain link fence. US Army tests have shown that a 2.4m chain link fence can be defeated in less than 10 seconds. This time is dramatically reduced if the intruder is assisted.

Chain link fencing can be defeated by climbing, burrowing and by lifting the 'skirt'. Some basic principles of chain link fencing are:

Minimum 2.4m high, with 0.6m coiled razor wire topping to take height to 3m.

At least 9-gauge wire thickness. Constant surveillance of fence as easy to cut.

Coiled razor wire on inside face makes penetration more difficult.

Should be checked regularly for evidence of compromise.

Some sites, particularly military ones, use chain-link fence in a double skin configuration. However, this does not significantly increase the delay value unless:

The area in between is patrolled, or

The area in between is alarmed, or the area in between is filled with razor coil, or

The intruder can be prevented from using a ladder to lay across the two fences.

The British Standard for chain link fencing is BS 1 722.

Palisade - Palisade fences are very popular in urban settings, especially in the UK. They are more expensive than chain link fences but are generally more aesthetically acceptable.

Palisade fences are available in a variety of heights. Some palisade fences are made from poor materials, or have poor fixings, making them prone to defeat. In some instances, burglars have broken a bottom securing bolt and have swung open the corresponding 'upright' on repeated occasions to gain access.

Palisade fences are generally erected without hostile topping, but it is a relatively simple task to mount atop flat-form coiled razor wire. The British Standard for palisade fencing is BS 1 722112:1999.

Welded Mesh - Welded mesh fences provide a much higher degree of protection than chain-link but are more expensive. Like palisade, welded mesh is available in a wide range of qualities, and the imperative must be on the security manager to ensure that they have obtained materials of appropriate quality.

What are the advantages and disadvantages of each fencing option?

Welded mesh fences, unlike chain link, are relatively rigid, which allows for the support of a wide range of perimeter intrusion detection systems.

Good quality welded-mesh fencing provides excellent protection and, as such, is used extensively in high security applications such as prisons, where it can be several metres high. This type of fencing, although relatively expensive, should be a first consideration when designing protection for a high-risk site.

The British Standard for welded mesh fencing is BS 17221 12:1999.

Walls - Provide an alternative to fences, with the added benefit of screening, but do not necessarily provide a greater level of physical security. The decision to erect a wall or fence will depend on—many acceptability. For small sites, on which there is no overnight guarding presence, walls are obviously better since they do not allow outsiders to see what is stored inside. On the other hand, walls are a hindrance to patrolled sites, as security staff cannot see what is happening on the outside of the perimeter.

The Workplace Law Security Management Special Report 2006 makes the following recommendations about walls: If the premises perimeter has a wall it should be:

Of substantial construction i.e. of bricks, cement blocks or stone.

Minimum of 3m high.

Minimum thickness of 100mm.

Smooth surfaced to hamper climbing. Enhanced by placing anti-climb devices on the top, i.e. barbed tape or spiked rollers etc. (depending on the threat). Kept clear of external structures which may facilitate climbing.

Kept clear of foliage and trees which may facilitate climbing or cause structural damage.

What are the advantages and disadvantages of a wall?

Gates

Any gate in a perimeter must present an equivalent security value to that of the perimeter fence or wall whilst acting as a legitimate entrance/exit for staff and visitors. The following criteria should be met for all gates in the perimeter:

Same height as the fence or wall. Hinges capped to prevent levering the gates.

Gates padlocked with a high-security closed shackle padlock fitted on a steel sliding locking bar. Chains should not be used.

For double gates the closed leaf should have a steel bolt padlocked into a steel sheaved hole in concrete.

Where possible a single leaved hinged gate or a steel sliding gate should be utilised and secured against the wall or a steel fence post.

To control routine vehicle access there may be a need to utilise a drop arm or lifting pole barrier controlled by a card swipe access, proximity card system or intercom/CCTV. Ideally, these barriers should be inside the main perimeter gates to enable the site to be secured out of working hours.

Where vehicle access is required on sites where a higher level of security is desired and there is available budget, the following measures can be considered:

Sliding gates.

Rising step barrier.

- One-way plates.
- Rising bollards.

For higher security sites consideration needs to be given to the positioning of the perimeter gates so that entryway tailbacks during times of increased alert do not interfere with the nearby public road system whilst vehicles are being searched before access to the site is permitted.

What are the main disadvantages of a gate?

(Source: Workplace Law Security Management

2006 Special Report (Stewart Kidd))

Each gate is a potential weakness therefore the number of gates should be kept to an absolute minimum, consistent with operational requirements. The physical security standard of the gate should match that of the perimeter fence, especially if the gate is not staffed during hours of darkness. This means that if there is hostile topping applied to the perimeter fence, this should be applied to the gate as well. Alternative gates which are infrequently used constitute a vulnerability, especially if they are secured by padlock. Padlocks can be removed and substituted. Worse still, if a person has legitimate access to the key, they may substitute not only the original lock but also the keys on the key ring with a copy of their own.

Perimeter Intrusion Detection System

The term Perimeter Intrusion Detection System (PIDS) is the name given to the use of dedicated electronic systems which detect and notify any intrusion, or attempted intrusion, through a specific external area, usually, but not always, a boundary.

Technologies used in PIDS systems include, but are not limited to:

Taut wire.

Vibration.

Electrostatic disturbance.

Magnetic field disturbance.

Ported coax (RF).

Acoustic.

Fibre optics.

Balanced pressure.

Infra-red (passive and active).

Microwave.

Electrified fence.

CCTV, coupled with video motion detection (VMD) and a suitable lighting source, could also be considered as a PIDS. CCTV is covered later in this handout.

Application of PIDS

In some environments, where the cost of providing effective protection by security officers is too high, PIDS are used in conjunction with rapid response units as a cheaper alternative.

PIDS can also be used to reduce the area size requiring protection. Many sites fence in large areas of open space unnecessarily. By redefining the perimeter of the most sensitive areas, PIDS can be deployed to protect only those areas, with or without demarcation fences and signs. Such systems are particularly useful on very large sites, such as refineries and airfields, where, even if it were feasible to alarm the entire perimeter, the intruder could easily disappear into the interior of the site before the arrival of the responding officers.

Classification

PIDS can be classified under many different headings. Some experts, for example, break them down into two groups; terrain

following and line of sight, whilst others classify them according to the technology used, e.g. proximity, contact and beam disturbance.

A particularly useful way of presenting PIDS from the educational point of view is to classify them according to where they are sited in relation to the fence:

Some systems are designed to be mounted directly onto the fence (1) and will alarm when an intruder meets either the fence or the sensor itself.

Some cable sensors can be buried to run parallel with the fence (2). Such sensors can also be configured to give warning of activity outside the fence, if required. Buried sensors can overcome the difficulties posed by perimeters which include areas of undulating terrain.

Post-mounted sensors create a line-of-sight invisible inner 'fence' (3) and serve the additional function of deterring employee misconduct near the perimeter.

Both post-mounted and buried systems require a sterile zone adjacent to the inner face of the fence. Accidental interference with this zone, such as stacked pallets, parked vehicles and construction works will significantly undermine the effectiveness of these systems.

Example — Fence Mounted Fibre Optic

Several kinds of sensor systems lend themselves to fence mounting, Including electrified fences, taut-wire fences, microphonic cables and fibre optic cables. In some cases, the sensor augments the fence by being attached, whereas in other cases (e.g. taut wire and electrified fences) the sensor may make up the entire fence.

Here are some of the characteristics of fibre optic cable.

- Very flexible in terms of deployment— can be attached to a fence, buried or used in conjunction with communications cabling.

- Contains a beam of pulsed light which when broken through interference activates alarm. Can be hidden in certain fence specifications making it undetectable.

Can be deployed over miles of fence length without requiring power or electronics.

- Generally, very reliable but expensive.

Example — Buried Ported Coax

Buried sensors can include ported coaxial cable, pressure-sensitive pipes, magnetic anomaly sensors and fibre optic wire or grids. Some of the characteristics of ported coax, a very common kind of cable are:

What are the advantages and disadvantages of each type of PIDS?

Notes

Creates an active detection field which activates an alarm when disturbed. Most effective when deployed in large clear zones of 6m or more.

Covert nature makes it undetected to an adversary.

Subject to nuisance alarms if large vehicles or burrowing animals are nearby. Should not be used near to running water, either surface or subterranean. Ensure you know the location of

water pipes entering and leaving the facility as sensitivity adjustments may have to be made here.

Sensitive zone is often up to 1m above ground and 2-3m wide.

Example — Post-Mounted Microwave

Post mounted PIDS have the advantage that they need not run directly alongside a perimeter fence, although most do. The two primary technologies used are active infrared beams and microwave (illustrated below).

Must be deployed across zones where there is a clear line of sight.

Microwave beam when interrupted will activate alarm. Invisible to potential adversary.

Will activate false alarms if grass becomes too long or detects animal movement.

Not reliable close to moving water as it will pick up movement from ripples. Do not use on rough or dipped ground.

Perimeter CCTV

Perimeter CCTV has become an important extra to perimeter security, and works particularly well when integrated into other systems, such as access control and PIDS. Perimeter CCTV is a primary means of PIDS alarm assessment.

To be effective a perimeter CCTV system should serve as a deterrent to a would-be intruder or to an employee seeking to use the perimeter as a means of removing property. Thus, the system should be carefully designed and thought out to deliver 24/7 coverage and recording of all areas of the perimeter. Many systems fail to achieve this, and the blind and weak spots are relatively easy to identify by any person serious on malicious intent.

Entire perimeter in field of cameras as opposed to PTZ to fill gaps. Don’t rely on guards to monitor images. I camera per Ensure adequate lighting throughout field of view.

If the budget extends to PTZ (Pan, Tilt, Zoom) cameras, then this money is far better spent on ensuring that the camera lenses are of high quality, that the image transmission ensures that images received are crystal clear, and that there is sufficient hard drive capacity to record images from all cameras at an appropriate frame rate for the required length of time. Lighting Introduction

Functions:

- To remove darkness as this is a cover for criminals.
- To allow for normal business activities at night.
- To allow for security activities at night.
- To provide illumination for CCTV.
- To reveal the movement of any person
- As a cover for moving patrols.

Areas to Illuminate

Protective lighting systems should be deployed to illuminate at least a site's perimeter, and especially sensitive areas or structures that are close to, or traverse, the perimeter (such as roads, piers etc.) and all internal areas of a sensitive nature. These might include:

Vulnerable or mission-critical facilities.

Finished goods storage areas.

Vehicle parks.

Fuel points.

Administration and headquarters building.

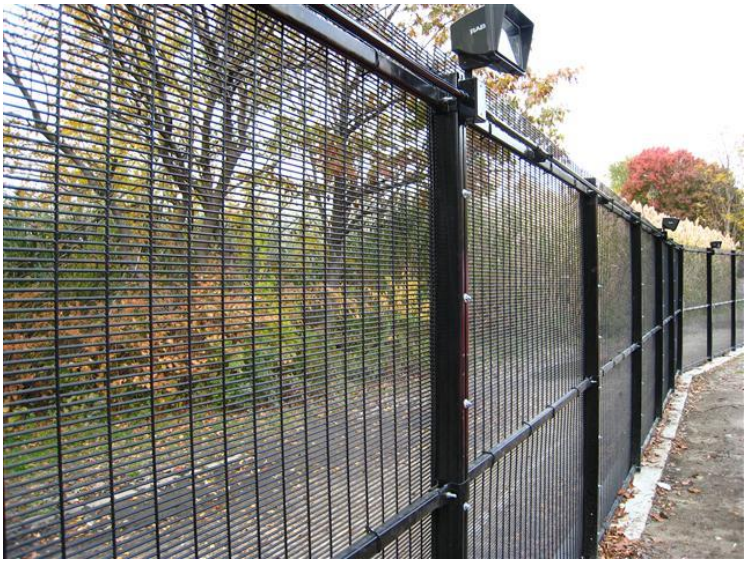
Communications control points.

Generating facilities. Etc.

Perimeter Lighting

Good perimeter lighting increases the security of the fence and increases the chances of security officers detecting any loiterers outside the fence or any attempt to climb or interfere with the fence and its gates. It also serves as a significant deterrent. Lighting should also be of a standard which would enable security officers to detect any attempt by a dishonest employee to throw stolen property over the fence onto the outside.

In practice much perimeter lighting takes the form of standard columns, located 1-3 metres inside the perimeter, onto which are fixed downwards facing sodium-based (orange) lanterns. Such a system often extends to cover the area within the site.



The advantage of such a system is its relatively inexpensive running costs, when compared with other, more radiant, systems. It is also virtually "off the shelf" since the same columns and lanterns are used extensively in street lighting.

In most cases, standard low-pressure sodium (LPS) lanterns are used. In contrast to other

Consider the types of lighting currently in place — evaluate their effectiveness for your site and recommend replacements or improvements to better support PIDS, fences and

CCTV measures

lighting systems, LPS lanterns are relatively inexpensive to purchase and operate. The main disadvantages are the poor colour rendition and relatively short range of operation.

For higher security applications, high-pressure sodium lanterns provide a reasonable alternative.

Most perimeter illumination takes the form of strip lighting (below).

Checkpoint Lighting

Good checkpoint lighting will enable security staff to effectively check pedestrians, vehicles, goods, documentation etc. Lighting inside the gatehouse should be subdued. Outside lighting levels should be such that no intruder can pass by unnoticed. Floodlight lanterns should be sited in such a way as to illuminate vehicles as they enter the site and wait to be processed.

Conclusion

Perimeter protection requires a combination of effective planning and specification, supported by rigid enforcement of procedures and control measures. If properly planned, a perimeter protection system will allow your organisation's operations to continue as securely as possible whilst maintaining a degree of control and some freedom of movement for those who need it.

The ability to conduct a risk assessment will allow protection and freedom of movement due to the appropriate selection of perimeter protection. If inadequate thought is applied and selection of perimeter barriers is not done carefully, security will not be achieved, and the risks will become a reality.

PHYSICAL SECURITY

Introduction

Since buildings usually contain a company's key assets, these are usually the areas on which a business focuses the greatest security attention. Once an intruder can gain illicit entry into a building they will be able to carry out their action unobserved and undetected, unless the building's security has been designed and configured correctly.

Perhaps of even greater concern than intruders are employees, since it is they who usually have legitimate access to many parts of many buildings. In terms of assets lost, research has shown that the cost of staff theft is often as great as or higher than that of the cost of loss at the hands of intruders. One reason for this is that many security systems are configured only to detecting a threat coming from outside the premises.

There are many potential adversaries to buildings and their occupants:

Walk-in Thieves, Maintenance Contractors, Public, Journalists, Spies, Protestors, Terrorists

Risk Analysis — The First Stage

As for any protection system, the first stage in any consideration of building security is to conduct a thorough risk analysis to define the threats and to consider the appropriate mitigation measures. Possible mitigation measures will be covered in detail in this unit and your selection of the appropriate measures will depend as always on the assets and operations at risk, the potential adversary threat and the potential impact of losses. These elements will dictate your

Can you think of any additional potential adversaries to buildings and their occupants?

selection of protection measures and systems — as will the cost of installation.

Adversary Routes for Illicit Entry

The range of adversaries mentioned previously will have many different motivations and potential methods for gaining unauthorised access to buildings and it is important to ensure that as much as possible, these routes are blocked. Some possible scenarios are shown below with suggestions for mitigation:

False ID, perhaps posing as a contractor or maintenance person - This risk should be addressed by ensuring contractors are registered and by prior liaison between the contracting company, the host and the security department.

An employee intent on committing a malicious act during working hours - Reducing opportunity, reducing anticipated rewards, increasing risks to offenders, compartmentalisation and on-need access control, patrolling, and CCTV are all tried and tested ways to reduce this exposure.

An employee entering a premise after working hours on a pretext, but with intent to steal - An employee should obtain line manager authority to enter after normal working hours. This permission can be emailed or phoned through to security.

An employee staying back or hiding after work with the intention of committing a malicious act - Security personnel should search and clear all potential hiding locations during lock up patrol procedure and these should then be secured and alarmed as appropriate.

Legitimate access to one building, or a part thereof, then using that access privilege to enter another area with intent to commit a malicious act - Access privileges must be strictly enforced regardless of the individual's position.

Forced entry (e.g. burglary) - Physical security measures, including locks and access control systems must be in place and robust enough to delay an adversary to allow effective response.

By tailgating a legitimate employee - Security awareness of all personnel is essential to ensure that each employee is careful in closing access points securely behind them and is prepared to challenge anyone who attempts to tailgate through a door or gate.

By access card pass back collusion between an employee and another person Again, security awareness is essential to prevent this; as is a system for discipline or sanction of employees who allow others to use their access cards.

By employee collusion (e.g. opening a back door for an intruder) - As above.

By smokers leaving a back door open in error - Security awareness and the use of signage and posters.

By poorly secured or poorly fitting doors Good door security depends upon regular inspection and maintenance. Regular and programmed security surveys and audits will detect such deficiencies if carried out correctly.

Buildings Protection during and after Working Hours

During working hours emphasis should be on creating deterrence, layered access control, and monitoring for deviance. After working hours emphasis should switch to searching and sealing

the building, both internally and externally, the activation of intrusion detection systems and lighting and the positioning of a credible response, usually a security officer. Deterrence is especially important, and this can be achieved in many ways, not least of which is unpredictable patrolling.

Working Hours - The advantage during normal working hours is that there are more staff within the building and this can be an effective deterrent. However, more people means that more access points will be in routine use and

How can the security of doors and windows be improved?

there is a higher chance that an adversary can gain access either through a routinely used door or gate but also potentially through unsecured and unlocked fire doors and windows. Therefore, there must be a strictly and fully enforced system of access control covering all such potential routes into the building.

These will include manned access points, the locking of unused entrances, the control of access to sensitive areas, and the use of swipe cards and ID badges. There should also be systems in place to prevent tailgating and to meet and escort visitors.

Patrolling - Security Officers should be aware of routine delivery and working patterns and behaviour, have access to a list of expected visitors and become familiar with the workforce in all departments. Patrol patterns should be planned to cover a vulnerable area especially during periods of high activity. A culture of security awareness within the organisation can be very helpful as members of staff in all departments will be aware of what normal behaviour is (and thus what is not).

Because the building will not be as tightly secured physically during normal working hours there will remain a need for passive detection systems to cover access and exit points and other potentially vulnerable areas. High levels of human and vehicular traffic will prevent the use of IDS in most areas and thus the optimum method is the use of CCTV monitoring. Cameras should be continuously monitored and properly sited to ensure coverage of the correct locations and activities. There are many different types of CCTV system which can be specified, and these will be covered in detail further in Unit 2.5.

After Working Hours - During the quiet hours when routine activity has ceased, there are few or no staff using the building and it is dark, the requirement for premises security changes and methods of enforcing it need to change also. Once all routine activity has ceased the first stage is to search the building. All areas, including store cupboards and toilets should be checked.

At the same time, occupants should be beginning the process of sealing the building.

All external windows should be locked and checked, and office doors secured on exit. The final phase of the sealing process will be to close the final access point or door and secure it accordingly.

Once the building is sealed, the Building Intrusion Detection Systems (BIDS) can be activated to ensure that any attempt to either breach access controls or to move around the interior of the building can be detected. Thus, the building should have both SHELL and SPACE IDS in place:

Shell IDS will include door and window contacts and switches, as well as break glass and vibration sensors.

• Space IDS includes PIR, microwave and dual technology sensors.

CCTV systems should be more extensively used outside working hours and such use will extend from covering those points and vulnerable areas closer to the building to the perimeter and approaches to the premises. Of course, CCTV will need to be supported by appropriate security lighting systems and closely and continuously monitored. CCTV system requirements are covered in detail in Unit 2.5.

Patrolling

The importance of patrolling increases substantially outside normal working hours. Patrols must be planned to follow different routes and take place at different times each time they are carried out. They should check vulnerable areas which are not sealed and protected by IDS and perimeters and access gates. Security Officers should be issued with appropriate communications, alarm and surveillance systems in line with the threat against the building and its vulnerabilities.

The provision of appropriate lighting systems is essential to the effective protection of a building during the hours of darkness. Lighting deters, assists in monitoring and detection, and can be covert or overt — it can cover large areas, particularly vulnerable points or prevent surveillance from the exterior of the facility. Illuminated areas should be patrolled and monitored. Lighting is covered in detail in Unit 2.3 Perimeter Protection.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) are specifically designed to detect and indicate that an adversary has entered the building or premises. It is most important to realise that IDS detect — they do not prevent access by an intruder.

The Intrusion Detection System will comprise various components and linkages:

The sensors.

- Keypads to arm/disarm the system.

User codes.

- Control panels.
- Local alarm indicators.
- Connection to a central station.

The connection to the Central Station, if it is used, can be by a direct telephone line, a party line, multiplexing, a voice line dialler, a digital dialler and receiver or over the cell phone network.

The range of sensors which may be applicable could be door or shutter contacts, PIR sensors, dual technology sensors which use a combination of PIR and microwave, internal and external beams and microwave sensors, vibration and break-glass sensors.

In certain situations, ancillary equipment may be specified such as smoke machines. These flood specific areas with dense smoke to make it difficult or impossible for intruders to operate. Intruder alarm systems often operate in conjunction with CCTV systems, access control systems, and even as part of a major integrated system.

Securing Doors

Doors, along with windows, are a fundamental point of weakness in any building. Regardless of the strength of construction of perimeters, walls and other barriers (not to mention the effectiveness of detection and alarm systems), weak doors and windows will make access simple. Often, the choice of door selected for any building will depend on security as only one of various considerations such as: legislation; required function, safety and appearance. Door materials can vary from glass to wood or synthetic materials and the associated locks, hinges and frames will also vary in strength, durability and resistance to attack. It is essential to remember that a door 'system' comprises these elements — the door will only be as secure as its weakest component.

There are many types of door available for use both internally and externally such as:

Final exit doors these doors should always open outwards and be of the strongest possible construction.

Routine entrance and exit doors for use during normal operating hours.

Emergency doors.

Vehicle access doors and entrances.

External Doors - All external doors must be of solid construction throughout. Doors with hollow cores, thin panels or glazing should not be used. They must be fitted with hinges which cannot be forced or lifted free of the door - this can be achieved by fitting recessed hinges with inaccessible screws and by welding or flanging the tops of hinges. The frame and door surrounds must be of the strongest possible construction.

Internal Doors - Internal doors should not be ignored as far as security is concerned. There will be in most businesses and organisations areas and rooms to which access needs to be restricted and thus doors must be able to withstand assessed threats of attack. Whilst such doors will tend to be weaker in construction they can be adequately secured using appropriate locking and self-closing systems.

Glazing - Glass should be avoided in doors wherever possible (and often it is not). If glass must be used it should be of the maximum

What are the advantages and disadvantages for each of these types of sensors?

PIR sensor

Microwave sensor

Dual technology sensor

possible strength and properly beaded and framed to avoid simple removal of panes. The strengths and types of various glazing materials will be covered in the 'Securing Windows' section of this unit.

Procedural Controls and Awareness - It does not matter how strong your doors are if employees are unaware of the need to secure them. Most buildings and rooms are entered illicitly through doors that have been left open or unchecked at the end of the working day. Therefore, it is essential that all employees are made aware of the need to secure doors properly and to report damaged or improperly functioning doors. Doors are often left unsecured by propping open with fire extinguishers or by habitual users such as smokers using a door regularly. It is essential that security patrols regularly and meticulously check doors and their locking devices.

Locks - No one lock is appropriate for every door. Low-security internal door locks can be relatively cheap to prevent casual access whereas the final exterior door to a building or a door to a restricted area will need to be to the highest possible specification. A lock will never guarantee total protection — it must be considered only as a delaying device and where appropriate must be layered with other protection and detection systems to allow response to a breach or attack.

Locking devices can be mounted on the outside of or within a door and can be operated by key (most commonly), electrically or by numeric keypad. The effectiveness of a lock depends upon the robustness of its construction, the security of its fixing to the door, the complexity and tamper proofing of the keying system and the 'strike' depth of the locking bolt into the recessed door frame.

Locks can be attacked using various methods — they can be drilled, unscrewed, ripped from the door frame, sawn out, the door frame can be spread apart using a vehicle jack or a crow strut. Concealed methods include lock-picking and the use of credit cards to bypass bolts. All

can be defended against by selecting an appropriately constructed lock and by secure fixing. It is worth noting that poor maintenance of locks contributes directly to their vulnerability and therefore doors Devise a policy to follow for should be checked routinely for operation and key security. security.

Key Security - Locks are useless as security devices if the keys to them are not properly secured and controlled. The following measures must be followed to ensure that locks and security are not compromised:

• Wherever possible the use of padlocks should be avoided. Padlocks are subject to substitution and replacement by employees with criminal intent, who will replace your key on the key ring with theirs, keeping a key for themselves to enter the location at will.

If using padlocks, ensure they are not purchased locally, but from a proper security lock supplier. Select close-shackle - as opposed to open-shackle - locks and do not use in conjunction with chains.

When a new lock is fitted a record should be made of the number of keys supplied. These should be engraved. Typically, there will be three keys, one of which should go into the safe/cabinet and the remaining two kept in a sealed envelope in a safe.

Keys should be kept in a locked container when not in use and not issued to personnel for longer than is necessary. Ideally keys should be returned immediately after they have been used to lock or unlock. Under such arrangements working hours security can be achieved by mechanical combination locks.

All key rings should be labelled with a number. The name of the location to which the key belongs should not be displayed on the label.

A key register should be established, and staff required to physically sign keys out.

Key registers and key holdings should be checked at security staff shift changeover times.

It is not good security practice to issue keys to cleaners, but where this is necessary the process must be closely monitored and regulated.

• Where, by necessity, keys to existing locks have been issued to construction contractors, locks should be changed upon completion of their project. In new constructions consider using professional locksmiths to install locks, rather than entrusting the task to unknown and unchecked building contract labour.

Regulations — Security can be compromised by fire or safety regulations; some doors need to be left open and unsecured during working hours and there are also construction standards and regulations to be followed. You must ensure that when surveying and specifying doors, locks and closing devices you consult the relevant standards and authorities to ensure compliance.

Securing Windows

Windows are the weakest part of any building because they are made of glass! However, there are measures and manufacturing processes which can be employed to ensure that windows are protected as much as possible and therefore provide an element of delay to the potential adversary.

The risk assessment that you carry out will influence the choice of window and its materials and its location. You will also need to determine whether the window provides adequate protection or whether it needs additional strengthening to reinforce it.

A well-protected window will fulfil some or all the following requirements:

Situated in an appropriate location. Constructed of appropriate glazing material.

Be fitted with adequate locks. Have an appropriate frame and mountings.

Have, where necessary, additional external or internal protection.

Be fitted with an alarm/detection system.

Building Intrusion Detection Systems

(BIDS)

Intrusion detection can be divided into two primary types: shell and space:

reed etc,

heat PIR

Protecting the building shell with switches, vibration detectors

Protecting the building space with volumetric sensors which respond to and/or movement. For example:

Movement detection senses movement (sometimes referred to as trap detection) and utilises:

- Passive infra-red (PIR) - The purpose of these devices is to detect the infrared heat emitted by an intruder. They provide a field of detection divided into elements that attempt to detect changes in temperature. The change in temperature is then focused through a lens onto the detection cell and any movement causes the system to initiate the alarm. They are most suited where a potential intruder is likely to walk across the path of detection and they should not be sited facing heat sources or looking out through windows.

Microwave detectors - These detectors use the Doppler effect to activate alarms on movement within the protected zone. A radio frequency signal is generated which is reflected from the walls, floor, ceiling and objects to form a protected zone. Movement - directly towards or away from the detector - will give the best chance of detection. Because radio waves can pass through low density building material such as glass, wood and plasterboard the range of detection can often extend beyond the perimeter of the protected area so care

What are the advantages of shell and space intrusion detection sensors?

must be taken in siting the detectors.

• Acoustic detectors - These systems react to the sounds caused by an intruder entering the area in question. They consist of a microphone system attached to an alarm which can be monitored over a loudspeaker by security staff if triggered. These systems need to be carefully sited and adjusted to avoid nuisance alarms and picking up low-level background noise in the area.

• Dual technology detectors These detectors are used to reduce or eliminate the possibil-



ity of false alarms which can occur when a single type of detector is used. They operate as 2 separate detectors, detecting both movement and infrared. With a dual PIR/microwave detector, if the microwave unit activates, the detector waits a few seconds to see the PIR unit detects infrared. If it does - the alarm will be activated; and if not, the system will reset.

• Active infra-red detectors These systems detect the presence of an intruder when an infrared beam is broken. The detector comes in 2 parts (transmitter and receiver). The receiver picks up the light signal sent by the transmitter and if reception is interrupted an alarm will be generated. The system differentiates between the beam and ambient light by modulating the beam which effectively produces a unique coded light pulse. For multi-beam systems a synchronisation signal ensures that each receiver picks up only the beam that is intended for it by the transmitter. The light beam can also be reflected around an area to produce complex patterns and provide better cover.

PHYSICAL SECURITY MANAGEMENT

Introduction

CCTV is an invaluable force multiplier in security, performing the functions of:

Deterrence.

Displacement.

Detection.

Alarm assessment. Monitoring.

Identification.

Evidence collections. An investigative tool.

However, the system must be chosen carefully. There are as many poor CCTV installations as there are good ones.

The Basic Components of a CCTV

System

Storage

Transmission

Camera

Monitoring

The following is a discussion of some of the basic components of a CCTV system.

Camera

In simple terms, we can group camera assemblies into fixed, pan/tilt/zoom, covert, overt, dome etc. But this is a very simplistic classification and makes no reference to the qualities of the camera contained in such assemblies.

To be able to select the correct camera, there needs to be a clear understanding of a range of selection and performance criteria which can combine, or conflict, when putting together an integrated CCTV system.

Can you think of any non-security applications for CCTV?

Introduction

CCTV is an invaluable force multiplier in security, performing the functions of:

Deterrence.

Displacement.

Detection.

Alarm assessment. Monitoring.

Identification.

Evidence collections. An investigative tool.

However, the system must be chosen carefully. There are as many poor CCTV installations as there are good ones.

The Basic Components of a CCTV System

The following is a discussion of some of the basic components of a CCTV system.

Camera

In simple terms, we can group camera assemblies into fixed, pan/tilt/zoom, covert, overt, dome etc. But this is a very simplistic classification and makes no reference to the qualities of the camera contained in such assemblies.

To be able to select the correct camera, there needs to be a clear understanding of a range of selection and performance criteria which can combine, or conflict, when putting together an integrated CCTV system.

Perhaps the most critical element of the camera is the lens. Here it is important to select not only high-quality optics but also the right lens for the job. Lenses come in various types, each one designed for a specific purpose. The main kinds of lenses and their specific purposes are as follows:

Standard Lens - Should be the lens of first consideration. In most circumstances this will be the best lens. However, to get the correct field of view, exact placing of the camera is essential.

Varifocal Lens - Like a standard lens but allows the installer to make minor field of view adjustments when installing. Therefore, exact camera siting becomes less critical. Sometimes, because cameras must be mounted on walls (which cannot be moved) varifocal lenses offer the best solution for normal fields of view.

Wide Angle Lens - Provides good depth of focus and extensive field of view. Suitable for interior office and reception areas.

Telephoto Lens - Allows distant objects to be magnified on the monitor and in the recording but restricts surveillance on either side of the object. Much of the area in front of the object and behind will be out of focus when this kind of lens is used. This focus condition gets worse as the light decreases.

Zoom Lens - A motorised lens that provides variable image magnification. It usually accompanies a pan/tilt head. Take care not to overuse.

When determining scene requirements and thus selecting lenses, it is useful to ask yourself what are you trying to achieve? Detection of the presence of an unknown person, recognition of a known person, identification of an unknown person. This is crucial to selecting the correct

Why do we use CCTV? What are the advantages and disadvantages of CCTV?

Most modern cameras have sophisticated circuitry that allows them to switch to monochrome when lighting levels drop. In low light conditions, using cameras in monochrome mode may provide up to ten times the clarity of colour, which becomes grainy when light levels decrease.

PTZ (Pan, Tilt, Zoom) cameras have some disadvantages. They are many times more expensive than regular fixed cameras, require a sturdier mounting (or mast) due to their increased weight, and, unlike fixed cameras do not provide 24/7 coverage of a given location since their direction of view is altered when operated manually. Thus, such systems (and the operators) can be deceived by a cunning intruder.

Dome cameras are often selected as an alternative to regular fixed or PTZ cameras. Not only are they discreet (and therefore more acceptable) but in alerting a would-be wrongdoer to the presence of surveillance, they create an impression of 360 surveillance.

Most modern cameras deliver colour images when lighting levels are good, and switch to monochrome when scene illumination falls below about 0.5 lux and the colour image becomes grainy. Three artificial illumination options are as follows:

For each of the bullet points below describe what you are trying to achieve through use of each CCTV system?

Detect

Observe

Recognise

Identify

Use of white light with good colour rendition. Depending on the illumination level, this will allow the camera to continue to be used in colour mode.

Use of standard sodium street lighting. Under these conditions, switching the camera to monochrome mode will probably produce the best results. Use of infrared projectors. Cameras in monochrome mode are inherently sensitive to infrared light. Image Transmission

The advent of digital technology has revolutionised the way in which CCTV images can be transmitted. Historically transmission was limited to coaxial cable (with a maximum transmission distance of 300 metres) or twisted pair cable. For long distance transmission it was necessary to use wireless means, which was often unstable. The first revolution came with the introduction of fibre optic cables, which allowed crystal clear images to be transmitted over very long distances. The second revolution occurred when digital imagery combined with computer technology, allowing CCTV imagery to be transmitted over a computer network using standard TCP/IP means.

Manufacturers and installers, however, sometimes inflate the capability of image transmission over computer networks. The first point to bear in mind is that Ethernet network cables (the standard cable for connecting computers on a network for transmitting data) are limited to 100 metres. Thus, the signal must be relayed for longer distances, which is not a problem with computer networks.

The second, and significant point is one of bandwidth. Ethernet cables have limited transmission bandwidth, so they may not be able to transmit CCTV imagery to the standard you may be anticipating, especially if they are

Notes

conveying images from more than one camera. Often, before transmission, the size of the imagery must be reduced through a combination of:

a. Reducing the frame rate. Cameras typically record at 25 frames per second (fps) but even at 16fps humans will perceive normal motion. Immediately, this provides a bandwidth saving of 36%. But significantly greater bandwidth savings can be achieved if a lower frame rate is used. For example, in many settings, just 10fps would suffice. But care should be taken not to

reduce the frame rate too low. Where acts of violence may be anticipated, for example, a punch can be thrown in less than one second and may not be recorded if the frame rate is too low.

b. Reducing the resolution. For many

cameras the standard quality recording rate is 4ClF. By reducing the resolution to CIF (1 CIF) only 25% of the original bandwidth will be required. Again, this functionality should be used with caution. A setting of CIF may not be sufficient to be able to read a vehicle number plate. Trial and error will determine.

Transmission means can be mixed in a single system. For example, images from perimeter cameras can be delivered via fibre optic cable, but internal transmission can be via TCP/IP across a computer network.

As technology and compression capabilities develop, there will continue to be significant developments in image transmission. One area of transmission means that is bound to see significant advances will be wireless. For example, Wi-Fi cameras exist already, but many systems don't deliver adequate results. This will change. Also, we will likely see CCTV technology seriously embrace 4G GSM.

Storing Images

VCRs have now given way to new, digital storage systems. Generally, these come in two forms:

a. Systems using proprietary encoding, hard drives and equipment. These are self-contained but usually expandable by the Notes installer as demand increases. These are commonly known as DVR-based systems.

b. Systems using TCP/IP means based around computer network architecture; in fact, often using the exact same workstations and cabling as the company network. These use standard computer hard drives, with built-in redundancy, in what is called a RAID arrangement. Such systems have great expandability, as demand increases. These are commonly known as NVR-based systems.

On the face of it, it may seem that option b. is the best, and maybe that is true. But option a. should also be considered, as these are self-contained, low maintenance units that may fully meet the needs of the organisation. They are also less susceptible to intrusion and malware, as they are independent of the IT network.

Option b. certainly provides the best and lowest cost option in terms of expandability and has the added convenience of being operable and accessible across the regular company network by anybody with the appropriate permissions. But IT networks are vulnerable; in the event of an emergency the IT network may go down. If this happens, there will be no live video to assist the management of the emergency. Also, the IT

network may be the target of a malicious attack or simply become infected. This could render any IT-embedded security systems inoperable for days, or even weeks.

A crucial consideration when using storage equipment is the storage capacity, and here you will encounter similar problems to bandwidth limitations. For example, a typical digital image data stream recorded at 4ClF resolution and 25fps could conceivably consume 20Gb of storage in 24 hours. With several cameras operating to the same parameters the storage capacity of most CCTV hard drives would soon become overwhelmed and would certainly not achieve the recommended minimum image storage time of 14 days, before being overwritten by new data. To this end, there are many options that should be considered to maximise storage space:

You may wish during quiet hours to restrict recording to event-only. The camera sensor will detect when movement or changes are present in the scene viewed and will record only under those conditions.

You may wish to reduce the frame rate to a low fps. You can configure most cameras to revert to real-time recording (16-25 fps) in the event of movement in the field of view.

You may wish to record at a lower resolution, for example CIF. But if you do this you should be aware that there will be no way to enhance the images back to how they may have originally been viewed live on the monitor.

While access to live imagery may be somewhat unrestricted across the organisation, access to recorded images must be strictly limited. And those who can alter data associated with recordings must be further restricted to just a select few supervisors, whose actions should be recorded by an audit trail. Preservation of CCTV images as evidence is dealt with in the Evidence module.

Monitoring Images

There are many display options for monitoring images, including TFT, Plasma, LCD, LED, OLED etc. Images can also be projected using an LCD projector. When selecting, you should investigate all options to see which best fits. In a control room it is normal to have one large monitor and several other monitors divided into camera scene grids. Care should be taken not to overload operators, however. While city centre CCTV operators may be able to operate dozens of monitors simultaneously, the same rule cannot be applied to company control room operators who

What are the advantages and disadvantages for the following lens options?

Standard

Wide angle

Varifocal

Telephoto

Zoom

may have other duties, or who may be required to monitor monotonous scenes with no change in activity.

TCP/IP CCTV surveillance allows for monitoring of CCTV images from many different locations, and with the advent of 4G technology, conceivably from anywhere with a smartphone and appropriate access credentials.

Some basic principles of monitoring are as follows:

Control room should be secure, with a designated person in charge. All visitors and contractors should sign in and out. Access to recorded images should be strictly restricted.

Images retained for between 5-30 days, depending on system capabilities and operational requirement. 14 days is often sufficient.

Operators constantly monitoring screens should take 10 minutes break in every hour. Images should be backed up and copies stored off site, if critical.

There should be a facility to extract specific scenes and save as individual files but editing functionality should be limited so that scenes cannot be spliced together to construct misleading images.

There should be clear operator instructions, including what to do in the event of an emergency.

Operators should be trained and made aware of data protection legislation. There should be a log of all incidents and actions taken.

Any access to recorded materials by other than control room staff should be authorised and logged, with purpose stated and signature.

There should be instructions on what to do when faults occur.

Operating instructions should detail how the monitoring is to be carried out (e.g. blank screen, full screen, split screen etc.).

For your own site, consider the specific CCTV considerations that you will need to consider considering the site layout, what the risks are, and the Home Office guidelines

Now assess and describe the elements of your current system that you would remove, retain, improve or upgrade to provide optimal coverage and protection,

Operating instructions should detail how the recording is to be carried out (e.g. frames per second for each camera, quality parameters etc.).

All monitoring and recording should comply with the Information Commissioner's CCTV Code of Practice. You can download your own copy from: http://www.ico.gov.uk

Dedicated CCTV control room operators should be trained in accordance with the SIA Specification for Learning and Qualifications for CCTV Control Room Operators.

Control Room Operations

Operating a control room efficiently requires effectively trained personnel who are self-disciplined enough to operate the system to required standards. Therefore, and most importantly, clear operational procedures must be provided to operatives. These instructions should include the following:

1. What is to be monitored? You should specify the locations and activities to be monitored and the frequency or duration of monitoring.

2. What is not to be monitored? State clearly and unequivocally what operatives must avoid monitoring, including private activities and neighbouring domestic sites. Training for operatives must include treatment of Data Protection and Human Rights legislation to ensure that they are fully aware of the implications and penalties associated with unlawful intrusion of privacy. If using PTZ, clear instructions on required fields of view should be provided.

3. Responsibilities. Operatives must be clear about their responsibilities.

4. Actions required. When an image or monitored area requires a response, what does the operative need to do to affect that

You should adhere to the BSI

Code of Practice 7958:2009

Closed Circuit Television (CCTV) Management and

Operation Code of Practice.

Additional information can be found in the Information

Commissioner's Employment

Practice Code on Monitoring at Work

Alarm and communication systems must be familiar to operatives and Notes any contact lists must be updated at least weekly, including up to date details for duty managers and technical staff should faults occur.

5. Image retention and storage procedures.

6. Shift plans and systems must be designed to allow operatives to monitor effectively. Constant monitoring of screens is demanding and physically tiring, and operatives should take 10 minutes break in every hour. Emphasis must be placed in both training and the development of procedures on the need to maintain continuity always and not to leave systems and control rooms unmanned and unattended.

7. A CCTV operations log should be provided for operatives to include details of any incidents and system faults.

8. Operating instructions should detail how the monitoring is to be carried out (e.g. blank screen, full screen, split screen, etc.)

9. Operating instructions should detail how the recording is to be carried out (e.g. frames per second for each camera, quality parameters, etc.)

HSE and Ergonomics

Even the best trained, most highly motivated operatives will not perform to the required standards if working conditions are not conducive to personal comfort, health and safety. The control room should be designed with good ergonomics in mind. You should plan the layout of the control room carefully to ensure that the following areas are adequately addressed:

Individuals are not over-tasked. There is a limit to one person's ability to monitor screens and systems. Although multiple screens and images may give the impression of a high-technology and detailed surveillance system, if they cannot be simultaneously monitored (and importantly, events acted upon) then they will be of little value.

2. Seating, control desks, human/machine interfaces and communications must be set up to be compliant with health and safety requirements to avoid fatigue-related performance issues and to avoid injury to operatives.

3. Screen distances must be carefully set up to ensure compliance with regulation. As a guide, the following maximum viewing distances from operator to screen are recommended:

Screen Size	Viewing Distance
9" 23cm	1 .5m
12" 30cm	2m
17" 35cm	2.5m

4. Ventilation, heating and air conditioning systems must be adequate to provide breathable air and to maintain temperatures adequate for comfort and system operation.

5. Room and individual workstation lighting must be adequate to allow correct monitoring and to avoid stress-related fatigue for operatives.

6. Adequate provision must be made for meal breaks and for beverages within the control room. Instructions should underline the importance of keeping food and drinks clear of control room desks and operating systems.

CCTV System Planning and Management

BS 7958:2005 sets out a code of practice for the management and operation of CCTV. This can be purchased from BSI and is a "must-have" document if you oversee operating a CCTV system.

Best practice on how to specify a CCTV system is provided in the form of a CCTV Operational Requirement Guide, issued by the Home Office Scientific Development Branch. This can be downloaded from http://www.designforsecurity.org/downloads/

How can you ensure your staff and organisation follow the points made on the left to ensure you get the best performance from the Security Team?

If you need to plan and specify a CCTV system, there are many considerations. It is not simply a case of asking a sales person to provide a complete system as they will invariably try to sell you the most expensive (and not necessarily the best) system. So, in addition to the normal risk assessment, the following are some of the factors that should be taken into consideration and that you should ask yourself before you start:

What are the purposes for which the system is being deployed?

What is the area to be covered and how much detail is required?

Will the system be required to detect and provide positive identification of intruders? What are the various technologies available and do I need to ensure future expansion/upgradeability?

Are the day/night lighting levels adequate for the type of system I am considering, or do I need to think about alternative sources of illumination?

Can I accept monochrome images during hours of darkness?

What are the scene variables? Will I be recording fast movement? If so this will affect the frames per second recording rate and influence significantly my storage requirements.

Will I be required to produce recordings for submission to courts of law? Should the system be linked into other security systems, such as intrusion detection and access control? Does the system require an anti-tamper circuit or other protection for the cameras? If a retail location, is it wise to record on-site or should the images be transmitted for remote site recording?

How will the system be monitored and by whom?

What type of maintenance contract is required?

Will I take a chance and liaise directly with a supplier or will I bring in an expert consultant to find me the most appropriate systems at the best price?

What are the main legal, regulatory and security implications of running a CCTV control room effectively and safely whilst maintaining the rights, freedoms and safety of your security operatives?

• Will I issue a performance or technical specification?

These questions will help you to make a start on deciding what you need to implement a CCTV installation project. You may even decide that you do not need a CCTV system at all!

If, having considered the questions above you decide that you are going ahead then you need to think about the type of specification you are going to use.

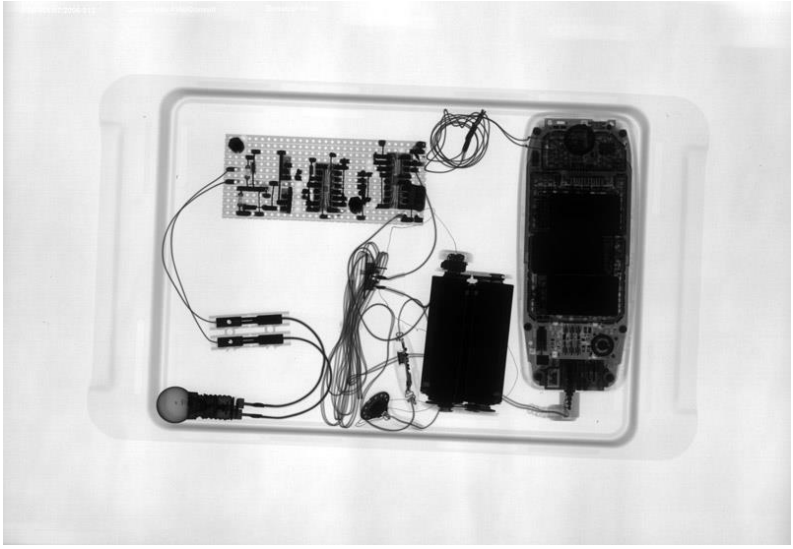
The CCTV Operational Requirement Guide provides all the information that the security manager requires to begin the operational requirement process including examples and checklists for CCTV planning and implementation. The manual states that you should consider the following factors when planning and implementing the OR and expands upon the specific areas in detail.

1. Location — where on your premises do you need to monitor?
2. What potential threat or activity do you wish to monitor?

(drugs, fighting, intrusion, internal theft etc.)

3. What is the purpose of the observation? (monitor, detect, recognise, identify)
4. What will be the target speed?
5. Who monitors?
6. When is monitoring to take place?
7. Where monitored (where is the CCTV control room)?
8. What happens when an event occurs?
9. Alert function — what action should the system take when an event is detected?
10. Display — how will the images be viewed?
11. Recording — how long should video be retained, image quality, frame rate, any additional data to be recorded with video?
12. Export and archive of data.
13. Constraints — licensing regulations.
14. Legal issues.
15. Maintenance.
16. Resources required operating the system.

The Improvised Explosive Device (IED)



The IED is the favourite weapon of the terrorist, accounting for 90% of all attacks. An IED is relatively easy to manufacture and has a huge

psychological impact not just on the victims, but also on the intended audience. A typical IED comprises six to eight components, as follows:

The timer.

The power sources.

The initiator.

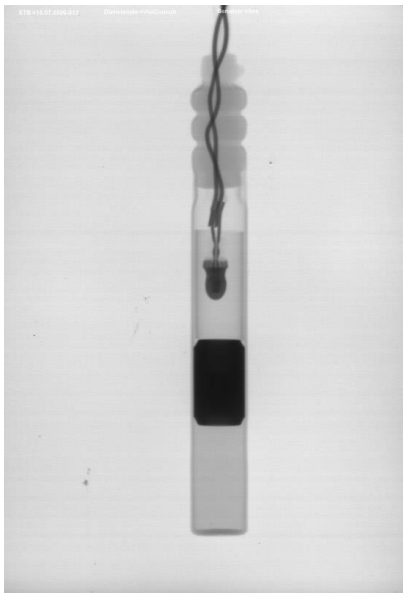
The explosive.

Container or disguise.

Arming device.

Wiring.

Shrapnel.



The Hand-Delivered IED This is a device which is left by a bomber and is intended to detonate at a certain time, when touched or upon a specific remote command. It is often disguised as an ordinary object and in addition to the main triggering device, booby trapped.

The effects and lethality of a hand-delivered IED can be enhanced in many ways:

By adding shrapnel (nuts, bolts, nails etc.).

By adding radioactive materials (dirty bomb). By use in an enclosed space (i.e. inside a building, bus, train etc.).

By use against a vulnerable moving target such as an aircraft.

By the addition of a flammable liquid.

The most likely location for a hand-delivered IED is usually one which allows ease of access, undetectability and maximum damage (people or critical systems). Many bombers only get one chance to attack their target, so they will wish to maximise the potential for damage/casualties. Internal blasts satisfy this desire as reflections and re-reflections of the blast wave can theoretically increase the destructive power of a bomb up to ten times and cause considerable fragmentation hazards. Areas to which public have access, such as busy reception areas, make good targets for the bomber. Devices may be planted at night, in which case it is more likely that the bomber will choose a vulnerable target close to the perimeter rather than risk deep site penetration. As such, any potential targets should be identified and protected accordingly. For example, skips and bins should be relocated to 10m from any vulnerable parts of buildings, and any outside walls of fileserver room locations should be strengthened.

Standard protection measures against a hand delivered IED may include the following:

Staff Awareness - To ensure that they are aware of the appearance of an IED and are alert to anything out of place or any person acting suspiciously.

Good Housekeeping - To ensure that locations for the concealment of an IED are reduced and anything out of place is noticed.

Regular Patrolling by Guards - Checking all vulnerable areas, especially those which are close to the perimeter and where there are concentrations of people or other mission critical areas,

gaseous, explosive or flammable substances. All recessed entrances, building features and shrubbery adjacent to exposed windows prior to the commencement of the working day.

Access Control

Metal Detectors and X-Ray - To detect an attempt to introduce an IED, either assembled or in component parts.

Off-Site Parking - To make it more difficult to introduce an IED onto site.

Personal and Visitor Bag Labelling - Used in times of heightened alert to identify unattended bags.

Response Capability - A plan for a coordinated search operation in response to a bomb threat.

Describe what you consider to be your organisation's responsibilities to its employees concerning the measures which need to be in place to protect against explosive devices

Basic search equipment and the means to cordon off an area in the event of a suspect discovery.

Evacuation and Assembly Plan - To ensure all staff have a safe route to a safe place of refuge.

The Vehicle-Borne IED

Vehicle-Borne IEDs (VBIEDs) can be broken down into four essential types:

Remote Control Improvised Explosive Device (RCIED).

Suicide VBIED (S/VBIED) - A vehicle bomb which is driven to its intended target and detonated on arrival by a suicide bomber. From a commercial perspective the concern is that an attempt will be made to drive a S/VBIED into a building momentarily before detonation to achieve blast enhancement and building collapse.

Under Vehicle Improvised Explosive Device (UVIED) - A device placed under or attached to the underside of a vehicle.

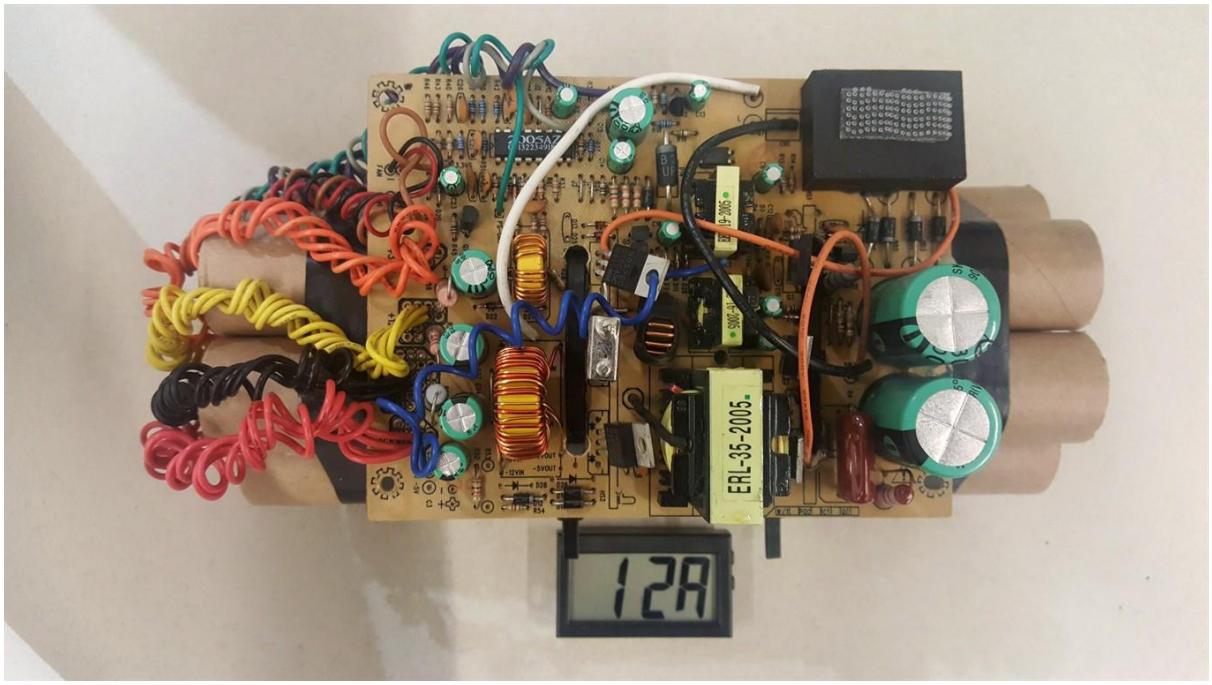
UVIEDs are designed to kill the driver and are usually activated by movement, typically using a mercury tilt switch. In addition, a UVIED activated by timing device may be attached to the underside of a vehicle before entering a facility. Vehicles which can park close to buildings (especially building entrances) or, even better from the bomber's perspective, vehicles which are destined for an internal loading bay area (blast enhancement) make attractive targets.

VBIED - A vehicle bomb which contains a large amount of explosive and which detonates in a crowded or built-up area, or outside a specific building, and which is designed to create widespread casualties and wide-scale destruction. Usually activated by a timing device.

A VBIED can be effectively deployed against congregations of people, in a built-up commercial district where high-rise buildings produce reflections and re-reflections of the blast wave, and against specific targets, such as a corporate HQ. In the context of the latter, it is glazing and other aspects of secondary fragmentation, such as suspended conduits, air conditioning equipment, internal glazed partitions etc., which will usually cause the greatest number of casualties.

A bomber will try to get the vehicle as close to the target as possible. They know that each halving of the distance between the bomb and the target increases the blast effect by a factor of eight, thus increasing the likelihood of structural collapse and building fragmentation. When attacking a building a bomber will seek to cause structural failure in the building, thus many times multiplying the casualty causing effect of the bomb.

It is difficult to generalise about the appearance of a VBIED. One feature is that it would likely



appear heavy on its axles with no visible internal load. According to US Government-sponsored analysis, approximately 80% of VBIED incidents involved explosive loads hidden in the boot, and the majority of VBIEDs are either timer or suicide (see next section) activated. Other possible identifying features of vehicles might include:

Abandoned or in the wrong place.

Parked in a hurry, badly or illegally. Number plates which look too new.

Heavily weighed down at rear.

Identified as being stolen or hired.

Incorrect licence discs.

Sterile, immaculately tidy inside.

Usually nothing suspicious visible underneath.

Controlling Parking - A key basic requirement is for all vehicles which are parked adjacent to buildings to be identified. Indeed, requiring vehicles to display passes while located anywhere on site is good practice, especially when the threat alert level is raised. In some cases, controls may require the vehicles to be searched prior to being allowed to park. As an added measure, and to increase staff reporting of suspicious vehicles, it is recommended that any vehicle that can park adjacent to a populated or critical function

Think about your own organisation, which areas of the facility are particularly vulnerable to suicide VBIEDs and what measures would you put in place to mitigate the

building during a raised alert state should display an A4 sized company-issued notice declaring that it is "security checked".

Designing out Terrorism Opportunities and Target Hardening There are many modifications that can be made to target design and behaviour to reduce the chances of a successful attack.

The most obvious is improvements to glazing. In a VBIED explosion in a heavily-populated commercial district, glazing failure can account for up to 80% of all injuries. Therefore, in VBIEDs-risk prone areas glazing should be strengthened by either the application of special window film to the inside of the window or, better still, the use of laminated double glazing in silicone rebates.

Many buildings use a great deal of glazing internally, for decorative purposes or as internal partitions. This, too, is a hazard. In the attacks in Istanbul in 2003 many people were injured by the failure and fragmentation of internal partitions.

Terrorists almost always reconnoitre a target prior to attack, and this process may begin weeks or months before. Sometimes, such as was the case with the bomber Timothy McVeigh prior to the Oklahoma attack, they may even conduct internal target reconnaissance to determine the most vulnerable areas. Thus, presentation of a potential target as "hard" may deflect the bomber to attack elsewhere.

Creating Awareness - When terrorists set out to bomb a facility, a great deal of effort goes into reconnaissance and planning. The bombers will want to ensure four things:

- That their attack will be successful in bypassing any countermeasures to achieve the desired objective.
- That their attack will be big enough to generate the desired message.
- That they themselves will not be killed in the attack (unless martyrdom is a deliberate motive).
- That they will not be caught and imprisoned.

Awareness begins with training security staff to look for, and encouraging staff to report, suspicious activity, be that out-of-the-ordinary 1 activity at vantage points overlooking the facility, out-of-the ordinary photography and videoing of the facility, cars parked outside containing individuals engaged in surveillance, approaches to staff and unusual requests etc.

The Suicide VBIED

A S/VBIED requires a different set of responses to that of a stationary VBIED. While there is much defence in common in terms of building engineering, site layout and security systems, etc., countermeasures to defend against a moving attack rely on specific measures to interdict the vehicle, and to reduce the momentum of the attack to prevent penetration of building walls or entrances.

Depending on the assessment of the threat to a facility, there are many defensive options that can be employed. Some of these can be enacted quickly, while others require careful planning and engineering. In no order, they are listed as follows:

Raised Blockers at Main Entrances - For a high-risk facility the default position of the blockers should be raised. Procedural measures and engineering should ensure the exit lane doesn't offer an opportunity for an attacking vehicle to enter as the blockers are lowered to allow exit. One recommended engineering solution is to create an airlock arrangement, with a forward boom barrier, whereby the boom will not rise until the blockers have redeployed.

Alternative Entrance in Case the Guard Post is Attacked - An interdiction of a moving VBIED at the gatehouse may result in detonation or, at very least, a crime scene. Thus, there should be an alternative entrance/exit with a temporary shelter for a guard and space to deploy a makeshift vehicle search area. When not in use, the gate should be protected by bollards or blockers to prevent breakthrough.

What are the specific differences between vehicle borne (conventional) and vehicle borne suicide IED and its targeting?

Perimeter Barriers - The site perimeter should be constructed so as not to allow breakthrough. This may be by means of strong fence construction or, in the event of a relatively weak fence such as chain link, by means of raised blockers, water obstacles, ditches, storm drains etc. Ideally any barrier should be outside the perimeter fence if space and land ownership allow.

Road Blockers En route Gatehouse to Site Interior - It is unlikely that a guard will be able to react in sufficient time to deploy a blocker sited at the main gate, so one option is to mount a further, rapidly deployable blocker a little way into the site, which can be immediately deployed by the guard in the event of a successful breakthrough. Such a configuration would have to ensure that roadside kerbs were such as not to allow a large vehicle to leave the designated road to bypass the barrier. Such a barrier may be designed to disrupt an attacking vehicle or to divert it to a safe place.

Traffic Circulation Systems - Traffic circulation systems allow for suspicious activity to be identified quickly and, if designed carefully, will ensure that there is no opportunity for a vehicle to gain sufficient momentum to penetrate a heavily

populated or mission critical building. Such systems should include roundabouts, high kerbs, chicanes and speed-retarding road humps. In the event of an increased alert level indicating an imminent threat, and in the absence of roadblocking hardware, stationary vehicles can be used as temporary blockers.

Direct Approach Roads and Roundabouts With regard to gatehouses, there are pros and cons to having a perpendicular approach road. The obvious con is that a long perpendicular approach road will allow an attack momentum to break through a barrier. The pro is that the approach may be seen, allowing guards to take defensive action. Countermeasures include chicanes, speed humps, but especially a roundabout immediately in front of the at-risk building. The roundabout must be of an impenetrable design to prevent crossing by vehicles.

Water Features and Ditches - Water features make it difficult for an attacking vehicle to find a fast route across land towards a target building and have the added advantage of allowing good lines of vision for guards. Furthermore, in the event of a detonation deep water features have been shown to be able to absorb and deflate an element of shock wave, which might otherwise have reached vulnerable buildings.

Planters in Front of Buildings - Breakthrough can be made much more difficult by the mounting of decorative concrete planters and bollards at 3m intervals in front of building entrances and vulnerable walls. If implementing countermeasures in the design stage, however, a raised steps entrance of about 1m provides excellent resistance to vehicles trying to ram the entrance.

Communication - In the event of a moving VBIED breakthrough at the main entrance, a warning signal must be communicated immediately to building occupants. A telephone is insufficient for this purpose. Two acceptable solutions are building PA systems, addressable from the gatehouse, or a specific siren, which employees will recognise as a warning to take cover.

Refuge Area at Back of Building away from Axis of Attack - Consideration should be given as to the likely approach of attack of any moving VBIED and internal safe havens on the side of the building considered safest should be identified and marked. In the event of a high threat level, deployment to such areas should be practised.

Monitoring - CCTV should monitor open space to provide guards with early warning of suspicious vehicle activity. Some advanced digital systems provide a range of criteria for out-of-the-ordinary activity to activate an alarm. Consideration should be given to establishing a central security control monitoring room above ground floor level to provide for good visibility and monitoring.

The Pedestrian Suicide Attack

Suicide attacks which are carried out on foot are particularly difficult to defeat since the target is usually congregations of people. Such congregations can occur inside a facility, within a controlled area, or outside the facility beyond the boundary of control. Examples of the latter might include staff who frequent in large numbers a bar or restaurant, staff queuing to enter a facility or being bussed to or from a facility, or staff who are congregated outside the facility as a group, perhaps in response to a telephone bomb threat intended deliberately to lead them to a point of exposure.

Statistically pedestrian suicide bombers are far more likely to attack public transport systems, bars and restaurants, sporting events and music events, crowded markets, shopping malls etc., than a secured commercial or industrial facility.

Entrance scrutiny and searching constitutes the main defence against such an attack, but this itself may create a target by causing people to congregate or queue while waiting to be processed. In addition, an armed police presence, if available and applicable, constitutes a significant deterrence.

Recognising an imminent suicide attack is difficult, but there may be some indicators, as follows:

Someone nearby videoing the facility. An out-of-place individual approaching the facility in an abnormal way.

An approaching individual muttering and glancing upwards to the sky.

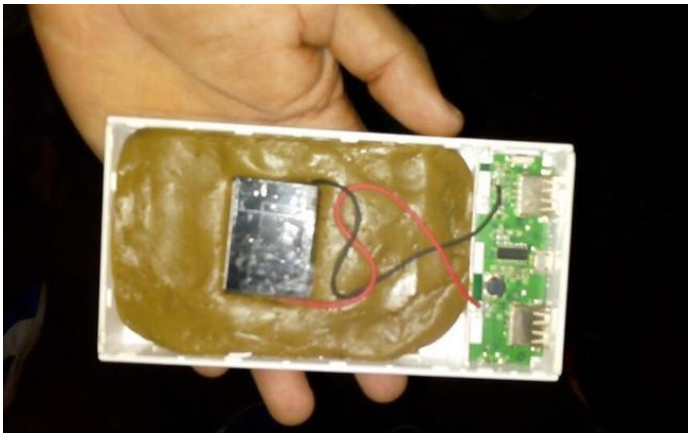
An individual who is trembling, sweating and red-faced.

Bulky clothing unusual for the time of year or climate (but note that very thin bombs have been built into corsets, vests and thigh-high socks, rendering the device "invisible").

Postal IED

Postal IEDs are relatively simple to construct (following instructions on the internet) and can comprise components and ingredients found in any DIY and electronics store. The charge can be either high or low explosives. The most usual types of high explosive used in postal devices are sheet explosives or plastic explosive rolled into thin sheets. Plastic explosives are stable enough to be suitable for using in a device which must withstand the rough treatment to which most items of mail are subjected.

Postal bombs work on the theory that the closer a bomber can get their device to the target, the less explosive that will be required. Since postal devices are designed to explode immediately in front of the target's body, a charge of just 50g is usually sufficient to kill.



Most postal devices are victim operated and are fired by the action of opening the envelope. Triggers vary but include: An insulating strip attached to the bottom inside of the envelope and a book containing explosives. When the book is removed, the insulating strip remains inside the envelope and the device fires.

A microswitch at either, or both, ends of a piece of card. When the envelope is opened, or the card removed the device fires.

A magnetic reed switches. When the two parts of the switch are near the device is "safe". As soon as the object to which one part of the switch is connected is withdrawn from the envelope, the device fires.

A light-sensitive diode. Exposing the diode to light induces an electric current, which fires the device.

A device built around the circuitry of a musical greeting card. Devices modified in such a way are difficult to identify, even by x-ray.

More sophisticated devices may contain a delay (timer), which is designed to arm the device once it has passed through the postal system. Thus, if the device has been subjected to rough handling, the arming of the device at a pre-determined time may, occasionally, fire the device prematurely.

Some 'postal bombs' contain no explosive at all, but may, for example, contain blood-filled syringes with the warning 'aids-infected blood', or razor blades which, it is threatened, have been contaminated with the deadly Hepatitis C virus.

Postal IEDs are less common than in the past but have been used against some businesses by individuals in recent years. Considering your own organisation, identify the potential risks from postal devices and the possible mitigation processes that you could implement to better protect assets,

The main defence against postal devices is awareness. This means knowing that a threat exists and knowing how to recognise a suspect device. Whilst equipment exists to help in identification, visual identification must always be at the forefront of any protective system.

It has been stated that awareness is the best form of defence against a postal device. This implies recognition by visual characteristics and touch. Some of the most obvious characteristics have traditionally been:

Grease stains on envelope.

Excessive weight at one end.

Address details suspicious.

Privacy markings.

Excessive markings.

Urgency markings.

Protruding wires or tin foil.

At least 3mm thick and 40 grams in weight.

Inflexible package.

Unusual smell.

Arrival from unusual or unknown source.

The modern use of plastic packaging and bubble wrap, as well as the simple ability to produce printed computer labels and forge bar codes etc. allows the potential postal bomber to

produce a far more convincing device than in the past and can be sealed to avoid grease marks and the escape of unusual smells. It is important therefore that any measures in place to protect against postal bombs allow for this.

Upon discovery of a suspect postal device in the mail room, the following steps should be followed:

1. Place the device on the nearest surface and summon a colleague or supervisor for a second opinion. Do not, however, handle the device again.

Notes:

a) Postal devices are usually activated by the action of opening the package. Some devices have, however, detonated prematurely without any intervention.

b) Some organisations have specially designated isolation areas for suspect postal bombs. However, it is against UK and European legislation to compel an employee to deliver a suspect device to such a location. Likewise, no employee may be compelled to relocate a suspect device to a 'bomb bin'.

2. Following a second opinion, if the device is still considered to be suspect, place an obvious marker next to the device to make it easier for the emergency services to identify the suspect device without delay. In the meantime, instruct a colleague to summon the emergency services and evacuate the rooms above, below and adjacent to the mail room. At the same time ensure that a site-wide and company-wide alert is issued to warn staff to look for other suspicious mail items.

Notes:

a) Attention should also be paid to the area adjacent to any windows in the mail room, which will act as blast vents in the event of an explosion.

b) The company-wide alert should contain a description of the suspect item. The most accurate way of doing this, if the facilities exist, is to follow up any verbal alert with an e-mail with an attached jpeg digital photograph of the suspect item.

3. Lock the mail room door and place a notice on the door to the effect that there is a suspect device inside. Remain on hand with the key until the arrival of the emergency services.

Notes:

a) A pre-prepared warning notice should be available in every mail room. This can be simply 'home made' and attached with blue tack.

b) Do not allow anybody else access to the room once the emergency services have

What are the three-main means of activating an IED?

been summoned. Typical of those who will try to seek access are security staff and managers.

The following actions should never be carried out:

Shake or try to bend any suspect device.

Put any suspect device in a bucket of water.

Take the device to a police station.

Drop the device out of a window.

Attempt to open any suspect device.

General Protective Measures

There is a tendency, particularly amongst less experienced or less aware security managers, to assume that to be able to protect effectively against terrorist IED attack it is necessary to invest in expensive and specialist equipment.

Whilst specialist equipment is certainly an advantage in the defence against certain types of devices, for example postal IEDs, most of the measures necessary to harden a potential target against terrorist bomb attack probably exist on site already.

In most of cases involving terrorism, staff, and security officers, are the most important line of defence. One reason for this is that terrorist planning for attacks, including those against targets of opportunity, usually entail an element of prior reconnaissance. Another factor is that the nature of terrorism means that terrorists enjoy a target rich environment, which allows the attacker to select the least well-protected of a range of potential targets.

Protection, however, means much more than numerical superiority of security staff to terrorists. In many cases the predictable way security staff carry out their duties enables the terrorist to identify gaps in protection and to exploit these.

Other elements of security which provide effective protection against terrorist attack include CCTV, access control systems, intrusion alarms and fences. Look at Annex A for a summary of how general protective measures can be "fine-tuned" to Notes increase protection against terrorist attack. The list is not exhaustive by any means.

IED Detection Technology

Without doubt, the best means of identifying a terrorist IED is an alert member of staff, security officer or member of the public. However, the fact that many devices are disguised as other objects, or are concealed inside bags, pockets, equipment etc. - and are often protected by an anti-handling mechanism - makes it necessary to use special types of detection equipment.

Despite the best efforts, and sometimes premature and exaggerated claims, by manufacturers and suppliers of IED detection equipment, there is no one single device that can detect most devices in most circumstances. Indeed, success depends more often on the skills of the operator in using the equipment, rather than the equipment itself. A detailed description of detection technologies is provided in Unit 2.7.

Telephone Bomb Threats

All bomb threat calls should be taken seriously and reported to the police immediately as they might have additional intelligence which puts the call into context. In some environments the police may order an evacuation and conduct a search. Conversely, as is the case in the UK and USA, the police may leave the decision to evacuate and/or search to the recipient of the threat call.

Essentially, there are three options upon receipt of a bomb threat call:

I. Assume the call is a hoax.

2. Order a partial evacuation.

3. Order a full evacuation.

Parcel bomb Entire building to a radius of 50m

Small hand delivered bomb 100m

Large hand delivered bomb

Sports holdall 200m

Under-car booby trap bomb 200m

Car bomb 400m

Lorry bomb 1000m

Bomb threat calls cannot be totally ignored. At the very least the target should order an immediate superficial search of the site to confirm the nonexistence of any unusual objects. Those best placed to carry out this quick check are the employees themselves, with security staff in support to check common areas, corridors and building exteriors. At this point also, security staff should inspect the designated evacuation routes and assembly areas and confirm that they are clear of any suspicious objects.

Evacuation and Assembly

The Evacuation

When an evacuation is ordered, it must be carried out quickly and with 100% compliance. The evacuation should be under the overall control of the incident controller, who will usually be a senior member of staff with an intimate knowledge of business operations and criticalities. The authority of this person will be absolute. Evacuation marshals may be appointed to supervise all the practical steps necessary.

Specific minimum evacuation distances exist for different types of bombs. These are based on past incidents and predicted explosive charge sizes, and are as follows:

Bomb threat evacuations differ to fire emergency evacuations and should not be initiated by the fire bell unless necessary. A PA system is the recommended means of initiating and controlling an evacuation, but, in the absence of such a system, quick and efficient evacuation can usually be achieved by precise verbal instructions by marshals and telephone cascades. One of the main dangers in initiating a bomb threat evacuation by the fire alarm is that it may lead evacuees past or to a point of danger.

Upon receipt of instructions to evacuate, all staff should pick up portable belongings, if nearby, and proceed to the assembly area in accordance with the precise instructions given at the time. Unlike fire, there is no need to close windows or doors; open doors and windows help vent any blast.

The reason for taking bags and coats is twofold:

Firstly, staff will have to remain outside for a long period of time before the area can be made safe.

Secondly, and more importantly, the removal of personal items will greatly assist in the search for, and identification of, suspect devices.

Under no circumstances should lifts be used as these may fail in the event of an explosion. As a precaution, security staff should ensure lifts are grounded and secured.

The evacuation process itself can be dangerous and must be closely controlled and coordinated. People, especially members of the public, are inclined to panic in such circumstances and there have been many instances where an uncontrolled evacuation has led to people falling and being trampled to death.

The evacuation must take place quickly and efficiently, using all possible exits. Alternative routes should be made available so that people can leave the premises without being placed in danger by passing close to a suspect device.

Lights should be left on to facilitate the search, but plant and machinery shut down.

If the area being evacuated is a public facility, such as a shop or cinema, it is advisable to instruct customers to go home, rather than to assemble behind a cordon where they may be in danger.

When there is a bomb threat, what are the 6 steps that need to be achieved for effective incident management?

In the event of an evacuation following a bomb threat warning, no member of staff should be allowed to re-enter the premises until a thorough search of all areas has been carried out. In the event of a bomb threat telephone call, nobody should re-occupy the premises until at least one hour after the threatened time of explosion.

Assembly Areas

The Bomb Threat Response Plan should designate at least two assembly areas on opposite sides of the premises. These should be chosen with the following points in mind:

They are large enough to accommodate the entire workforce for up to three hours in local weather conditions.

They are away from any form of glazing.

They are not likely to be used by other organisations in the event of a wide-scale evacuation

Access routes do not pass likely places for the planting of a bomb.

They can be searched and deemed safe in a matter of seconds, prior to the arrival of the first evacuees.

In addition, evacuees should be out of line of site of the device and, if possible, behind cover which has no glazing.

Where there is an ever-present threat of car bombs, a less than rigid approach to the choice of an assembly area may be needed.

For example, at locations in which a suspect car could be left at many different points, perhaps inside or outside the premises, it may be prudent to take a map of the area and draw 400m radius circles around all the main parking places. Thus, in the event of a suspect car being discovered, people can be evacuated to a safe location beyond the appropriate circle. Such a method is used at airports and other similar multi parking location facilities.

In built-up areas where no suitable assembly areas exist some organisations have selected specially designated bomb shelter areas, usually

underground, deep inside their own or a neighbour's premises.

Notes

Whilst this is an option, the selection of such an area should only be made by a suitably qualified structural engineer, who will need to be able to confirm that the shelter is not only safe from a VBIED explosion directly outside the building but also that the building will not collapse on top of the shelter in the event of a nearby VBIED explosion.

Conclusion

Explosive devices can come in many forms from many threat sources your organisation is responsible for protecting its personnel against them. Also, although your organisation may not be a target, the impact upon it from targeting your neighbours could be devastating. Security managers and their operatives must ensure that they understand the risks and potential impacts and what they will need to do in the event of an incident.

Risk analysis, protective measures and contingency planning are essential to protecting your assets and you should concentrate on ensuring that your readiness is at the correct level to meet the range of threats.

General Protective Measures

Patrolling

Patrol on foot by night and day.

Create an image of vigilance to anybody who might be watching.

Vigilance should extend to beyond the perimeter.

Patrol times and route must vary.

Patrolling officers should retrace their steps and, especially at night, stop in the shadows, listen and observe.

Access Control

The identities (and legitimacy) of all persons entering the premises should be confirmed. The identities of visitors should be thoroughly checked by security staff before notifying visit host.

Access control should be based on 2-factor authentication.

The wearing of ID cards by staff should be strictly enforced.

There should be some system for searching and labelling incoming bags.

Access control should operate on a need-to-go basis.

Staff must be encouraged to challenge strangers.

Reception areas should be designed not to allow free access to toilets. Visitors should be asked to register their cars if parked on site.

Staff Awareness and Trainin

Security staff should be trained in IED recognition, search and immediate response.

- Area searchers should be nominated and trained.
- A bomb threat co-ordinator should be appointed and trained.

Intrusion Detection

Intrusion detection should not be used as a substitute for strong physical barriers.

Intrusion detection should be configured to give the earliest possible warning of intrusion.

There must be a credible, rapid and efficient on-site response to any alarm.

Dummy systems should not be used — the clever terrorist will test them.

The most effective systems are those which use an overt and covert means. Consider using CCTV with Video Motion Detection.

CCTV

Keep all recordings securely for at least 14 days, preferably 1 month.

Don't upgrade to digital storage systems at the expense of image storage capability.

An installation comprising several fixed cameras is better than an installation comprising few PTZ cameras.

Use dome cameras internally.

Ensure good lighting at night.

Reliance on operators to identify on-screen activity is generally ineffective, except in special circumstances such as shopping centres.

Site Perimeters

Ensure gates, when closed, are to same physical standard as fence.

To be effective a perimeter fence should be at least 2.4m high, on top of which should be mounted some form of hostile topping.

Chain-link fences are not an effective barrier unless heavily reinforced or protected by patrolling officers.

Concrete walls should be steel-reinforced, not blocks.

Ensure no objects close to fence are an aid to climbing.

- Consider concrete blocks or ditches to block suicide vehicle attack.

Site Entrances

Provide parking for visitors before checkpoint and require them to dismount and walk to reception for ID.

Strong identification of any delivery driver — try to get suppliers to use regular driver.

Ensure vehicles are searched before entry — vehicle selection and search routine should not be predictable, i.e. a 100% search of car boots only is ineffective against a terrorist threat.

Limit the number and types of vehicles allowed on site.

Ensure 100% CCTV coverage of entire area.

At night strong floodlighting directed from high point towards fronts of an approaching cars.

Lighting

Ensure 100% coverage by use of fill-in lighting — avoid shadows.

Use PIR-activated lamps where necessary.

If permitted, project glare lighting beyond perimeter. Protect lighting circuits against deliberate sabotage.

Higher levels of illumination at building entrances, car parks and vulnerable or critical areas.

Environmental Design

Bushes to be no higher than 1m.

Tree canopies to be no lower than 2m.

Remove recessed doorways.

Straight perimeter fences.

Security lodge to overlook car park.

Smoking and rest areas to overlook perimeter.

Vulnerable or critical areas to be relocated to areas of good natural surveillance.

PHYSICAL SECURITY OPERATIONS AND MANAGEMENT

Introduction

This unit will examine the searching process with a specific focus on the management requirements and the planning and conduct of operations. Often, searches are carried out for the following reasons:

To deter.

To detect and to discover.

To prevent the unauthorised introduction of items. To prevent the unauthorised removal of items.

To support an investigation.

Search Objectives and Methods

There should be a security policy statement, agreed with HR, on search objectives, terms of reference and methods. Some typical search objectives and methods are as follows:

Person Searching

The scope of person searching will depend on the type of contraband likely to be concealed. Searches are common in industrial, retail and warehousing facilities. Searching for evidence of information theft is almost impossible, as the perpetrator has many places they can conceal a flash memory storage device which you cannot under any circumstances search. For example, under most circumstances, you may not touch any person in any area that would be reasonably considered to be private.

Searching can be an emotive issue and must be regulated carefully to ensure that the privacy and human rights of individuals are not compromised. There must be due respect for different religions. For example, it would be unreasonable to ask a Sikh male to remove his turban, or a Muslim woman to remove her headscarf.

Searching must be polite, non-invasive and fast. An employee rushing to get to work will become resentful if delayed by a long search process, and employees leaving work may have urgent commitments, such as collecting children from school.

The Right to Entry/Exit Search

It is important to note that you do not have an automatic right to search. No private person, which includes a private security officer, has the right to search any person, their property or vehicle without consent. Even if you believe a person to have committed a theft, if that person refuses to be searched the refusal can be overruled only by a police officer, who must carry out the search in accordance with PACE 1984. For powers of arrest under such circumstances refer to the Private Security and the Law module. Of course, you may insist on search as a condition of entry but insisting on search as a condition of exit is more problematic. Here, you will need to seek clarification from your legal department.

Of course, where an employee accepts an offer of employment under the condition that searches will be carried out, a "contract" has been made. If the employee fails to comply with the conditions the contract is broken, rendering the employee liable to disciplinary action.

There are gender issues associated with searching. Physical person searches must be same sex, although some organisations allow for searching of bags and, less often, hand-held metal detector searches by the opposite sex. Again, you do not have an automatic right to search by these methods. Consent is a prerequisite and your procedures should state clearly what action you should take on refusal of a search request.

Search Procedure - Entry

A notice should be clearly displayed at the entry point informing people what items are prohibited on site, requesting that they submit to an inspection, and advising them that non-cooperation will result in admission being denied.

Entry searching is usually rapid, often with the support of technology such as X-Ray. Of course, there should be a clear understanding of why the searching is being undertaken and what the searchers are looking for. In most cases entry searching is carried out in public view and is applicable to 100% of those entering.

Search Procedure Exit

Exit searching is more emotive, since there are usually insufficient resources or time to carry out 100% searching. Selective searching is the norm and should be carried out according to a schedule that appears to those exiting as if it is random. Many methods to achieve this exist or can be devised.

Exit searches may be in open view or in private. Open view and under CCTV recording is recommended. The basic procedure should be as follows:

Greet the person cordially, explain what you are doing and politely solicit cooperation.

Identify the person by means of the ID card.

Enter the name of the person in the search register.

Obtain that person's consent and ask if there is a physiological (health/injury) reason why a search should not be carried out.

Ask the person if there is any property in their possession that they shouldn't have. Search first anything that the person may be carrying.

Ask the person to empty the contents of their pockets.

Search the person, after first asking permission to touch.

Run hands along the obvious areas; don't pat.

Upon completion, ask the person to sign the register to confirm that they don't have any complaint

If you can achieve the above in less than 2 minutes, good. And in less than 60 seconds, excellent.

Upon discovery of any contraband your search procedures should advise you on what action to take. Every security operative should have a notebook to record any incidents or events.

Search Procedure on Specific Suspicion

Where a person refuses to be searched on exit, and only if you have reasonable grounds for believing, not just suspecting, that a criminal offence such as theft has been committed, the person may be lawfully arrested, and the police called. Arrest is always a last resort option, but a person cannot be detained against their will without lawful arrest.

After arrest, a person can still refuse to empty their pockets or baggage, but you are advised to at least request that they comply to:

' Remove any weapon or anything that could be used as a weapon.

Find and secure evidence.

If you are called to a work location where you have reasonable grounds for believing that a person is guilty of stealing or concealing stolen items, it is probably inadvisable to attempt to make an arrest at that location. Theft specifically requires proof of ulterior intent to permanently deprive without the owner's permission. Best evidence of intent occurs when the suspect tries to leave the facility, and this is the point at which interception should be made if the aim is to secure a prosecution.

Contractor Searching

Contracts with contractors carrying out work on site should stipulate that they be subject to the same search terms and conditions as regular employees, including vehicle searching. Any objections to complying with searches should be reported. With delivery contractors this may be more problematic, and you may have to decide to have deliveries dropped off at the entrance point if you are not prepared to allow delivery contractors on and off site without searching.

Manual Searching for Explosive Devices

Searching for explosive devices may be proactive (for reassurance) or reactive (in response to a specific threat).

Key considerations of proactive searches are:

Can be routine or when threat level increases.

To give confidence.

Part of 'search and seal' operation.

Can be superficial or extremely thorough.

Often prior to visit or event.

Sometimes at daybreak before work.

Sometimes as a 'wide awake' exercise. No evacuation necessary.

Reactive searches must be carried out very quickly and be well coordinated from a central point.

The efficiency and speed of reactive searches can be greatly improved by:

Regular practices.

The use of floor plans.

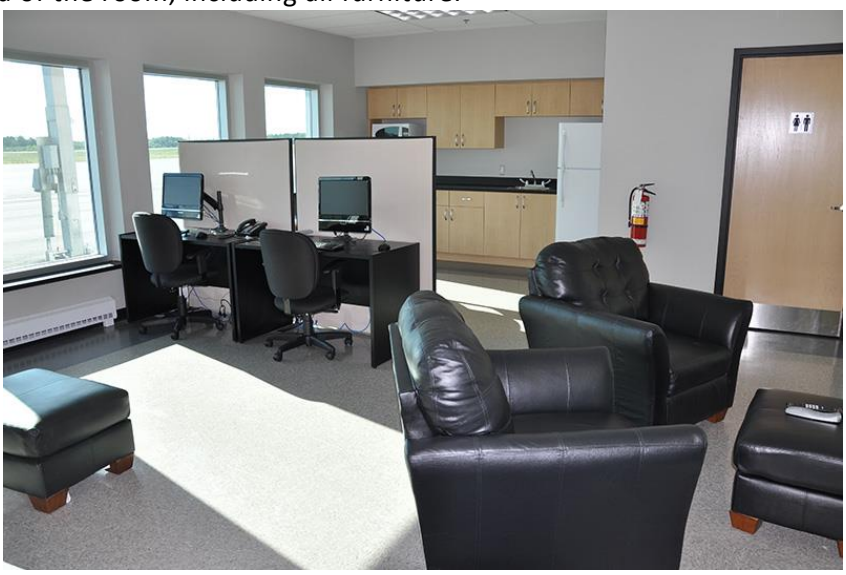
The use of room checklists.

A reactive search should always commence with a search of the assembly area and the routes

Keep mobile phones switched off.

Stage 1 - Work methodically around the room, checking the walls and the floor and fixtures immediately below.

Stage 2 - Check the main area of the room, including all furniture.



Stage 3 - Inspect the ceiling for any out-of-place objects.

Metal Detectors as an Aid to Searching

There are two kinds of metal detectors which are used as an aid to search:

Hand-held metal detectors (HHMD).

• Portal metal detectors.

Both use active radio wave technology and detect all metals, and are used primarily to detect guns, knives and IEDs. They do not specifically detect explosive substances.

Portals are very thorough but are expensive and time-consuming, frequently being activated by persons inadvertently, especially those persons who are not used to using them. Nevertheless, users can become quickly habituated, as in the United States.

Portals have the added advantage of not requiring same-sex operators.

There is no health risk associated with using portal metal detectors, but you should consult closely with the distributor about whether safe for persons with pacemakers.

HHMDs are much cheaper than portal metal detectors and can be deployed where the need arises. They can be used as a stand-alone device, and to locate precisely the source of any alarm generated in a portal metal detector. Often, they are used in situations where a physical search would be considered unacceptable or intrusive. They are also more generally acceptable when there is a need to search more intimate areas. Passed over the groin area, for example, from 15cm, they should be able to detect large metallic contraband.

Depending on your location, culture of the workers and policy, HHMDs may require same sex operation.

X-Rays

X-Rays are used for entrance screening (conveyor units) and mail screening (cabinet units). Depending on the unit selected, they have varying degrees of success in detecting organic substances associated with explosives.

Single energy units are good for detecting metallic objects and may possibly reveal to the operator the outline of an IED, but they are weak at detecting explosive substances. Multiple energy units have better explosives detection capabilities, but often confuse harmless organic substances (chocolate, cheese etc.) with explosives. Low explosives made from deflagrating materials (e.g. black powder) are very difficult to detect by X-Ray. X-Ray is also ineffective against detecting CBR powder threats, such as anthrax.

There is a need to constantly train operators and not to deploy an operator for long periods of looking at a screen. Tests have shown that an experienced operator can fail to discriminate between a disassembled pistol and a bag of tools, and attention drops significantly after 60 minutes, so breaks are essential.

When using conveyor X-Ray in conjunction with a portal metal detector, it is important that what does not go through the portal must go through the X-Ray. For example, if a small pedestal is placed next to the portal, passers-through will be tempted to place phones there to avoid the X-Ray.

Explosives Detectors

Explosives detectors come in three basic types:

- Desktop units for fixed positions. You will have encountered these at airports.
- Hand-held portable units.

What are the advantages and disadvantages for each of these aids for searching?

Metal detectors

X-Rays

Explosive detectors

Dogs

- Unfit for purpose detectors.

There are a lot of unfit for purpose explosives detectors on the market, so great care is required when selecting a unit; lives may depend on the success of your selection.

The fundamental requirement is that the system should can detect all common commercial/military explosives, plus:

- Nitrate/fuel compounds, e.g. ANFO (commonly used in VBIEDs).
- TATP Triacetone triperoxide (and its relatives), a home-made high explosive favoured by Al Qaeda.
- HMTD Hexamethylene triperoxide diamine, another Al Qaeda home-made high explosive less common than TAT P.

Desktop units are usually used for analysing swabs and are rare in commercial applications except in very specific circumstances.

Portable units are more common because most offer detection in two modes:

- Particulate. Vapour.

Most security officers operate portable units in vapour detection mode because this is quick. The theory being that they can draw in air and suspicious vapours from inside containers, pockets, bags, vehicles etc. The practice is somewhat less precise. In vapour mode such units can usually only detect high vapour explosives (such as TNT) and may be completely ineffective against the UK explosive threat, which is typically low vapour TAT P when protecting against Al Qaeda.

Much more effective screening can be achieved by operating the units in particulate mode. This requires a swab of the suspect area and analysis of that swab in the unit. This may take about a minute, so is impractical for a 100% search at a busy checkpoint. However, it can detect the smallest of traces of common explosives that make up the current UK explosives threat spectrum.

Canine Olfaction

Dogs are useful for the detection of drugs and explosives but can be expensive to 'run'. Apart from needing specialist handlers, the dogs themselves need regular updated training to ensure that they remain current in their detection skills and ability. As important as the dog's ability, is also the skill of the dog handler.

Vehicle Searching

You may be required to carry out vehicle searching. The aim of vehicle searching is to discover concealed items and it is important that the search is thorough. Your assignment instructions

should state the purpose of the search (contraband, explosives etc.). As with personnel searching, this process demands a high degree of diligence and training to be successful.

The key issues with vehicle searching are:

When stopping a vehicle for search, stand to one side with your hand out. Never stand in front of the vehicle.

Begin the interaction by explaining to the driver your intention, asking the driver to step out and checking ID and, if relevant, legitimacy to enter.

Ensure the engine is switched off and the driver has removed the keys.

If searching for IEDs focus on boot and back seat area. The driver should move around the vehicle with you opening tailgate/doors on request.

If searching for a weapon, check also glove box, under car seats, in area of spare wheel etc. Be sure to wear protective gloves. Some adversaries may also try to conceal weapons under vehicles.

If searching for stolen contraband, especially small amounts, you are probably not going to be able to find it within the terms of reference of a regular, nonintrusive search. The best defence here is to separate parking from operational areas

Vehicle searches require specific and detailed procedures to be put in place and to be carried out thoroughly by search teams. How would you design and equip a vehicle search area within your own organisation?

with a pedestrian gate, where person searching is more effective.

Ensure there is a documented procedure for action on finds.

Ensure that officers know to report any attempt to bribe.

Ensure that officers remain polite, not overfriendly, and that their own human rights are not violated by abusive language. But expect as the norm some persons not to be happy with search.

A good, trained searcher can search a vehicle in less than 2 minutes.

The Importance of Search Training

As an experienced officer or supervisor, it is essential that you understand and implement the requirement for training for all types of search operations. The importance of this cannot be overemphasised. The consequences of inadequately trained personnel making errors in the search process can be far reaching and encompass the following:

Litigation and complaint from personnel being searched. This could be due to:

Perceived inappropriate behaviour.

Discourteous, aggressive or sexually inappropriate comments or requests.

- Damage to personnel or their belongings.
- Invasion of privacy or human rights.
- Unduly detailed or laborious searching.

Loss to the organisation:

- Due to undetected theft or smuggling out of items.
- Lack of thoroughness of search. ' Lax search procedures.

Death or injury to personnel. This could be due to:

- Searchers missing hidden items.
- Searchers not recognising threat items. Searchers failing to act correctly upon a find.

Lack of vigilance due to extended duties and shift working.

Notes Failure of monitoring and detection devices to detect threat items.

Failure to detain carriers of suspect items.

Searching for Listening Devices

Searching for listening devices first and foremost requires a physical search and recognition training. Some organisations develop an in-house capability, but due to this being an area of rapid technological developments, a reputable outside contractor is often a better choice. Two key technologies support the search process:

Non-linear junction detectors can be used to detect the presence of semiconductors. Semiconductors have universal application and are also used in bugs. A positive reading from a common electronic component, therefore, does not indicate the presence of a listening device, but a positive reading from behind a curtain, for example, would be suspicious.

Spectrum analysers detect transmissions. There are limitations: 1. The transmitter may be using GSM, making it difficult to discriminate from legitimate transmissions. 2. The transmitter may be activated only when the target is present, making it difficult to detect beforehand. The transmitter may not use wireless.

Conclusion

Searching is emotive, can be difficult to carry out and requires detailed training and effective management and supervision. Although often regarded as a mundane task, search procedures are a fundamental addition to perimeter and building security and access control measures. It is incumbent upon the security manager to ensure that any searching procedures are conducted with a clear remit and guidelines. Also, recording and reporting must be accurate. For these reasons it is essential that the security manager is thorough and methodical in planning and supervising such operations.


SECURITY NOTICE
ALL PERSONNEL
SUBJECT TO SEARCH

INFORMATION AND PERSONAL SECURITY MANAGEMENT

Introduction

Knowledge and information are amongst the most valuable assets that an organisation owns. In the highly competitive business environment, the organisation that judiciously and effectively employs and controls its sensitive information will develop and maintain an advantage over its competitors and adversaries. Because this information is such a vital asset it is a prized target, but its theft or loss is often underestimated as a workplace offence. As information is so valuable, the consequences of lack of protection can be catastrophic to an organisation.

There are two primary categories of information that an organisation needs to protect:

Proprietary Information — Proprietary information is information which belongs to the organisation and from which it derives economic benefit. This may include formulations, future, know how, financial projections etc. Some of this information is highly confidential. Insiders as well as competitors and foreign governments may pose a risk to this. Loss of proprietary information may lead to a loss in competitive edge.

Personal Data — This is information relating to living individuals. It may be staff personal information, or consumer personal information. The main threat to personal information comes from insiders (targeting customer databases) and organised criminal groups (targeting bank account details, credit card details etc.).

Individual Rights and Personal Data

Regardless of their position in society, every individual has the right to have their personal information protected and managed effectively by those authorised to manage and hold it. Those authorised to hold information about individuals will include employers, the government and its associated agencies, including the Police. The Data Protection Act 1998 gives all individuals (known under the Act as 'data subjects') these rights:

To find out what information a data controller holds about them.

To prevent the data controller from using personal data for the purposes of direct marketing.

To notify the data controller that information held about them is inaccurate. To have inaccurate information about them amended or destroyed.

To object to their data being processed if the processing is likely to cause them or someone else to suffer substantial damage or distress which is unjustified.

To claim compensation if they have suffered damage or distress because of the data controller failing to comply with the Act.

To ask the Information Commissioner to assess whether personal data has been processed lawfully.

The 'data controller' will be the person or department within your organisation responsible for managing and retaining information.

Often confused with the Data Protection Act, The Freedom of Information Act 2000 deals with access to official information. In addition, there are also regulations which provide access to environmental information (Environmental Information Regulations). The Act applies to most public authorities and to companies which are wholly owned by public authorities; it also requires public authorities to have an approved publication scheme, which is a means of providing access to information which an authority proactively publishes.

It can be seen therefore, that it is important, and a legal requirement that any information that you hold about individuals is correctly managed. Therefore, you should become familiar with the outline requirements of both Acts and your first port of call should be the Information Commissioner's Office.

Proprietary Information

Threats to proprietary information are many and varied. Some of the key threats are listed below:

Threat

Sources

Targets Methods

Foreign governments, information brokers, competitors Know-how, R&D, customer databases, sensitive pricing information, forecasts, financial reactions etc. Social engineering, IT penetration, insider spies, imagery, pretext visits and enquiries, data mining

Organised criminal groups More inclined towards personal data theft. IT penetration, password compromise, buying used computer hard-drives etc.

Employees Customer databases, presentations, formulations etc. Theft by USB drive or cell phone, photocopying, un-authorised printing, uploading to internet storage.

A broader list of threat sources might be:

Competitors.

NGOs.

Direct action and pressure groups. Governments.

What are the main types of information and the criteria to determine its value to the organisation?

Media.

Organised criminals.

Terrorists and insurgents.

'Whistle-blowers'.

Information brokers.

Commercial intelligence agencies.

Unions.

Disgruntled staff.

Temporary staff.

Trusted employees!

Information may be subject to espionage (theft) and leakage. Leakage may occur when there is an unauthorised release of information, deliberately or through carelessness and indiscretion — the aim or consequences of which is to place it in the public domain to discredit the organisation. In most circumstances under English law, neither of the above are criminal offences so are not indictable (arrestable) offences under The Theft Act. Action taken against information thieves is usually through the civil courts.

Information Security and IT Security

Much sensitive information, whether proprietary or personal data, is now stored in IT systems. This has many operational benefits but brings with it associated security problems. One problem is that large amounts of information are relatively easy to steal unless effectively safeguarded. The second is that the lines of responsibility are often blurred over who oversees protecting information from compromise.

If you are storing personal data on your IT systems, such as personal data associated with access control privileges the storage systems must be encrypted, with access on a strict need to know basis. Additionally, the USB ports on computers used to store or access such personal data should be locked down. This is covered in greater detail in the IT Security module.

Proprietary Information Assets

Some of the more common proprietary information assets that require protection are:

Client lists.

Research and development details.

Marketing plans.

Product launches.

Future expansion or downsizing plans.

Security plans. Financial and pricing details that are not for public release. Product formulation.

Research and development.

Executive travel plans.

Marketing / strategic plans.

Client's proprietary information.

Product designs.

Tenders.

Forecasts. Payroll.

Customer secrets.

These are stored — and are vulnerable to attack — in four basic domains:

' In people's heads.

In hard copy form.

As electronic data in computer systems. As information in transmission.

Specific Threats Social Engineering

Social engineering attacks manipulate staff to gain unauthorised information which can then be used to damage the organisation or for criminal purposes. Social engineering concentrates on exploiting the weaknesses of people, rather than IT systems or the computer security process. UK companies have reported attempts by attackers using social engineering techniques to elicit internal information by means of telephone, email and face to face contact. Email attacks are increasingly using more sophisticated social engineering techniques to appear more credible. Staff targeted tend to be those who work in customer facing roles, especially IT, help desks, receptionists, security guards, cleaning and catering.

Consider your own organisation and using the risk analysis matrix in the Security Risk Analysis Module, identify the top 5 risks to information within the organisation-

Specific Threats - Searching Waste

To a skilled adversary, waste, especially paper waste, can present a rich source of intelligence. In fact, intelligence agencies have been carrying out this practice for centuries. At the end of the day you should be alert to anything placed in bins that could be of potential use to an adversary. Don't entrust this to the cleaners — they could be working for the adversary in return for a bribe!

Sensitive waste should never be stored openly but should be shredded immediately or placed in specially designed receptacles.

Most importantly, all waste should be stored on site and, if possible, arrangements should be made for the waste removal contractor to come on site to collect. Waste that is left out in bins on public land, such as pavements, becomes the property of the local authority and you will lose control of who browses through it in search of confidential information.

Specific Threats — Employee Theft

Employees often represent the single most serious threat to sensitive data. This is especially the case with employees, who are about to, or planning to, leave. Information may be removed as documents, but it is more likely to be emailed out to personal email accounts, uploaded to personal internet storage sites, copied onto personal flash drives or onto memory in cell phones.

Information Protection Measures

We have established that an organisation's information is valuable and that the threats to it are varied. Having carried out the information risk analysis there are a range of measures that can be put in place to protect this asset and to prevent its unauthorised removal or transfer:

1. Target hardening - The Government of South Australia defines target hardening as 'the concept of opportunity reduction'. In terms of protecting information, where the holding and use of hard copy documents is still required;

target hardening, and access control encompass measures to increase the difficulty for adversaries to reach the information asset. Hardening may include the physical securing of documents and processing equipment, and the use of vaults, and containers. Complementing hardening, asset protection often relies heavily on access control in varied forms. Both methods are effective but restricting access can inhibit information flow.

2. Deflection - Even with hardening and access controls in place, the determined information thief is difficult to deflect. To adequately protect, measures to deflect the adversaries should aim to shift their attention to information of lesser or no value to the organisation. Alternatively, the aim could be to deflect adversaries to a piece of information whose loss can be immediately detected, although this measure should ensure that there is no undue risk of being accused of entrapment.

3. Technological Measures Even strict physical measures can be confounded by the rapid growth of availability of information loss facilitators which can be brought into the workplace (mobile telephones, flash drives, mp3 players and cameras). To defeat these threats the facilitators should be removed, either physically by banning electronic devices from the workplace or procedurally through regulation.

4. Deterrence Requires that potential adversaries think about the consequences of their actions, as many fail to do so. More important, deterrence requires that those who do think about the consequences see some real risk that they will be caught and punished. With the intangible nature of information, and the difficulty in controlling its use and leakage, adversaries' perception of risk and reward may be skewed further. The perception of reward may be best influenced by the threat of sanction or punishment against adversaries, but if there is a lack of effective procedural controls over information,

How do you protect sensitive information in accordance with information security best principles?

the rewards will outweigh the risk and make the theft of information an attractive proposition.

5. Searches - Even if the adversary decides to commit an offence, physical entry and exit screening can be effective in protecting information; searches for sensitive documentation and storage devices at workplace entry points will deter to some extent. Electronic systems can also screen information that is transferred to and from computer systems. Although effective for detection, this will not improve deflection and may be too late to stop leakage. Also, the effectiveness of such measures will be difficult to gauge until the effects of the leakage become evident. Screening employees before hiring and after termination can be more valuable for information protection as it allows an organisation to carry out a degree of due diligence against potential adversaries.

6. Surveillance - If it is assumed that some insider adversaries will evade screening, formal surveillance, surveillance by employees and natural surveillance will all have a part to play in protecting sensitive information. Physical measures such as patrolling security guards and CCTV will deter and deflect but can sometimes be intrusive and may infringe an employee's human rights. Vetted administrative staff in sensitive areas can be more effective as it is less overt and aggressive whilst achieving a level of control and monitoring of access and movement. Natural surveillance of photocopiers, printers and fax machines, controlled and located in working areas where there is oversight, will reduce the opportunity for theft or transmission of documents. This can be supplemented by the introduction of a strong 'challenge' culture where identities are checked, and unknown visitors are challenged. Conversely, and in the spirit of 'need to flow' there will be areas where surveillance needs to be inhibited — for example in board meetings and when sensitive information needs to be copied or transmitted securely.

7. Reducing Targets - Because an organisation needs to use sensitive documentation and resources both electronically and in hard copy, it will be impossible to fully remove the target. Measures can be put in place to rationalise the number of possible targets by reducing the information held, disposing of non-essential and expired information and retaining only that which is useful to the organisation. In terms of physical protection, the risk of loss of laptop and software held information and associated consequential losses can be usefully managed by controlling laptop use and the implementation of procedures and processes designed to limit the range of information held and processed by one individual.

8. Marking Property - With many targets unable to be removed, making them clearly identifiable as company property is a possible prevention measure. A company logo marked document or laptop computer will be an attractive and easily identifiable target for espionage, the media or a business competitor. Identifying property physically is often a brand requirement but will not be effective to prevent pure information loss. This human territorial instinct to take ownership of assets is strong and thus clear ownership definitions and delineation and policies of rights for personal use are essential to containing information loss.

9. Reduce Temptation and Deny Benefits Motivations and anticipated rewards for information theft can be compelling and the temptation for adversaries such as hackers to attack a computer system will far outweigh any risk concerns. Adversaries who are motivated by financial gain will be difficult to deter especially if there are a wide range of access points to information that are relatively weakly protected. The denial of information benefits can only be effective if the information that can be accessed is time expired, inconsequential or compartmentalised to ensure that it is of little use to the offending end-user.

Describe the threats to your organisation from information loss and explain the consequences to your business of this risk if inadequate protection js in places

10. Classification - If organisations recognise the information risks previously mentioned and accept that they must be dealt with, the imposition of clear rules concerning the handling of information in any organisation should have a strong mitigating effect on information leakage.

11. Procedures and Awareness This is possibly the most important method to protect against information loss. Throughout the workplace there should be a clear and properly

published policy for all personnel to be aware of the risks of losing information and the indicators that information is being lost. Such indicators may be:

- Hostile leaks to the media.
- New product copying by a competitor.

' Unexpected loss of a key customer due to price.

' Loss of key suppliers.

All personnel, either in the workplace or working elsewhere, must have the risks clearly communicated to them or know what to do if information is lost or compromised. They must know the processes and procedures to follow to protect information and the consequences of loss.

12. Protect Business Travellers Many organisations tend to forget that their employees who travel on business are particularly vulnerable to information theft. Such personnel carry information not only on their laptops and memory sticks but also in their heads. The business traveller and homeworker can be targeted either using alcohol, social engineering or 'honey-trap', leading to theft of documents and IT, inadvertent disclosure of critical information or the threat of blackmail. These employees are vulnerable risks in that they are away from the workplace and thus envisage themselves beyond management control. Business travellers, if in an exotic location, may well become dangerously vulnerable. Information loss through espionage, theft or loose talk can begin at the point of departure

INFORMATION AND PERSONAL SECURITY OPERATIONS AND MANAGEMENT

Introduction

Information Technology plays a vital role in all business activity. Without IT most businesses would struggle to survive. Yet the level of IT security in many organisations is alarmingly weak, and often enterprises survive by good fortune rather than by comprehensive security programmes.

IT security is especially important to you because many of your technical security systems have migrated to IT platforms and have converged. A security lapse on the part of just one user could literally take these systems offline for several weeks.

Key Assets at Risk

The key IT assets at risk are:

Workstations: Attacks can be both logical (i.e. through the system using computer code) or physical (e.g. a break-in and theft). Physical threats against workstation equipment may pose a significant threat for some businesses and few have contingency plans to recover quickly from attacks where large numbers of workstations have been stolen in a single burglary.

Laptops: Laptops are particularly vulnerable for the following reasons:

They are portable and concealable.

They have a reasonable resale value and can be relatively quickly disposed of due to demand.

They contain very large amounts of data, often more than is necessary, or safe.

For foreign intelligence agencies they are a rich source of commercial intelligence and can be relatively easily accessed when left in hotel safes.

They are left in view of thieves in specially designed laptop bags (in cars, when checking in to hotels, at railway stations, bars and restaurants etc.). They are taken home, where burglary protection may be significantly less than in the workplace.

There have been several cases recently where companies have suffered significant negative publicity (and, potentially damaging litigation) due to laptop theft and loss of employee data contained in them.

Unlike critical physical assets, sensitive data on laptops is rarely identified, stored in a single place and encrypted.

Fileservers: Fileservers should be in a central fileserver room, which should be secured and to which access should be restricted. Biometric access and exit control, with anti-tailgating photo-electric beams should be considered. Furthermore, the room should have no windows, strengthened walls and doors and should not adjoin properties not under the owner's control. It should not be situated near a car park or anywhere else where a bomb may be placed, such as a mail room.

Threat Sources

Threats to IT systems emanate from four main sources:

' Pathogens (e.g. viruses).

Hackers and other external adversaries.

Employees.

Hardware thieves.

Employee Misuse

Employees pose significant threats to IT systems, especially as use of desktops and laptops increases. Such threats include:

Misuse or use for personal purposes (e.g. running one's own business). Manipulation of data to commit fraud.

Software theft (copying or "borrowing").

Loading unlicensed software.

Internet and email misuse.

Accessing websites and inadvertently downloading spyware or other malware. Lack of productivity due to accessing Internet services.

Make some notes on the

Computer Misuse Act 1990.

Theft of peripherals.

Collusion with junior IT staff to steal "replaced" components. Information theft.

Many employee threats to IT systems are inadvertent. However, when a deliberate act is carried out against a computer, it may be in violation of the Computer Misuse Act 1990.

Hardware Theft — Risks and Solutions

There are four kinds of hardware theft that you should be concerned about as a security professional:

Theft of laptops — These may be taken from an individual when they are off-site or stolen by an intruder. By day, all laptops should be secured to desktops using cable locks, and if left on premises overnight should be locked away in a secure cabinet. Laptops should be indelibly marked with the owner's details. Laptops should be encrypted to render data inaccessible.

Theft of Desktop PCs — When thieves come on site to steal PCs they often steal in large quantities, causing major business interruption as a result. Some organisations prefer to protect office space after hours by patrolling, but whenever offices spaces are unoccupied after working hours, a cornerstone of protection should be PIR sensors and CCTV. Desktop PCs should be encrypted to render data inaccessible.

Theft of Fileservers — Fileservers are sometimes the target of burglars. Fileserver rooms should have special security arrangements and should never be in rooms with a shared wall to another property.

Password Violations and Solutions

The following are important recommendations when selecting a password:

Use a string of letters, numbers and symbols, including a mix of upper and lowercase, at least 8 characters long.

Never write down a password.

Use memorable phrases to help memory, for example taking the first letter of the following sentence:

I went to Spain in 05 and had a FAB time (IwtSi05&haFt)

Spyware — Risks and Solutions

Spyware is any software that covertly gathers user information or seeks out sensitive information. There are two kinds of compromise:

Software.

Hardware (keystroke loggers).

Software spyware compromises a computer using the same methods as viruses (flash drives attached to USB ports, web browsing, downloads, email attachments etc.). User awareness, discipline, and locking down of USB ports are key defences.

Keystroke loggers are the kinds of spyware device that you, as a security professional, are more likely to encounter. These are small plugs which are inserted between a keyboard cable and the back of a PC. They are very difficult to see if you are not specifically looking for them. The plug is a storage device, which harvests all the user's keystrokes. They are planted by those who have continued access to a location as there is a need to recover the device once it has done its work. Historically, the planting of such devices has been associated with cleaners and even security officers — in return for bribes.

Flash Drives — Risks and Solutions

Flash drives (USB thumb drives) pose two very significant risks to company computer systems:

Explain what is meant by the following:

Keystroke logger Distributed denial of service attack Phishing

If you are stuck, use the Internet to help you find the answer-

1. They can be used to introduce pathogens (malware) to computer networks. This is often inadvertent. Voluntary checks of security managers attending security management training have identified that up to 20% of them may be in possession of virus-infected flash drives! Additionally, the pathogen may be introduced to the network maliciously. Through social

engineering, an employee could be given a flash drive, perhaps at an exhibition, which, following attachment to the target network may open that network to remote file browsing.

2. Flash drives (which also include mobile phones, tablets, cameras and MP3 players) are a very convenient way for employee thieves to steal sensitive information from company PCs. You have no legal right to demand that an employee surrenders such devices for inspection on exit, and even if you did, the data could easily be encrypted.

The only sure way to prevent these risks is to use special software to lock down all USB ports. This will also block keyloggers.

Internet (Cloud) Storage Sites

Internet storage sites provide PC users with an online storage site to which they can upload files surreptitiously without first downloading software onto the PC. In a typical "attack" a user will create an online storage account from a domestic PC, mainly for innocent purposes. Once in the workplace they will then access network files and upload them to the online storage account. Once this has been done, they can download them onto the home PC later, or provide an outside accomplice with the storage site log-on details.

As a security operative you are not going to be in a position where you can prevent this, but you must ensure that appropriate safeguards are in place on security computers.

Printing

Printing unauthorised copies of documents is less of a threat than it used to be since there are now many more effective means of copying the original computer file. Probably the biggest vulnerability in this area comes from inadvertent disclosure — the discarding of unwanted printouts into a bin, which is then disposed of with the regular waste.

Some solutions:

Site a shredder next to printer for overruns.

• Use a passcode system and networked printers, whereby the user must enter a unique passcode to print out the documents that they send to the printer.

Email Attachments

Email attachments provide an obvious means by which sensitive data can be smuggled out of the company. A few basic steps can significantly reduce this risk:

1. File/folder access control based on file/folder permissions.

2. Network (and not workstation hard drive) file saving.

3. Specific workstations for specific employees. System configured to prevent users from logging-in on each other's workstations.

4. System configured so that users are prevented from sending file attachments unless authorised (Some users will have blanket authorisation).

5. No access to personal email. (Blocked "logically" and prohibited "procedurally").

6. Network monitoring and spot-checks to identify violators.

The Internet and the World Wide Web

The Internet is infected with literally millions of viruses, some attacking computers that browse to a page, others infecting downloads (video files, audio files, programs etc.). Unrestricted browsing can easily compromise a computer. There must be procedures and firewalls that restrict

List ways viruses can enter a computer system.

unauthorised web browsing on computers used for security purposes.

Public Computers - Risks and Solutions

Public computers are unsafe for business communications and should never be used for such. This is a message that should be made clear to all email account holders who can access their email accounts from outside the business premises.

Most of the dangers residing on public computers, such as those found in internet cafes or airport lounges, are hidden, but typically include:

Viruses and other pathogens (which can transfer by email or onto USB data sticks).

Keylogging spyware, designed to harvest user log-on details.

Foreign government "spyware", designed to collect intelligence against foreign companies (this need not have been planted by the host government, but by an agent of a foreign government who has simply used the computer or network on which the computer resides).

The threats are too prevalent to justify the use of such facilities for business purposes, and travellers should be provided with the necessary portable computer and communications equipment.

Data and Hard Drive Destruction - Risks and Solutions

Vulnerabilities

Deleting data from a computer (or any computer media) using the delete function merely removes the "signposts" to the data, not the data itself. Software to recover deleted files is freely available on the Internet. To permanently remove data requires the use of special "shredding" software.

There should be a specific procedure for all decommissioned hard drives and memory devices using one of the following methods:

' Using special destruction software to overwrite.

Degaussing.

Physical disintegration — best.

Wireless Networks Risks and Solutions

Wireless networks are often less secure than hard-wire networks, so care should be taken if using security devices via wireless protocols.

Business travellers should be advised to beware of 'Evil Twins' in which a spoof broadcast is set up near a legitimate broadcast to catch unsuspecting users and steal their data or payment information.

Data Backup

Data backup is important for business continuity.

The safest backups are those which are off-site. Increasingly, cloud solutions are being used, whereby data is uploaded to secure internet storage sites on a real-time basis.

Laptop data backup should not be overlooked. Often, for reasons of convenience users put large amounts of data onto laptops and the way in which they are used sometimes circumvents back-up measures.

Travellers should always take backups of their most critical data relating to their assignment in case of laptop theft.

Laptop General Security Principles

Laptops are both a particularly attractive target for thieves and, in many cases, a store of some of a corporation's most sensitive data. While workstations are routinely configured to save data to a fileserver, laptops are generally exempt from this protocol, making them a rich vein of competitive intelligence for a determined

How can viruses be uploaded on to personal and company computers and what measures can you take to prevent this?

adversary. The impact of loss is further increased by the fact that data back-up on laptops is not as regular as workstation data back-up, due to the way in which laptops are used.

The following is a list of best practice guidelines for laptop security. It will not be possible to adhere to every recommendation, but the more closely these recommendations are followed, the less will be the risk exposure.

1. Data Storage - Discourage the storage of large quantities of confidential data on a laptop. Confidential data should be protected by encryption but be aware that most commercial encryption can be cracked by many state security services. When travelling it is best to store confidential data encrypted on a removable drive.

2. Personal Data Do not store any personal/personnel/client data on laptops which could be of value to those engaged in ID theft. If the laptop is lost, or if the drive isn't cleaned properly upon decommissioning, you could become tomorrow's headline news story and your company could face prosecution under data protection legislation.

3. Hotel Room Safe Insecurity - Ensure that users are aware of the risks to data when laptops are left in hotel room safes. State security and other groups can engage hotel staff to open a safe (in a matter of seconds) and can copy the contents of hard drives in a matter of minutes using devices that can bypass passwords.

4. Hotel Room Security (General) - Assume that your hotel room is insecure and be alert to staff thieves, external thieves and thieves amongst the guests. A thief is likely to be able to think of all the "secret" places that you can think of to hide your laptop in a hotel room.

5. Cable Locks - Secure laptops when in use by day. The usual method is by

combination cable lock. At night laptops should not be left out on desks, even if secured with a cable lock, but should be taken home or locked away in a secure cabinet.

6. On-Site Secure Storage - Accept that there may be circumstances when a laptop holder may go to a bar or restaurant after work and may not want to take their laptop due to the risk of theft. Provide appropriate on-site secure storage for such eventualities.

7. Asset Engraving - Ensure that laptops are clearly engraved (and registered) to discourage theft. "DNA" watermarking may be an additional consideration.

8. Decommissioning Procedures - Ensure that when a laptop reaches the end of its useful life it is not sold on to a third party, but that it is destroyed or disposed of in some other safe way. Research carried out by a UK university revealed that confidential data could be recovered from many used laptops sold on eBay, even after the hard drives had been cleaned.

9. Be Thief Aware - Assume that a potential laptop thief is always nearby and provide appropriate safeguards. Never leave laptops in hotel conference rooms at lunch under the "guard" of banqueting staff, and never leave them in open view in a vehicle. Always ensure vehicle doors are locked, especially when stopping at traffic lights.

10. Malware Protection - Ensure that laptops are provided with their own suite of antivirus, anti-spyware and firewall software and that they are configured in such a way as to be resistant to penetration when using a public wi-fi hotspot or hotel guest network.

1 1. Backing Up - Ensure that laptop hard drives are backed up regularly. Laptop hard drives are many times more likely than PC hard drives to fail. If you need data for an event or meeting, always ensure that a copy is carried on an encrypted flash drive or CD/DVD.

12. Data Stick (Thumb Drive) Dangers - Be wary of transferring files between laptops using USB thumb drives. This activity can mask a range of dishonest activities.

13. Passwords - Use passwords and secure folders to protect confidential data. Setting up a boot-sector password, while not providing water-tight security, is very important. Passwords should be a mixture of letters and numbers using both upper and lower-case letters.

14. Password Storage - Do not use the Windows option to remember passwords. If you need to store them on your computer use an encrypted file such as that provided by Steganos

(if allowed to use such software). Do not store them in MS Word password protected documents as MS Word passwords can be broken in seconds.

15. Windows Updates - Ensure the laptop is switched off properly after use. This will ensure that automatic Windows security patches and updates are installed properly.

16. Bars and Restaurants - Try to avoid taking a laptop into bars and restaurants. This is where very many get stolen. If you cannot avoid this try at least ensuring that your hand or leg remains somehow "connected" to the laptop bag strap. Thieves are adept at creating diversions in such environments, and in hotel reception areas at check-in and check-out.

17. Peripheral Device Blocking - Consider the use of software to block all but authorised peripheral devices, such as USB data sticks. Remember that many personal audio devices and mobile phones can now be used to steal data via the USB port.

18. Confidential Data - If you must store confidential data on your laptop try to keep it in one place. Hide the folder and encrypt using 256-bit encryption software (note that it may be illegal in some countries to use this. This will often be because that country's national intelligence agencies can't break it, which may be a good reason for having it in the first place!)

19. Secure Communication Channels - Use VPNs to communicate with your corporate network.

20. Removable Hard Discs - If you have the option for a removable, as opposed to a fixed, hard drive, take it. This is especially the case if you stay in hotels and leave your laptop in a hotel safe. It takes 15 seconds to open a hotel safe without the passcode and override devices are often held in a desk behind reception, often with no "sign-out" or record-of-use procedure. It takes just a few minutes to clone a laptop's hard drive. Boot sector passwords can be bypassed by a prepared adversary. Hotel staff are sometimes in the "employ" of law enforcement or intelligence agencies. Foreign hotel staff in the UK, for example, may be in the employ of their own agencies. Some hotel staff are susceptible to bribes from outsiders (commercial information thieves).

21. Transferring Data to Secure Portable Media - Don't assume your data is gone if you delete it from your hard drive and transfer it to a portable drive. To permanently delete data, you must put it through a shredder or scrub the entire hard drive using special software to the standards outlined in this handout.

22. Screens to Restrict Peripheral Views Use a laptop privacy screen to reduce the risk of peripheral visibility when on trains, planes etc. Be alert to shoulder surfers and CCTV cameras in airport lounges, WIFI zones etc. These read both your screen and your keyboard actions.

Within your organisation, what are the IT hardware, software and network protective measures, policies and procedures in place? How can you improve these policies and procedures?

23. Hacking Risk - Be aware that Wi-Fi zones and hotel cable broadband can open your laptop to hacking. VPNs are no fix for this. Ask your IT specialists to provide you with a special firewall to reduce such vulnerabilities.

24. Spoof Wi-Fi Zones - Beware of the danger of spoof Wi-Fi zones. This is done by another user in the same vicinity blocking the genuine Wi-Fi site and generating a clone from their laptop. This is a relatively simple process for those with the technical know-how, and the purpose is usually to hijack logon details and to use the real network for free. More dishonest attackers may want to steal credit card details, whilst others may want to steal communicated or hard drive data.

25. Don't Use "High-End" Equipment Ensure the use of laptops which have the lowest specification consistent with operational requirements. High-end laptops are significantly more attractive to thieves, especially during breaking and entering activities.

Conclusion

The range of risks facing IT users is wide and ever-increasing. The problem for your business is that IT systems are business critical, almost all your business activities depend upon IT and therefore it is essential that systems are protected as much as possible. You and your IT department should consult regularly and agree upon an integrated programme to protect your business across the range of threats failure to do this could mean that, in the worst case, your business could fail completely.

Customer Care

Introduction

Security staff are often the first representatives of an organisation that a customer meets. The importance of good customer service in dealing with customers and clients is essential to preserving and enhancing an organisation's reputation and image and thus security staff have a pivotal part to play. It is important to ensure that by projecting a positive image, building rapport and communicating effectively and with courtesy, the role of security maximises its value to business and its operations.

A common failing of security departments is that they project a 'hard' image. Whilst this image and associated behaviour has its place, it is often not appropriate in a business context. Also, it is a fact of modern business life that security has extensive dealings with not only external customers but also counts the organisation's own employees as customers.

To be effective, the security staff must clearly understand the need for effective customer service and the methods which they can use to enhance their own and the organisation's image and reputation.

Identifying Your Customers

Before you can devise a customer care strategy, you need to identify your customers. What type of customers will your security officers be expected to deal with as part of your daily business and at what levels?

Customer Attributes

Having identified the range and type of customer that you will be required to deal with, the next stage is to consider the following:

> What do they want from you? Different customers will require different things from security staff. Some will expect protection; some will treat security staff with contempt.
>
> What sort of people are they? They may be keen and well disposed towards the company or they may be aggressive or have a bad attitude towards both the company and individuals who work for it.
>
> What do they think of you? Security personnel are often viewed with suspicion; it is important to understand the views of individuals.
>
> What do they think of your service? Some may feel that your staff provide a good service, others may feel that security restricts freedoms; others may not have an opinion at all.
>
> How can you make them feel valued? If your staff are brusque, abrupt and rude, their customers will not feel valued or included in corporate activity.
>
> How could you fail them? Your staff should make every effort to ensure that the service that they deliver provides customer satisfaction, commensurate with corporate security goals.

Your Product

All business functions have an output which adds to the organisation's operational effectiveness and thus strengthens progress towards achieving profitability and continued success. Security is no different. Security is a business function which protects assets (people, property, information, operations) against predictable and unpredictable threats using a system of appropriate proactive and reactive measures. Your customers expect you to deliver this product and ensure that it is delivered properly in support of the business.

What Matters to the Customer?

Your customers' expectations are important and what matters to them should matter to you and to your department. Your customers will place great emphasis on the following:

Your product — Your customers will want you to deliver your product to a satisfactory standard. They will require the company's assets and their own to be protected and this will need to be delivered with courtesy and avoid as much as possible any detrimental effect on the company's operations or

Having identified your customers, consider now your own organisation in accordance with the questions above and identify the areas in which your customer service is adequate. More importantly, identify the areas where your department does not meet the necessary standards.

business. The product will also need to be delivered in a cost effective and efficient manner.

Product reliability — Your customers expect your product to work fully always, day and night. If your product is unreliable, security breaches will occur and thus become a pointless expenditure for the business.

Consistency of service — You must ensure that the product meets expectations as far as consistency is concerned. The product must be delivered to a common and consistent standard, not only for reliability but also to ensure that there are no inequalities or discrimination when dealing with the customer base.

Speed and efficiency Lethargy and inefficiency are inappropriate in security personnel. Your customers expect you to be able to provide a service that is timely and conducted with a degree of vigour and commitment. You should aim to instil a culture of efficiency amongst your staff.

Courtesy — This is fundamental to effective customer management. You should ensure that a culture of courtesy is applied throughout the security department. This is especially important as security officers will often face provocation, disdain and sometimes abuse. It is rare that any approach other than a courteous one will contribute to resolving a difficult situation.

Telephone answering — You should ensure that your security officers are trained and practiced in dealing with customers over the telephone. In the same vein as considerations for courtesy,

an effective telephone manner will not only get the job done but also enhance the reputation and standing of your department within the organisation.

Value of information given Personnel should know their business and what their required level of service is. They should also be aware that the information, guidance, advice and instructions given to customers must be correct in both content and in the way, it is communicated. It will take only one error in this regard to begin to erode respect for the security department.

Positive attitude by staff — This is everyone's responsibility. The job of a security officer can be thankless and sometimes repetitive and without your input their morale can potentially be damaged. An effective security supervisor will not only encourage positivity but also will encourage their personal and professional development. They should apply a range of effective management techniques to support their team and ensure that they meet all requirements of both customers and business.

The Provision of Quality

Quality is often discussed in the workplace. Quality is about supplying customers with what they want, in accordance with their standards and expectations, and with a predictable and consistent degree of reliability and consistency. Meeting your customers' expectations is another essential component of effective customer service.

In effect, quality of service is defined by your customer. If you, the service provider, try to define your own level of quality without consumer consultation then it is highly likely that you will not meet customer expectations. In effect, it is more likely to reflect what you want rather than what they require.

It is important to remember here that customer expectations move on. In changing social climates, it is important to ensure that we meet the needs of customers based on their expectations. Although customer expectations vary from culture to culture.

Also, consider the fact that only the customer can determine whether they have received an expected level of quality. If the feedback that you get about your security provision is negative or you have many complaints, you should acknowledge the fact that there must be some justification. Identify what has gone wrong and put it right.

Look at each of the previous sub-headings and describe the areas of your department where you have procedures in place to meet customer requirements. Highlight any areas where you feel that your staff fall short of requirements and explain clearly whether the source of the problem lies with individuals or the training and procedures you provide for them.

Human Factors

The most important aspects of enabling your staff to do their job are to ensure that they can deal with other people effectively. The basic skills that your staff need to master are:

> Building rapport - The effectiveness of your security programme will not be compromised if your staff can manage to build rapport correctly. Whilst it is important to have an efficient, uniformed presence there is no need to alienate customers. On the contrary, your customers will be more inclined to cooperate with security processes (often seen as an inconvenience) if your security operatives can build a rapport.

Building trust - This goes hand in hand with building rapport and is based not only on what your security personnel say and do, but also on the fact that they can be relied upon to act fairly and without distancing the customer.

Rapport - Rapport and trust cannot be established without the security operatives listening to, and acting upon, the customer's requirements. This is especially important when dealing with customer complaints and feedback, where it is essential that the individual feels that their views are noted.

Communication - Your personnel will be required to deal with other people in various situations and they should be ready and able to communicate clearly and courteously with individuals and groups of people. An aspect of communication which is often overlooked is the need to develop an efficient and effective telephone manner. Similarly, your operatives should be able to communicate in an appropriate tone and style when using email.

Appearance - Your customers will respect your personnel if they are properly presented. You should ensure that your operatives' uniforms fit properly and that they maintain minimum standards of cleanliness and tidiness in their appearance. A well-presented security operative will give the impression of efficiency and capability, which will in turn engender trust and rapport with customers.

Handling Complaints

Notes

It is a fact that with any business or organisation where there is a customer and provider relationship, complaints will occur. Complaints may arise because the customer feels that they have not received the service that they require and although the service provider may not agree. It is useful to remember and adhere to the principle that 'the customer is always right'. Of course, the customer may not be in the right on every occasion, but it is most important to ensure that the customer is assured that everything within reason is being done to accommodate their problems/issues. It is therefore very important to establish a relationship with the complainant that is based upon empathy and trust.

The aim of providing an efficient complaint handling process is to enhance customer satisfaction by creating a customer-focused environment that is open to feedback. If there are perceived issues with the security programme or department it is essential that they are faced and resolved to the customer's satisfaction and this in turn will ensure that the security department will can operate more effectively and, in a manner, appropriate to its customer base.

However, it is important to ensure that you do act upon complaints rather than paying lip-service to resolving any complaints received. Customers will look to see if their complaint has been actioned, and failure to do so may result in the perception that the security department is not committed to supporting its customers and enhancing the organisation's ability to improve its product and customer service.

When dealing with an irate or dissatisfied complainant, your personnel should be prepared first and foremost to listen thoroughly to the complaint. This will have two purposes: firstly, to ensure that the complaint is fully understood; secondly to ensure that the complainant feels that the complaint is being taken seriously. During dealing with the complaint, security personnel should verbally acknowledge the statements being made without necessarily admitting fault or blame for an incident.

Further to the previous actions, the fundamental procedure for handling a complaint is for the organisation to take it seriously and to manage it positively until it is resolved. Neither the security department, the business, nor the complainant will gain any benefit from you ignoring the difficulties associated with a complaint. This will require the security department to take 'ownership' of the complaint and to record any actions carried out in response to it. It will be useful to establish not only a clear complaints procedure which should be followed but also a complaint registers and reporting process so that no details are missed.

It is important to emphasise here that, although a complaints process should be planned, it will be rare for any two complaints to be the same and therefore there must be flexibility in the procedures and plans, to ensure that a bespoke solution can be reached.

Training in Handling Complaints

It is easy to spell out in writing how your personnel should react to what may be irate and possibly unreasonable demands from customers and to draw up procedures. It can be more difficult for your personnel to respond calmly and productively in the face of provocation. It is important that you ensure that your personnel who do need to face customers have been trained and made aware of the issues involved. You should aim to convince your top management that such training is crucial for both personal and professional development in addition to the organisation's good reputation. There are many training providers available in the market that can provide enhanced training in subjects such as:

Conflict management.

Complaints handling.

'Transactional Analysis' understanding customer behaviours.

Developing a policy for handling complaints.

Communication skills.

Building customer loyalty.

Recognising and addressing the needs and expectations of complainants.

By investing in training for your personnel you will give them the best chance of resolving complaints appropriately and efficiently.

A Process Example

There are many methods to approach the issue of complaints. Many organisations take the view that complaints are welcome (to an extent) because they allow them to have a second chance at providing customer satisfaction and give feedback to the organisation on its performance. A good example of complaint management can be found at the website of the Scottish Ombudsman: http://www.valuinqcomplaints.orq.uk/

Websites such as this provide not only guidance on general complaint handling but also links to best practice in industry and public organisations who are required to deal with such issues on a regular basis.

Conclusion

Customer service can be a difficult issue for the security department. Whilst balancing the needs of customers, the security officer will need to ensure also that they maintain their focus on protecting yours, the client's and the organisation's assets. If you can manage your customers and their complaints properly, then they may even return as more loyal customers in the long term. The consequences of failing to manage customers and their expectations can also have long-term repercussions and far-reaching effects on the department and your organisation. You should by now have a clear view of the strengths and weaknesses of your department in customer service functions Devise and describe the process that you feel can be recommended in your organisation to meet both the organisation's and customers " expectations

Drug and Substance Abuse

Introduction

Businesses and other organisations employ people, and their workforce reflects the society in which they operate. Drugs and alcohol are increasingly used across all levels of society and because your workforce is a part of that society, employees will bring their substance abuse problems with them into the workplace. Approximately 70% of substance abusers are employed full-time and they are far more likely to be involved in an accident or other incident than their workmates who do not abuse.

Abusers are prone not only to more accidents but also to:

Sickness and general poor health.

Psychological impairment.

Absenteeism.

Low productivity.

Criminal acts.

If you discover an employee in the workplace in possession of drugs for personal use, or under the influence of drugs, the usual course of action is to remove that employee from a position where they can cause harm to themselves or others, then refer the matter to line management or HR. The action usually taken is that the employee will then be offered an opportunity for treatment under an employee assistance programme.

Classifying Drugs According to the Law

The types of substance that are generally misused are either drugs or alcohol. The types of drugs that are abused vary greatly in cost, effect and availability but all are in use within UK society. The Misuse of Drugs Act 1971 lists the drugs that are subject to control and classifies them in three categories according to their relative harmfulness when misused:

Type of Drug

Class A Drugs (includes ecstasy, LSD, heroin, morphine, cocaine, methadone.) Up to 7 years imprisonment or an unlimited fine or both. Up to life imprisonment or an unlimited fine or both.

Class B Drugs (includes amphetamine, cannabis, dihydrocodeine.) Up to 5 years imprisonment or an unlimited fine or both. Up to 14 years imprisonment or an unlimited fine or both.

Class C Drugs (includes GHB, temazepam, valium, temgesic.) Up to 2 years imprisonment or an unlimited fine or both. (Applies to temazepam and valium without a prescription). Up to 14 years imprisonment or an unlimited fine or both.

Being in possession of illegal drugs is a crime How would you approach a situation at an entrance checkpoint in which you discovered small wraps of white powder in the possession of an employee?

Theoretically, the possession of many drugs is an indictable offence, but you are not advised to arrest an employee if you believe they are using illegal drugs in the workplace. Instead, the matter should be reported to HR or line management for immediate action. Your legal department may have a different view if you discover that the workplace is being used for production or supply. In such a case proactive police involvement is best as evidence is easy to destroy and the suspect may be able to mount a plausible defence if the evidence is not processed meticulously.

Classifying Drugs According to Effect

Drugs can be grouped into:

Depressants (e.g. alcohol, barbiturates, opiates, benzodiazepines). Not all of these are illegal, but they may impact on safety if used in certain jobs or areas. Certain opiates are prescribed for severe pain, while benzodiazepines can be prescribed for stress, anxiety, insomnia or bereavement.

Stimulants (e.g. ecstasy, cocaine, crack cocaine, amphetamines). Not only are these commonly abused by the young, but also (especially cocaine) white collar workers in high pressure jobs. Can cause severe mood swings and over-confident, aggressive behaviour.

Hallucinogens LSD, magic mushrooms). A user under the influence of hallucinogens may be a danger to themselves and co-workers. Persistent abusers may suffer flashback hallucinations.

Mixed Effect (Typically cannabis.) Various strengths cause various reactions. Cannabis is often a social drug. Look for groups of workers sharing a cigarette.

Alcohol

Despite alcohol being socially acceptable, many company terms and conditions have a zero-tolerance policy towards alcohol consumption during working hours. Due to its social acceptability

alcohol is often the highest cause of lost productivity and is a significant cause of accidents and workplace incidents. If alcohol is smelled on the breath of an employee entering site, a report should be passed to that employee's line manager, who will determine whether that employee is fit or safe to work.

Cannabis

Cannabis is the most widely-abused illegal drug in the UK, and contains the active ingredient THC, which can make you feel very chilled out, happy and relaxed. Cannabis comes in three main forms, marijuana, hashish and skunk.

Marijuana, also known as grass and weed, is made from the dried leaves and flowering parts of the female cannabis plant and looks like tightly packed dried herbs. It is usually smoked in a cigarette. The paraphernalia associated with marijuana abuse is the same as self-rolled tobacco cigarettes, so it is very difficult to identify users, who may try to disguise the smell of the marijuana with tobacco smoke.

Hashish is stronger and can cause hallucinations. Hashish is a black or brown soft lump made from the resin of the cannabis plant.

Skunk is the term used to refer to strong forms of herbal cannabis that have increasingly dominated the UK market. This is both imported and grown illegally in the UK under artificial lighting. The general effects of cannabis are euphoria; relaxation; slowed reaction time; distorted sensory perception; impaired balance and coordination; increased heart rate and appetite; impaired learning; memory; anxiety; panic attacks; psychosis.

Cannabis is most commonly smoked, but may also be ingested, disguised as food.

Opiates

The most commonly-abused opiate is heroin, although certain prescription opiates may also be abused. Heroin is a drug made from morphine, which is extracted from the opium poppy. Opiate users on a rehabilitation programme may also be under the influence of methadone, and here a decision must be made as to how they can be safely employed.

Morphine is a very strong painkiller and a small dose of heroin gives the user a feeling of warmth

Use www.talktofrank.com to list typical vocabulary clues that may indicate a person is associating with substance abusers, or may have an unhealthy association with illegal substances

and well-being, and relaxation. It is highly addictive, and people can quickly get hooked, causing users to be associated with higher levels of theft to feed their habit. Heroin is usually supplied as a white or brown powder.

Heroin paraphernalia includes hypodermic needles, small cotton balls used to strain the drug, spoons or bottle caps for "cooking" (liquefying) the heroin, and a "tie-off" that the user wraps around his or her arm to make his or her veins protrude. Paraphernalia for sniffing or smoking heroin can include razor blades, straws, rolled bank notes, and pipes. Also, balloons are used as a method of transporting and/or trafficking the drug.

Because of the destructive effects of heroin, users often exhibit a decline in personal hygiene and an unkempt appearance.

Heroin is most commonly injected but may also be smoked or snorted.

Benzodiazepines

Benzodiazepines are widely prescribed by doctors for sleep disorders, anxiety, stress, bereavement, muscle relaxants (e.g. back injury), etc., so it is conceivable that members of your workforce may be using this class of drug legitimately. However, there are question marks over which kinds of benzodiazepines (and in what doses) should not be used by employees in hazardous areas or in hazardous occupations, for example driving. This is a matter for HR and the company drug and alcohol policy, which should address these issues within the bounds of privacy legislation.

Benzodiazepines are Class C drugs. Most of them are only supplied and produced by those authorised to do so, and it is an offence to possess such without prescription.

Benzodiazepines, especially diazepam, have been illicitly imported into the UK, resulting in their wide availability and use, even though the number of prescribed drugs has decreased in recent years. Abusers may take them specifically for their tranquilizing effects, or to come down from a high induced by stimulants.

Stimulants

Three main kinds of stimulants are cocaine (also known as crack), amphetamine and methamphetamine.

Cocaine is a white powder that is usually snorted. Its effects are short lived temporarily speeding up the way the mind and body work, making the user feel on top of the world, very confident, alert and awake, but also leading to over-confidence, arrogance and aggression and risk-taking behaviour. Crack cocaine (a rock-like form of cocaine) that has been prepared for smoking reaches the brain more quickly than snorted cocaine and has a much stronger and more immediate effect, which is usually of lesser duration than regular cocaine. The paraphernalia associated with crack are home-made crack pipes containing foil, and lighters.

Cocaine comes in a white power form and tell-tale evidence can often be found in toilets. Paraphernalia associated with cocaine are rolled banknotes, razor blades, straws and mirrors. Due to the risk of aggression, it may be difficult to remove a person under the influence of cocaine from the workplace.

Amphetamine and methamphetamine induce similar effects to that of cocaine, and can be taken in various ways, including as pills. The crystal form of methamphetamine, sometimes called crystal meth or ice, is extremely powerful and addictive. Smoking crystal meth, a purer form of methamphetamine, gives a very intense 'high', like crack cocaine but much longer lasting between 4 and 12 hours.

Club Drugs

The most common club drug of abuse is MDMA (ecstasy), usually supplied in the form of small pills, and often with image engraved. Ecstasy causes an energy buzz that makes people feel alert, alive, in tune with their surroundings, and with sounds and colours often experienced more intensely. Effects last for 3-6

You have found cocaine paraphernalia in the toilets What action should you take?

hours. Users often develop temporary feelings of love and affection for the people they are with and for the strangers around them.

Hallucinogens

Several illegal drugs taken in large quantities may cause hallucinations, but LSD and psilocybin (magic mushrooms) are specifically identified as hallucinogens.

LSD, commonly called "acid", often comes as what looks like small stamps of blotting paper, often with an emblem print. LSD is a powerful hallucinogenic drug, which means that users are likely to experience a distorted view of objects and reality, including seeing and sometimes experiencing hallucinations. These can be pleasant or terrifying to the user. Perhaps the most important thing for you to know about LSD is, once the "trip" has started you can't stop it. You must remove the user to a place of safety and this can be exceptionally difficult if the person is experiencing a bad trip.

Magic mushrooms are of the "liberty cap" variety (although other mushrooms may be abused). After picking, they are often eaten raw or are dried out and stored. Some people use the dried mushrooms to make tea. The main effects and risks of magic mushrooms are that colours, sounds and objects appear distorted, and sense of time and movement can speed up — or slow down.

Inhalants

Volatile substances that are illegitimately inhaled cover a wide range of products, such as gases, glues and aerosols. Abused products all have a legitimate day-to-day use, and many can be found in the workplace.

When inhaled, volatile substances have a similar effect to alcohol, causing inhibition, euphoria and dizziness and sometimes giggling. They can also cause mood swings, aggressive behaviour and hallucinations. Effects are short lived, prompting the abuser to repeat the inhalation. Substance abuse can cause sudden death; between 2000 and 2008, volatile substance abuse killed more 10-15-year olds than illegal drugs combined. Notes

According to www.talktofrank.com, common signs of using volatile substances are mainly non-specific and could have other common causes. However, they can include:

Dizziness.

Slurred speech.

Loss of coordination.

Talking as if hallucinating.

Paranoia and anxiety.

A chemical smell.

Changes in appetite.

Persistently runny nose or eye irritations.

Complaining of headaches.

Rashes and pimples around the nose and mouth, though these occur only with the use of specific products and may just be due to normal teenage acne.

In addition, there may be:

Lots of used products (empty aerosol cans, tubes of glue, etc.). Teeth marks on nozzles.

White marks on towels.

Solvent soaked rags left lying in unusual places.

Plastic bags with solvent evidence left lying in unusual places.

What to Do if Abusers are Suspected or Discovered in the Workplace

Organisations do have options available to them when substance abusers are suspected or discovered in the workplace. These options can be limited by law, regulation and workplace employment agreements and it is important to ensure that any actions either planned or conducted are carried out in accordance with such measures.

Surveillance The use of CCTV or other surveillance in the workplace is subject to strict regulation to protect the human rights and freedoms of individual employees. Unit 2.5 (CCTV) provides guidance on the employment of such systems and the requirements to warn employees that the area in which they operate is under surveillance. Likewise, CCTVs used for monitoring production processes or similar operations should not be re-tasked to monitor for drug use without this fact being clearly advertised and signed. Organisations and their managers, including security, must be clear on the rule of law and of the consequences of monitoring without permission or advertising.

Searches - Whilst searching an individual or their property and vehicle may be a very effective method of detecting drugs and of deterring their use in the workplace, the adoption of any search programme should be made only after serious and detailed consideration. Searching is intrusive and can seriously damage employer/employee relations if it is conducted clumsily or inappropriately. Unit 2.7 (Managing the Search Process) provides more details on the specific requirements and considerations for conducting searches in the workplace.

Police Involvement There may be a requirement to involve the police once substance abuse has been discovered in the workplace. This decision will again depend upon the individual company and its corporate culture. If your organisation regularly brings in the police to conduct investigations there may be a problem with distrust and distance between employer and employee. Also, there is the risk the police will not wish to become involved, especially if it is related to alcohol and Class C drugs. Importantly, police involvement may mean that you will lose control

over the investigation. All these considerations mean that police involvement must be carefully considered before implementation.

(Adapted from 'What are the UK Drug Laws?' Drug scope 2009)

Substance Abuse Programmes

Employing organisations should aim to establish procedures or policies so that help can be provided in a professional and consistent manner. Employee Assistance Programmes (EAPs) can be

Notes devised and put in place to help employees to deal with their substance abuse problem. It is important for supervisors and managers to have a resource or procedure that they can rely on if the need arises. Employees need to know that everyone will be treated the same way. Preplanning, as for many other occupational health and safety issues, is the best way to avoid confusion and frustration in situations that are already difficult to manage. In addition, managers and supervisors should be educated in how to recognise and deal with substance abuse issues, and employees should be offered educational programmes.

To ensure that it is ready to face substance abuse issues in the workplace, the organisation should:

1. Write a Drugs and Alcohol Policy, which may include:

    A statement of the purpose and objectives of the programme. A definition of substance abuse. A statement of who is covered by the policy and/or programme.

    A statement of the employee's rights to confidentiality.

2. Ensure that arrangement has been made for employee education.

3. Offer provision for assisting chronic substance abusers.

4. Outline how to deal with impaired workers.

5. Issue a statement of under what circumstances drug or alcohol testing will be conducted.

6. Arrange provision for disciplinary actions.

7. Ensure that the main points of this policy are included in employees' induction programmes.

8. Provide continual employee education using in-house publications and notice boards.

9. Provide pre-employment screening at least for safety-critical posts.

10. Provide drug use awareness training for managers and supervisors.

11. Provide drug recognition training for security staff.

12. Provide a confidential point of contact for employees with a drug problem.

Employee Screening for Substance Abuse

Companies and organisations can initiate drug screening procedures in the workplace, to ensure that employee substance abusers' activities are limited, and to reduce the potential incidence for drug or alcohol related accidents.

Screening could be carried out in the following circumstances:

As part of the recruitment process for job applicants.

Randomly within the workforce.

Compulsorily for safety-critical work where the consequences of abuse-related accidents can be serious.

As part of a rehabilitation programme to support an abuser.

In the event of suspicious behaviour or that indicating substance abuse.

Following an incident or accident which may be due to substance abuse or its effects.

An outside agency should be engaged to conduct the screening programme. The benefits of this are obvious: reliability, impartiality, sound advice, expertise and experience. Another benefit is that the agency will often be able to provide bolt-on options such as an education and rehabilitation programme.

Because testing and screening can be seen to be invasive or an imposition upon personal freedoms, companies which carry out their own testing risk either alienating the workforce or generating inaccurate results, which may lead to claims of unfair dismissal being upheld at industrial tribunals.

In the UK the Forensic Science Service is widely accepted as the leading drug-screening authority

although there are many private companies which can provide a drug screening service.

When a screening system is in place, an employee's obligation to submit to testing should be written into the terms and conditions of employment, which will provide protection and guidance for both employers and employees in the event of any subsequent disputes or problems.

Types of Drug Screening

There are five main types of drug test — these are urine, blood, hair, saliva and sweat. Each type of test has its unique attributes and the cost, effectiveness and level of accuracy of the test will influence the type employed. It is important also to realise that drug tests can be intrusive and may well cause an atmosphere of mistrust or hostility in the workplace. It is essential therefore that any type of screening programme is very carefully considered before implementation and the risks and benefits to the organisation are considered and balanced.

To ensure that appropriate methods are used it is strongly recommended that a professional external consultancy or agency is employed when screening is deemed to be necessary.

Success in Dealing with Substance Abuse With an effective substance abuse programme in place, your organisation will can meet the problems associated with the problem. Throughout the process of maintaining the programme, there are several steps which can be taken to maximise your chances of success:

1. Keep written records that objectively document suspect employee performance. These can be used as a basis for referral for testing or for other disciplinary action if specified in your organisation's policy.

2. Know your employees. Become familiar with each one's skills, abilities, and normal performance and personality. This will make it easier for you to identify the erratic and

Draft a template that other employees in your organisation can use for dealing with a suspected employee who is abusing drugs or alcohol

unusual behaviour associated with substance abuse.

3. Become familiar with common symptoms of drug use.

4. Document job performance regularly, objectively, and consistently for all employees.

5. Act whenever job performance fails, regardless of whether drug or alcohol use is suspected.

6. Know the exact steps to be taken when an employee has a problem and requires help.

7. Communicate immediately with the correct level of management when you suspect a problem and have a witness to your action when confronting an employee.

8. Do not misuse the drug prevention programme to discipline employees for problems not related to substance abuse.

9. Do not single out any employee or group of employees for scrutiny under the company's policy. Be consistent with all employee groups or classes.

10. Do not confront a suspected drug dealer alone. Always have a witness to your actions. Consult local law enforcement for advice or assistance in these cases.

11. Do not assume that anyone in your organisation is immune to the problem of drug and alcohol abuse.

12. Always have a written substance abuse policy.

13. Do not address drug abuse without including alcohol abuse in the policy

14. Do not implement a policy and programme unilaterally if you have a unionised workforce.

15. Do not forget that the majority of the nation's workforce is drug-free and does not abuse alcohol.

Contingencies and Emergencies

Introduction

Your organisation has an obligation to protect its employees, stakeholders and shareholders and shareholders' interests through provision of an appropriate system by which to manage all foreseeable emergencies, crises and disasters. The way in which organisations do this is through contingency planning.

The aims of contingency planning are as follows:

To protect the short and long-term interests of the business.

To maintain the continuity of the business. To avoid the deterioration of any emergency or crisis into a disaster. To quickly restore business operations in the event of unavoidable interruption. To effectively communicate with the outside world.

In many organisations, because the security manager has a good overview of the strengths and weaknesses of the organisation, and because of their relationship with law enforcement and other agencies, the security manager is well placed to take on the role of the contingency planning coordinator. The security manager's role is therefore often extended to include responsibility for the formulation of the contingency management plan, devising exercises, resourcing training, establishing a crisis management centre etc. This unit will describe the nature of emergencies, crises and disasters and the contingency activities that you can conduct to mitigate the risks from them.

The Contingency Management Family

Contingency needs to be in place for all kinds of emergencies. Emergencies can be expressed on a continuum, ranging from incidents (which should be addressed by routine plans) at the one end of the scale to full-scale business crises at the other. Events which are specifically defined by the term "emergency" fall somewhere in the middle.

Management

Incidents develop Crisis engagement and into emergencies. special Business Continuity plans are invoked. Often. security staff play key roles.

An emergency may be defined as any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public image. The key elements of emergency management are preparing for, mitigating, responding to and recovering from an emergency (Source: US Federal Emergency Management Agency).

Consider to what extent you may play a role in the management of any of the following emergencies:

Theft or sabotage of mission critical equipment.

Site protest, blockade or site invasion.

Total failure of IT systems.

Power blackout.

Industrial disaster (e.g. Loss of containment).

Injury or death accident. Robbery.

Specific plans should exist in all organisations to manage emergencies. Where emergencies are not effectively and immediately managed, they can quickly develop into crises, which can have a long-term negative effect on the enterprise, damaging reputation and attracting unwanted media attention.

The Civil Contingencies Act 2004

In the UK the Civil Contingencies Act 2004 is designed to provide a management framework for civil emergencies, but it is unlikely to be something you can rely on in a site emergency. Your first point of contact will usually be the regular emergency services.

The Civil Contingencies Act 2004 is designed to provide the framework for response at local and national level to a wide range of scenarios, from attack by a foreign power to mass flooding. It may also be used when there is a mass strike event (such as coordinated fuel strikes) which threatens the functioning of the state. You can read in more detail about the act at http://www.cabinetoffice.gov.uk/content/civilcontingencies-act

Consider how you require staff to notify an emergency on site. Do you require them to notify you on a central emergency number? If so, that number must be attended 24 hours a day. Or should they report the emergency direct to the emergency services? You should ensure that the requirement is communicated to staff clearly so that there can be no misunderstanding. In an emergency, confusion over immediate reporting responsibilities can lead to delays, and possibly fatalities.

Natural Disasters

While the Civil Contingencies Act 2004 does address major natural disasters, you will need to develop emergency plans at site level for any natural disaster which may affect you as a business. In the UK, natural disasters may include (but are not limited to):

Floods, including sudden inundation by fast flowing water.

Hurricanes.

Landslides.

Lightening.

Wildfires.

Extreme cold, winter storms and isolation due to snow.

Extreme and prolonged heat.

The Cabinet Office doesn't publish detailed information about what to do in the event of a specific natural disaster, but there is generic information at this link http://www.cabinetoffice.gov.uk/ukresilience

The US Government has a good website with basic advice on specific natural disasters Notes http://www.ready.gov/natural-disasters.

You may also find advice on specific local authority websites, for example http://www.london.aov.uk/priorities/londonprepared/home and on the websites of specific organisations, for example http://www.redcross.org.uk/What-wedo/Preparing-for-disasters.

A useful publication that can be purchased is "How to Handle a Crisis" by Evers and Silva.

Emergency Management Planning

Emergency planning is cyclic, beginning with establishing a risk profile to help determine what should be the priorities for developing plans and ending with review and revision, which then restarts the whole cycle.

Revision

Emergency Plans

For certain sites, including major industrial hazard sites, there is a statutory requirement for emergency plans, which will be drawn up from a multi-agency response perspective. If not required by law, it makes good sense to draw up plans anyway. Emergency plans not only provide guidance on how to deal with emergencies but may also be used in defence if an allegation of negligence is made against the company in any inquiry following an emergency.

Emergency plans may take the form of generic plans - which set out the core response and recovery requirements to any emergency or specific plans dealing with hazards or sites. Often, the best solution is to have a generic emergency plan with emergency-specific annexes.

Advice in this regard from the UK Cabinet Office is as follows:

Specific Plans - Relate either to an emergency or kind of emergency, or to a specific site or location. Go beyond generic arrangements when they are likely to prove insufficient in a case. A specific plan usually relies on a generic plan or may be an annex of such.

Generic Plans - Core plans which enable the organisation to respond to and recover from a wide range of possible emergencies. Include procedures for ensuring the welfare of staff and the provision of sufficient resources for responding to the emergency.

Details in how to write an emergency plan, what it should contain, and templates can be found in: http ://www.cabinetoffice.gov.uk

The Emergency Management Plan must be a living document, which is designed to be tested, exercised and updated regularly. It is not a rigidly fixed rule book, and this will soon become apparent when an emergency occurs. The variables in any emergencies are almost immeasurable and so the flexibility of the plan must reflect this. Notes

The US FEMA Emergency Management Guide for Business and Industry identifies the following four key components of any emergency management plan:

1. Executive Summary.

2. Emergency Management Elements.

3. Emergency Response Procedures.

4. Support Documents.

Security Staff in Support of Emergency Management

It is likely that security staff will play a key role in any emergency, and so will need to be trained appropriately to do so. There should be means in the event of an emergency to quickly redeploy security staff to help with the emergency (access control, salvage, co-ordination, emergency procurement etc.).

Specifically, responsibilities placed on the security team may include:

Cordon and control.

Establishing and guarding alternate access points.

Protecting exposed assets.

Aiding the emergency services.

Interviewing witnesses.

Traffic control and parking.

Provision of communications. Maintaining event logs.

Emergency Management Centre

The needs and nature of the site will determine where the emergency management centre is located. Sometimes this is a dedicated facility. Other times it may be the boardroom. One method adopted by some companies is to have it co-located with the security control room. There are several advantages to this including shared infrastructure (much of which is common) and the ability to marshal emergency responding services.

The following are some of the key points:

It should be readily accessible but in a secure location to prevent unauthorised or unwanted entry and distractions. It should be sited away from high-risk areas.

It should be equipped with communications. It should be fully furnished. It should have access to catering, refreshment and toilet.

It should be regularly swept and scanned for listening devices.

It should be equipped with satellite TV and transistor radio for news.

It should have clear walls on which to mount maps, task boards, call out boards, location boards, status boards, contact numbers etc.

Mutual Aid Agreements

Mutual Aid Agreements (or associations) are agreements under which different organisations within a defined geographical area come to the aid of another organisation (or share resources) in the event of an emergency, such as fire, explosion, natural disaster, loss of containment etc.,

based on the assumption that an event could overwhelm on-site response resources. The arrangements usually focus on managing the emergency directly.

Emergency Response — Fires

Fires, whether accidental or deliberate, are by far the greatest cause of death and damage to buildings and facilities. On business premises fires are as likely to break out during working hours, when the facility is populated, as they are by night.

The Law - In many organisations security staff are looked to, officially or unofficially, as first responders in the event of a fire. The Regulatory Reform (Fire Safety) Order 2005 addresses fire prevention in non-domestic premises. Guidance, with which all security officers should be familiar, can be downloaded at:

http://www.communities.qov.uk/publications/fire/guidancel enforcement2005.

The Regulatory Reform (Fire Safety) Order 2005 stipulates the need to appoint a Responsible Person, who oversees site fire prevention. Normally this will be the employer, but this role will of course be delegated, sometimes to a member of the security team. In many cases, the prevention, detection and extinguishing of fires are a fundamental part of security duties. Security staff should receive regular refresher training on fire detection and response, including practical use of extinguishers.

The Regulatory Reform (Fire Safety) Order 2005 mandates that the responsible person is required to ensure a risk assessment is conducted and that relevant precautions are followed to ensure compliance with the Order and the safety of personnel. The main steps will be:

Identify potential fire hazards.

Decide who may be in danger.

Evaluate the risks.

Record the findings.

Review and revise when necessary.

Detailed guidance on the responsibilities required is contained within the link above.

To enact the requirements of the Order and to ensure rapid response and evacuation in the event of fire, it is a sensible precaution to nominate and train fire wardens from within the workforce. Fire wardens will be given the role of coordinating evacuation and ensuring that buildings are cleared in the event of fire. Such personnel should be clearly identifiable as fire wardens and be provided with colour-coded hard hats and/or tabards. They should also have clear and straightforward instructions and checklists

It is important to train your personnel properly for emergency management What would be the elements of an effective training plan?

Fire routine and evacuation drill procedure and management control.

Ensuring personnel know location of fire alarm points.

Ensuring that primary and secondary escape routes are used as appropriate.

The close procedure.

Assisting employees and visitors to nearest exits.

Fire Extinguishers - In the UK, there are six fire classes as follows:

Class A - organic solids such as paper and wood.

Class B - Flammable liquids.

Class C - Flammable gases.

Class D - Metals.

Class E - Electrical fires.

Class F - Cooking fat and oil.

Each class of fire has a fire extinguisher suited to it and each must be used for the correct class. The British Standard, BS 5306-3, specifies that all extinguishers should be painted red with a band or circle of a second colour covering at least 5% of the surface area of the extinguisher, indicating the contents.

It is critically important that the correct type of extinguisher is used for the appropriate fire — for example, the use of water extinguishers on an oil fire will cause severe injury to the extinguisher user. Also, a water-based extinguisher must not be used on a fire where electricity is present. Thus, the Notes chart shows that only Dry Powder or c02 extinguishers can be used when electricity is present.

Fire hose reels using water, fire blankets and buckets may also be available in the workplace. All users of fire extinguisher systems must be competent and trained in their use.

Fire Alarms - Fire alarm systems detect fires by monitoring changes associated with combustion. Such systems can be automatic, manually activated, or both. Systems can alert personnel and initiate evacuations, and call emergency services. Alarm systems consist of:

Initiators - Input to the fire alarm control unit and are either manually or automatically activated. These will include push buttons, pull levers or smoke and fire detectors.

Control unit (panel) - This component, the hub of the system monitors inputs and system integrity, controls outputs and relays information.

Power supply - (primary and back up).

Annunciator - The annunciator in most cases will be the alarm bell or klaxon, sometimes accompanied by flashing or strobe lights. Alarm systems can be linked to external monitoring systems and thus initiate a response.

Detectors - There are various types of fire detectors in use as follows:

Smoke detectors - These are used to detect the presence of smoke in a room or building either by photoelectric or ionisation methods, although some use both detection methods to increase sensitivity.

Heat detectors - Respond to changes in ambient temperature. If this rises above a predetermined threshold an alarm signal is triggered. Heat detectors are of two main types: rate-of-rise and fixed. Rate-of-rise detectors will react to sudden temperature changes from a baseline condition, whilst fixed detectors will activate once the temperature passes a certain threshold level.

Flame detectors — Use optical sensors, either infra-red, ultraviolet or video cameras to detect flames.

Sprinklers - A fire sprinkler system consists of a water supply and piping system, onto which fire sprinklers are connected. Each sprinkler head is held closed by either a heat-sensitive glass bulb, or a two-part metal link of fusible metal. The glass bulb or link applies pressure to a pipe cap which acts as a plug, which prevents water from flowing until the ambient temperature around the sprinkler reaches the activation temperature of the individual sprinkler head. Because each sprinkler activates independently when the predetermined heat level is reached, the number of sprinklers that operate is limited to only those near the fire, thereby maximising the available water pressure over the point of fire origin.

Emergency Response Loss of Containment

A loss of containment occurs where a volatile substance leaks into the atmosphere with the potential to harm employees or the surrounding neighbourhood. Harm may occur through explosion, fire, asphyxiation or poisoning.

Unmanaged, losses of containment may quickly escalate into civil emergencies and emergency services must be notified immediately for advice.

Emergency plans should envisage loss of containment events if volatile substances are used on site.

The emergency plan should determine whether and how to evacuate or invacuate. Prevailing wind should be taken into consideration as well as the properties of the substance, which may be heavier than air, render some emergency refuges unsafe.

There should be sufficient Personal Protective Equipment (PPE) readily available.

Emergency Response — Active Shooter

An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area. Fortunately, such events in the UK are rare, but there are, from time to time, occurrences.

Key points:

Events unfold unpredictably and require immediate law enforcement response.

The best advice to potential victims is that if there is an accessible escape path, get out, run and take cover. If not, find a place to hide and blockade the door with furniture.

' Hide behind large objects and silence mobile phones until emergency services respond.

Emergency Response -- Bomb Threats

Bomb threats can be delivered by various means, including email, but the most common is telephone.

Most of telephone bomb threats are hoaxes, and very few terrorist groups precede attacks with a threat call. But the minimum you should do is to notify the police immediately and carry out a search.

The Centre for Protection of National Infrastructure (CPNI), a UK Government lead body on providing anti-terrorism advice to businesses, provides useful information.

Emergency Response Bomb Explosions

The current threat assessment for the UK indicates that A will not precede a bomb attack with a warning. The first indication will probably be when a bomb detonates. Therefore, if you are in an elevated risk area or if your organisation is at specific risk, you should ensure that your emergency planning takes account of a no-warning explosion.

A bomb explosion is a scene of crime, but your primary concern must be rescue and immediate first aid. This requires training beforehand. At very least, you should consider training your security staff to the 3-day First Aid at Work Course.

Those evacuees not involved in administering first aid should be evacuated to a safe place, taking care to ensure they do not assemble near vehicles, which may contain secondary devices.

Envisage the possibility that the bomber may detonate at the security checkpoint; your contingency planning should take this into account.

Emergency management will be crucial, and bomb attack response should be a consideration when you exercise the emergency management plan.

Emergency Response — Robbery

The key emergency management elements of preparing for, mitigating, responding to and recovering are relevant in robberies and can be divided into proactive and reactive measures, which include (but are not limited to) the following:

Proactive

Reactive

Reducing targets.

Need to know.

Cash in transit services.

Time-locked and drop safes.

Second person present at risk times.

Enhanced physical security.

Bullet resistant glass.

Duress buttons.

Training for staff to include passive response and psychological survival strategies.

Cooperation with (no resistance to) robbers.

Keeping hands visible.

Memorising small details.

Locking doors when robbers leave.

Emergency Management

Elements

This section of the plan briefly describes the facility's approach to the core elements of emergency management, which are: e Direction and control

Communications

Life safety

- Property protection

Community outreach

- Recovery and restoration
- Administration and logistics

These elements, which are described in detail in Section 2 (of the FEMA guide), are the foundation for the emergency procedures that your facility will follow to protect personnel and equipment and resume operations.

Emergency Response

Procedures

The procedures spell out how the facility will respond to emergencies. Whenever possible, develop them as a series of checklists that can be quickly accessed by senior management, department heads, response personnel and employees. Determine what actions would be necessary to:

Protect employees, customers, visitors, equipment, vital records and other assets, particularly during the first three days to Get the business back up and running.

Specific procedures might be needed for any number of situations such as bomb threats or tornadoes, and for such functions as:

Warning employees and customers

Communicating with personnel and community responders

Conducting an evacuation and accounting for all persons in the facility

Managing response activities

Activating and operating an emergency operations centre Fighting fires

Shutting down operations

Protecting vital records

Restoring operations

Documents that could be needed in an emergency include:

Emergency call lists — lists (wallet size if possible) of all persons on and off site who would be involved in responding to an emergency, their responsibilities and their 24-hour telephone numbers.

Building and site maps that indicate:

Utility shutoffs

Water hydrants

Water main valves

Water lines

Gas main valves Gas lines

Electrical cut-offs

Electrical substations

Storm drains

Sewer lines

Location of each building (include name of building, street name and number) Floor plans

Alarm and enunciators

Fire extinguishers

Fire suppression systems

Exits

Stairways

Designated escape routes

Restricted areas

Hazardous materials (including cleaning supplies and chemicals) High-value items

Resource lists - lists of major resources (equipment, supplies, services) that could be needed in an emergency; mutual aid agreements with other companies and government agencies.

Private security and the law

Introduction

Security officers operate on behalf of the employer in exercising the latter's legal rights to protect his property against crime. Aside from this, they generally have no legal powers vested in them above and beyond those of a private citizen. It is therefore important that security officers have a good

understanding of the law and operate within it. Failure to operate within the law can cause liability exposures for the employing organisation and may lead to security officers being prosecuted.

Private Security and the Police - The Changing Relationship

Reasons for the changing relationship with the police include:

Increased terrorist threat.

Increased tasking of police. Increasing concerns over anti-social behaviour. Increased public use of shopping centres, arenas etc.

Better regulation, training and licensing within the security industry.

Many organisations provide a framework in which security operations can be professionally regulated and run and increased professionalism is giving the police and government increased confidence in the private sector's ability.

Skills for Security - This is the sector skills organisation for the security business sector, which has made significant progress in raising security officer standards to prepare them for changing tasking. Skills for Security works with employers and other stakeholders to deliver a range of educational and related services to improve skills, raise professionalism and increase business performance across the sector.

The Private Security Industry Authority

Security Industry Act came into being on the 1 1 May 2001. It regulates the industry and states that many of those working within it will need to be licensed to operate. The Security Industry Authority (SIA) is the regulating authority for the industry and carries out many functions, such as inspections of companies. The Private Security Industry Act 2001 is an enabling act. Licensing for security officers came into effect across England and Wales at the same time. It is now illegal to work in many areas as a security officer without an SIA licence. This applies to contract staff only.

The Inspectorate of the Security Industry (NSI) - This is an organisation that has the role of inspecting companies to industry standards such as BS 7499 and BS 7858. It is independent from any trade body and has no commercial interest. NSI enjoys active participation from the industry and involvement by the Police, Home Office, Ministry of Defence and the insurance industry. All NSI inspectors are independent of any commercial organisation to serve the best interests of the industry and its customers. NSI helps companies become more professional, to build stronger operations and to achieve wider recognition for their services. It assists clients by providing an informed choice of security provider with the backing of NSI registration. NSI is part of the new National Inspectorate of the Security Industry.

British Security Industry Association (BSIA) The British Security Industry Association (BSIA) is the major professional trade association for the security industry in the UK. The BSIA has over 550 members, who are responsible for more than 70% of security business undertaken in the UK market, including staffed security services, alarm systems, CCTV, physical security equipment, access control and transport.

Explain the linkage between your current operations and those of the police and describe your liaison activities.

Security Officer Powers

Security officers generally have no legal powers vested in them above and beyond those of a private citizen. When used in public space (or perceived public space, such as shopping malls), security staff may take on an order maintenance role. In public space, especially trouble spots, this may be in a collaborative partnership with the police, where, occasionally, the police service may formally confer upon named private security officers limited powers beyond those normally available to a private citizen.

You must ensure that you and any security staff working for you are fully aware of their limitations as far as legal issues are concerned. Inappropriate or unauthorised actions carried out by any member of staff could result in difficulties ranging from mild embarrassment for your organisation to major and damaging reputation issues caused by litigation against you and your staff.

Security Officer Powers of Arrest

Your powers of arrest are usually the same as those conferred to any private citizen, which means that you may arrest only if you are totally confident that an indictable offence has been committed. Indictable offences are those triable at a Crown Court, and include (but are not limited to):

Murder and manslaughter.

Serious assault.

Criminal damage.

Theft, robbery, burglary and fraud.

Possessing an offensive weapon.

Going equipped to steal.

Aggravated vehicle taking.

Indecent exposure.

Causing death by dangerous driving.

Before acting, it is important to be sure in your mind that an offence has been committed. There are two fundamental concepts in English Law that must be satisfied for an act to be considered a crime:

Mens rea is the legal term used to describe the element of a criminal offence that relates to the defendant's mental state. Different crimes have different mentes reae: some require intention, others recklessness, negligence, or knowledge. Some crimes do not require proof of any mental state of the defendant.

There is a cardinal rule that acts alone cannot amount to a crime unless they are accompanied by the Mens rea element. This means showing that the defendant had the required state of mind at the required time. The state of mind must relate to the offence in question.

But there are exceptions. For example, various road traffic violations such as driving with excess alcohol, and possession of weapons such as CS gas canisters are considered offences of strict liability, and the state of mind of the defendant is less relevant.

If you are in a role where you may be required to exercise powers of arrest (such as in a retail environment) you must be confident in your knowledge of which offences are indictable and which you cannot arrest for. If you make a mistake, you could find yourself on the wrong side of the law. The best desktop reference source in this regard is Blackstone's Police Manual, which lists almost every conceivable criminal offence. In many circumstances, however, your employer will advise you not to formally arrest, but seek to detain with consent. This is especially the case with business and industrial premises.

An important difference between your rights as a private citizen and those of a police officer is that you cannot arrest on the grounds of mere suspicion. Only a police officer may do this. You must be able to demonstrate reasonable grounds for suspecting that an indictable offence has been committed. Specifically, the Police and Criminal Evidence Act (PACE) Section 24A states:

1. A person other than a constable may arrest without a warrant -

a. Anyone who is in the act of committing an indictable offence;

b. Anyone whom he has reasonable grounds for suspecting to be committing an indictable offence.

2. Where an indictable offence has been committed, a person other than a constable may arrest without a warrant -

a. Anyone who is guilty of the offence;

b. Anyone whom he has reasonable grounds for suspecting to be guilty of it.

3. But the power of summary arrest conferred by subsection (1) or (2) is exercised only if a. The person making the arrest has reasonable grounds for believing that for any of the reasons mentioned in subsection (4) it is necessary to arrest the person in question; and

b. It appears to the person making the arrest that it is not reasonably practicable for a constable to make it instead.

4. The reasons are to prevent the person in question -

a. Causing physical injury to himself or any other person;

b. Suffering physical injury;

c. Causing loss of or damage to property; or

d. Making off before a constable can assume responsibility for him.

Blackstone's publishes a practical guide to PACE,

Exercising Powers of Arrest and the Use of Force

Section 3 of the Criminal Law Act 1967 and common law (for self-defence) allows you to use only reasonable force in effecting an arrest. In practice, this means minimum. Disproportionate force, especially if it results in injury to the detained person, may render you liable to charges of assault. Upon arrest you must tell the person why they have been arrested and administer the caution:

You do not have to say anything, but it may harm your defence if you do not mention, when questioned, something which you later rely on in court. Anything you do say may be given in evidence.

On arrest you must tell the person the reason for the arrest, but you are not required to cite the Act or Section which has been broken.

Procedure after Arrest

Once you have administered the caution you may not question the person further (as this could be a violation of PACE) and you must call the police immediately. If you want to question the person, this must be done before any arrest is made, but the person can exercise the right to remain silent at any time during or after apprehension. The responding police officer can question.

Arrest and detention brings with it many problems. For example, there may be underlying health problems that you are not aware of and which may be exacerbated by the arrest.

At the very least you should ensure the person is comfortable, not put under any form or duress and is accompanied by somebody of the same sex, and that you remain vigilant to attempts to dispose of evidence, especially in the toilet, to which the person must be accompanied by somebody of the same sex. You must also be vigilant to attempts by the person to harm themselves or other persons.

Statement Writing

Whenever you respond to any offence you should always make a record of that response. Depending on the circumstances it may be any one-off, or a combination of, the following:

- Notes in your pocket book.

' An entry in the incident database.

' An entry in the occurrence book.

- A full written statement.

In cases where you intend to hand over a perpetrator to the police, the police will need to take a statement from you. It has become good practice for security officers to write this immediately after handing over the perpetrator to the police. This can then be collected later by a police officer, and obviates the time-consuming

What does PACE stand for?

task of the police officer having to sit down with you while he writes your statement. You should liaise proactively with your local police force to establish their policy on this and the format in which they would like statements to be written.

Children and Arrest

Children are responsible for a lot of trespass onto, and criminal damage, against, property. An offence of criminal damage may constitute burglary and may thus be an indictable (arrestable) offence.

Children under 10 cannot be arrested or charged with a crime as they are below the age of criminal responsibility. Children aged 10-17 can be arrested and taken to court if they commit a crime, but you should clarify with your legal department your policy on dealing with child offenders. It is very easy to find yourself on the wrong side of the law if you detain a child incorrectly or use unnecessary force.

Trespass

Trespass is one of the activities which often face private security personnel during their everyday duties. The fact is that trespass happens on many sites routinely and can be accidental as well as intentional. The trespasser should be asked to leave the site and given reasonable time to leave peacefully. Common law allows you to use reasonable force, but this should be as a last resort as force often begets force. Persuasion is the best tactic in the short term.

Signs such as "trespassers will be prosecuted" are misleading. In most cases trespassers cannot be prosecuted or detained, merely evicted. However, if you have reasonable grounds for believing that the trespass is in connection with burglary, you may be able to execute an arrest, but you have no rights under law to search the suspect.

The police will only become involved in serious incidents. This is often the case when squatting or other passive trespass is carried out. The police will only apply criminal arrest measures when either criminal damage has been committed during entry onto a site or in the case of disruptive or violent activity.

More important, and of relevance to the private security industry, is the fact that although a business or landowner can use reasonable force to prevent a person from gaining access to their property, there are constraints which must be considered if the owner is to avoid prosecution themselves.

If the owner uses force against trespassers or even forces access to their own property and someone inside is opposed to it, this can result in prosecution under the Criminal Law Act 1977.

Violence or threats of violence towards trespassers can result in similar prosecutions. What constitutes 'reasonable force' is open to interpretation and of course violence can escalate once force is used. This can result in difficulty for the private security officer.

'Squatters' have certain rights which are protected by law and private security and the organisations for which they work must be very careful to avoid situations where confrontations and violence may take place.

Theft

One of the most common problems you will encounter is theft. Theft includes robbery and burglary and is dealt with under The Theft Act 1968. All forms of theft are indictable offences. Fraud is also indictable but is dealt with under The Fraud Act 2006.

To prove an offence of regular theft you should establish the dishonest intention to permanently deprive. Information theft is not usually covered by the act. Intention is sometimes difficult to prove. For example, in a retail environment arrest should only be considered if the suspect has passed all points of payment and has been stopped outside or leaving the store.

Burglary is a little different. You only must be satisfied of the ulterior intent of a trespasser.

What is the difference between burglary, theft and fraud?

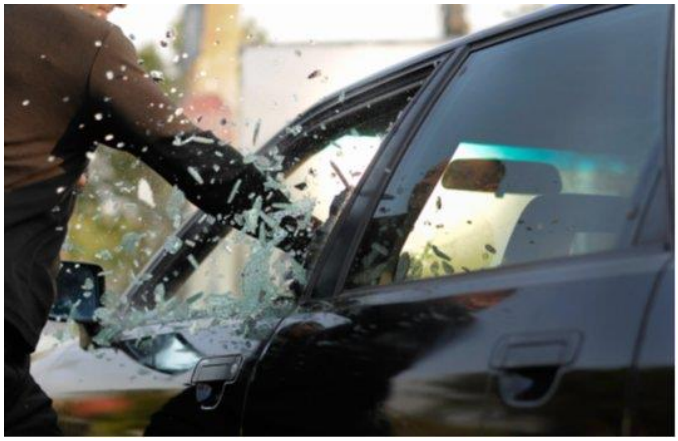
Likewise, the offence of robbery is complete when the assailant threatens the use of violence during an attempted theft. For in-depth information on The Theft Act 1968 you should consult Blackstone's.

Criminal Damage

Another typical crime encountered by the security officer is criminal damage. Under the Criminal Damage Act 1971, persons can be considered liable if they damage property 'without lawful excuse'. You should exercise great caution if you are considering arresting for criminal damage. While, strictly speaking, criminal damage is an "either way" offence, acts of criminal damage that are less than 25,000 are dealt with summarily under a lesser offence, for which you may not arrest. In practice, what this means is that if you catch somebody spraying graffiti on your wall it is not an indictable (arrestable) offence but a summary offence, but if they take a sledgehammer and badly smash up several vehicles on a car park it may become arrestable.

Substance Abuse and Arrest

If you encounter somebody under the influence of alcohol or illegal drugs, it is likely that you will be required to act (remove from harm's way or escort off premises), but the person should not normally be arrested unless another (indictable or either-way) offence is being, or has been, committed. This may include an offence under the Misuse of Drugs Act such as possession or intent to supply illegal drugs.



Other Laws Which May Affect You

There are implications for monitoring or recording the activities of personnel (employees, guests, customers, visitors or even suspected adversaries) within and around the workplace. There is a series of laws which protect the rights of individuals and limit the powers of organisations, be they public or private, to conduct activities which impinge upon privacy. The police and government agencies are empowered, under certain legal constraints, to conduct monitoring of mail, electronic communications and storage systems, telecommunications and activities. They may conduct physical or technological surveillance including entry into premises, bugging, eavesdropping and the use of surveillance officers either on foot or in vehicles with photographic and recording equipment. Also, they can use CCTV and associated national network systems for surveillance and investigatory purposes. These activities are based on the need to prevent terrorist activity, for example. However, you must be aware that these activities are carefully regulated and justified by the law. The police and government agencies are accountable for their actions under law.

Regulation of Investigatory Powers Act (RIPE) 2000 covers monitoring of telecommunications and IT systems as well as the conduct of surveillance. The Act was designed to provide regulation of police and intelligence agencies and clearly defines the legality or otherwise of such actions. Monitoring of telecommunications and IT systems is legal under this Act only if the system is private and all communicating parties have consented to such monitoring.

Data Protection Act 1998 stipulates that the processing of personal information must comply with eight principles of good information handling. The eight principles state that the data must be:

Fairly and lawfully processed.

Processed for limited purposes.

Adequate, relevant and not excessive.

Accurate and up to date.

Not kept longer than necessary. Processed in accordance with the individual's rights.

Secure.

Not transferred to countries outside the European Economic area, unless there is adequate protection.

The implications of this Act for all organisations and departments (not only security), are far reaching and include not only written information but CCTV and audio recordings, photographs, electronic files and records of activities such as transactions. Because the retention of such

Think about all the areas of legislation with which you need to be cognisant

records can be judged to be an infringement of an individual's human rights; the Act requires that a 'data controller' be appointed for organisations which use such data to ensure that the principles are followed, and that the organisation operates within the law.

Human Rights Act 1998 gives legal effect in the UK to certain fundamental rights and freedoms contained in the European Convention on Human Rights (ECHR). It was enacted to ensure that public authorities comply with the Act (and therefore with the European Convention on Human Rights). "Public authority" means every person or body carrying out a public function, including private bodies such as companies that supply electricity to members of the public. The Act protects the following rights of individuals:

The right to life.

The right not to be tortured or inhumanly or degradingly treated or punished. The right not to be required to perform forced labour.

The right to liberty and security of the person.

The right to a fair trial.

The right not to be punished for something which was not a crime at the time it occurred.

The right to respect for one's private and family life, correspondence and home.

The right to freedom of thought, conscience and religion.

The right to freedom of expression, freedom to hold opinions and freedom to receive and impart information.

The right to freedom of peaceful assembly and freedom of association with others.

The right to marry and found a family.

The right not to have Convention rights secured in a discriminatory way.

The right to peaceful enjoyment of one's possessions.

The right to education.

The right to free and secret elections at reasonable intervals.

Although some of the rights listed under the HRA may not at first seem directly relevant to your workplace, it is incumbent upon you as an employer to ensure that you do not contravene the requirements of the Act in your working conditions Notes or the imposition of any unreasonable and unlawful restrictions on your personnel. The Human Rights Act, along with the Data Protection Act protects privacy and personal freedoms and recent years have seen many employers prosecuted for contravening them. If you are in any doubt about your company or organisation's adherence or compliance with these Acts, you must consult legal advice.

Scottish Law

The law in Scotland is different from that of the rest of the UK and if you have responsibility for the management of security personnel who are required to operate under Scottish Law, you must ensure that they understand its specific requirements.

As in English Law, a uniformed security officer has no specific powers of arrest. In Scotland a major difference from English Law is that as far as evidence is concerned, two eye witnesses are required to corroborate that a (criminal) act may have taken place. Therefore, that evidence (known as 'best evidence') needs to exist before any arrest can be made.

As previously stated, the aim of this unit is not to provide detailed breakdowns of the various laws and regulations in force in Scotland and the rest of the UK. It is important, however to ensure that there is clear guidance available and accurately compiled based upon the relevant legislation. The onus is very much placed upon the security manager and the security department in ensuring that they are compliant.

Evidence - Introduction

Evidence is crucial to establishing whether somebody has committed an act of misconduct or a crime, and in eliminating possible suspects. Physical evidence often indicates that a crime has taken

place, proving the actus reus element of the crime, while non-physical evidence (e.g. witness statements) often establishes the mens rea intention element.

Physical evidence can be anything associated with the crime scene but may also be tools and contraband later discovered because of a search. CCTV and access control information may also be regarded as physical evidence. Physical evidence should be secured as soon as possible after the crime.

Physical Evidence at the Scene of an Incident

When an incident or event is reported or discovered there will always be evidence of some sort either in or around the scene. Physical evidence will need to be preserved and perhaps recorded so that it can be used in subsequent investigations or, if necessary, prosecutions. The types of evidence that will be in and around the scene could include many examples, such as:

Fingerprints	Documents
Tool marks	Fluids
Tyre prints	Chemical traces
Footprints	Disturbance
Bullet cases	Broken glass
Bullets	Fire damage
Handwriting	Soil
Cosmetics	DNA
Bodies	Fibres
Deliberate evidence	Physical position
Animal hairs	of objects
Printers and	Items found at the scene
Photocopiers	Hairs
Blood	

Not only is physical evidence important but it must be supported by the additional information that can be collated in relation to the site and incident.

This will include:

Witness statements - Who can provide direct evidence about what may have happened. The witness may not have seen the incident directly but may have experienced something which may contribute to the information collation process.

Sketches and photographs - There will be cases where evidence may deteriorate or need to be removed (for example, in an emergency). If possible, sketches and photographs should be used to record the site as accurately as possible.

Recordings and data - CCTV recordings will be crucial in some cases and have led to prosecutions on many occasions. Remember also that in the case of computer and data theft the evidence may be electronic, and you will need to liaise with your technological experts to capture relevant information.

Observations of processes and controls - It is always worthwhile examining the processes and controls in and around a site to determine whether they have made the incident or crime possible. Look at the security department and general security awareness and compliance. Also, in the cases of fraud and IT data loss or misuse, you will need to examine financial records and IT data.

Crime facilitators and tools Some areas, such as those with construction going on, often have an abundance of facilitators and tools available for the enterprising adversary. Scaffolding around buildings and builder's tools are obvious cases. In the case of fraud and IT, facilitators may include the ease with which funds can be accessed and an over-reliance on personnel placed in a position of trust.

Expert witnesses in examining and presenting evidence, the opinion of expert

What questions would you ask a witness that has seen a crime being committed?

witnesses, who understand and are qualified in appropriate aspects of an incident, will be required to be consulted.

Suspect statements - In any case, it will be necessary to speak to 'suspects'. They will need to be interviewed but be aware that in the case of an indictable offence, the police will be required to take statements. Therefore, you should be very careful and always ensure that the police are involved as early as possible if the incident is sufficiently serious.

Scene of Crime Processing

When arriving at a scene of crime, the first action you should undertake is to "stop all action" to give yourself some time to work out where the key evidence is and develop a hypothesis as to what has happened. After assessment determine whether to call the police. If this is the case, seal the crime scene until they arrive. If no police involvement is required determine what evidence is within your ability to process.

You should photograph and sketch the scene noting the locations of any items of evidence. Some evidence you may be able to collect (broken items) but some evidence may be critical to the business (tools).

When collecting evidence, consider whether you can process it. Collected evidence must be subject to strict chain of custody procedures:

Document.

Photograph.

Register.

Secure.

Limit access.

Record every access or handling.

Remember, if you are going to call the police leave evidence collection to them.

Evidence should be marked at the time of collection, with these basic principles in mind:

Cross reference to sketch of crime scene.

Marking must not deface object. If in doubt, use a tag or a labelled evidence bag. Describe and give examples of the following:

If too small to mark (glass fragments), put in sealed container and mark.

Photograph (or if paper, photocopy)

Evidence and the Courts

As a security officer you may be required to give evidence in court. The legal system in the UK views evidence in a very specific way.

Direct Circumstantial Hearsay

Direct physical Other, non-direct When a witness evidence, or what an evidence connected cannot give direct witness saw, heard with the fact to be evidence of a fact. proved Also, when a document cannot be 2nd Best produced by the person who wrote it;

Circumstantial evidence

It is important to note that any documents or exhibits in connection with the offence become disclosable and often admissible. This includes scribbled notes in a notepad. The following basic rules apply to notepads:

Number pages.

Cross out mistakes, but never obliterate. Never remove pages.

When called to give evidence in court, before you take the stand you should ask to see a copy of any statement you made to a police officer. This is important as you will not be allowed into the court-room other than to give evidence. When giving evidence, if unavoidable, you may refer to notes that you made contemporaneously with the case, if you ask the court's permission each time. You will make a stronger impression, however, if you are not overly reliant on notes.

Address High Court judge as "My Lord", a crown court judge as "Your Honour", a magistrate as "Your Worship" and a coroner as "Sir".

You should attend Court in uniform, if your employer permits. Clothing and personal appearance should be to the highest possible standard. Inappropriate or flawed appearance will have an adverse effect on the opinion of court officials and jurors and should be avoided:

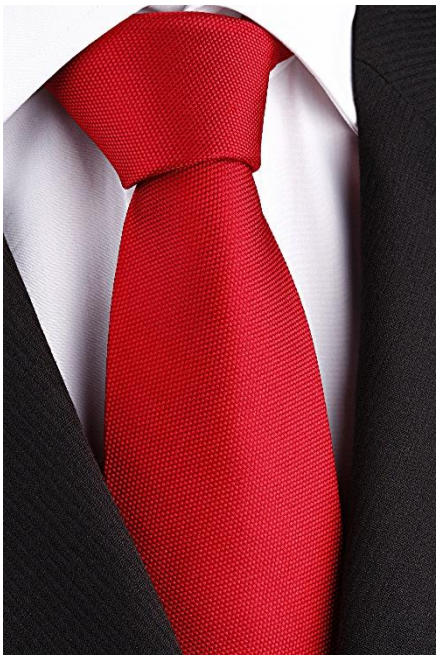
If in uniform, dress like a professional as you are representing your organisation. Dress conservatively and, when appropriate, wear good quality clothing. Avoid wearing loud colours, comedy ties and extremes of fashion. Always be neat and clean.

Avoid wearing tinted or dark coloured spectacles.

Wear only functional jewellery (wedding ring and wrist watch).

Avoid wearing items that may identify a personal association or belief such as political badges or club ties.

Your demeanour and behaviour will be of the utmost importance:



Avoid being perceived as aggressive, officious, argumentative, bored or defensive.

Do not fidget with items on your person that "jingle" (coins, keys, earrings). Never chew gum. It interferes with clear speech and appears disrespectful.

When not using your hands to gesture, keep them folded in your lap while seated in the witness stand.

Do not speak to any witnesses or the jury panel during the trial or its recesses; it will destroy the witness's credibility. When testifying, speak to the jury panel, they are your audience.

Be polite to the legal representatives on both sides of the case. Show respect to all the courtroom officials.

Be particularly attentive when the judge is speaking. Listen to what they are saying and be prepared to respond, if necessary. When addressing the Court staff, use their respective titles.

Computer Scene of Crime Processing

Upon being called to a computer scene of crime, best practice is to leave the computer switched on, don't browse any folders, don't close any programs and call in IT expertise.

Computer evidence can be easily corrupted, and clumsy handling may allow the perpetrator to go free.

Questioned Document Evidence

Private forensics companies can offer the following services:

Linking handwriting to a suspect with a percentage certainty value.

Proving or disproving the authenticity of a signature with a percentage certainty value.

Possibly linking a document to a printer, or at least a printer cartridge. Possibly linking a document to a photocopier.

Such services are expensive but may be considered if the crime is sufficiently severe. Malicious letters, for example, may not be processable immediately, but should always be kept for a long period under strict chain of custody, as they could be relevant in the future if a suspect is identified.

Violence Scene of Crime Processing

In any act of violence in the workplace, the overriding concern must be protection of people, treatment of wounded, and neutralisation of the aggressor. In such circumstances, scene of crime and evidence preservation take second place to personal safety. The same rule applies for workplace accidents and hazardous situations.

Write a checklist for security officers to follow when handling computers at the scene of the crime.

Securing CCTV Evidence

The Information Commissioner states that "recorded material should be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the material can be used as evidence in court. To do this you need to carefully choose the medium on which the images are stored, and then ensure that access is restricted. You may wish to keep a record of how the images are handled if they are likely to be used as evidence in court. Finally, once there is no reason to retain the recorded images, they should be deleted. Exactly when you decide to do this will depend on the purpose for using CCTV".

Equality and Diversity

Introduction

Notes

Security officers are very often the public face of an organisation and the first point of contact for customers and members of the public when they enter a site or building. Also, security officers and departments rely upon teamwork and cooperation to conduct their business successfully and efficiently. In the modern workplace, it is important that the security department and all its personnel can operate in a fair and non-discriminatory manner to work efficiently and fairly.

In the UK, there is a governing and regulatory structure in place to ensure that discrimination in the workplace is limited and to ensure that equal opportunities are provided and applied for all within the workplace and any customers, visitors or other stakeholders who may interface with a business or organisation.

This unit will provide you with an overview of the regulation and legislation in place, and to allow you to understand the specific requirements and applications of discrimination and equal opportunities in the workplace. The unit will also allow you to address management strategies for the application of law and regulation.

The Need for Equality

It is an unfortunate fact that in modern society, many people are discriminated against daily. In addition to this, and often because of it, some people are also harassed or bullied in the workplace. Clearly, this does not provide for a harmonious and efficient working environment and can have serious consequences for those on the receiving end. It is a basic human right to be treated with respect and to be afforded a degree of dignity — and the application of discrimination or harassment affects that human right. Therefore, the aim of the security manager should be to apply robust management processes to protect those at risk.

What is Discrimination?

In legal terms, discrimination is defined as being treated 'less favourably' than another person in the same situation. There are many 'reasons' for an individual or group of people being targeted but some examples are as follows:

Because of their age.

Because of their gender.

Because of their sexual orientation.

Because of their appearance.

Because of their personality or character.

Because of their race or origin. Because of their skin colour.

Sadly, the range of motivations for discrimination is as wide as the number of people in the workplace. Every person is conditioned with their own set of preconceptions, prejudices and personal preferences. All these factors can be compounded and magnified by a group or 'pack' mentality in cases of bullying, harassment or discrimination.

The 'reasons' for discrimination are only one component of the whole issue, the types of discrimination are almost unlimited, and we will all have seen or experienced examples of discrimination at some time in our lives. In the workplace, because there is usually a mix of differing races, cultures, educational standards, sexes, personal interests and so on, there are a unique range of possibilities for discrimination to take place. Some examples of discrimination are less obvious than others, but the following give some indication of the potential scale of the problem in any workplace:

Scenario 1: In an office environment, a person is excluded from conversations, discussions and social activities deliberately by colleagues. This can take the form of simply not telling the victim when such activities are taking place or by stopping conversations or group discussions when the individual approaches or tries to join in. This form of exclusion can be extremely demoralising and distressing, especially if the victim is the only one in the workplace to be treated in this way.

Scenario 2: Within a security department, the manager targets an individual. This can take the form of personal, insulting or disparaging comments, or even deliberately blocking opportunities for personal and professional development and advancement. The clear effect of this can be the inability

for the victim to gain promotions and rewards to increase their earning ability and worth in the workplace.

Scenario 3: A female working in an all-male environment (or conversely a male working in an all-female environment) is repeatedly targeted by colleagues who make sexual comments or who carry out physical harassment. This type of behaviour can also be manifested in actions such as leaving lewd messages on computer systems or introducing pornographic and similar images into the individual's workspace.

Scenario 4: An individual is prevented from practising or following their religion or beliefs in the workplace. This can range from ridiculing the individual's beliefs, to not permitting them to worship at prescribed times or in specific locations. Also, there have been many occasions where individuals have been prevented from wearing clothing or accoutrements specifically required by their religion or belief system.

To make it clear what each term means, the following definitions will be helpful. These are the legal terms for categories of discrimination:

Direct Discrimination - Is where a decision or action is taken on the grounds of an individual's characteristics. A classic example of this is the selection of an individual for employment over another individual, who may be as well or better qualified but is of a different gender or race.

Indirect Discrimination Is often more difficult to identify but is of the type where there are rules or conditions, policies or practices at work that apply to everyone but cause disadvantage to one group of people more than others without good reason. An example here would be a company which specifies a qualification in English where it is

Conduct a survey of your site and its infrastructure and assess those areas which can be improved or changed to provide increased accessibility or ease of use for the less able

not strictly necessary, and thus discriminates against immigrants whose command of the language may not be fluent.

Harassment - This is defined as a person's unwanted conduct which violates another's dignity or creates an intimidating, hostile, degrading, humiliating or offensive environment. Scenario 3 above gives an example of such conduct.

Victimisation - This is where a person is treated less favourably because they have threatened to bring proceedings, give evidence or make a genuine allegation of discrimination.

Discrimination can also extend beyond an individual's current employment, if for example an employer gives an untrue or discriminatory reference to a person's potentially new employer or takes some other action which may unfairly prejudice their application for employment.

What is Management's Responsibilities?

Clearly, there can be many types of discrimination and victimisation and these are simple examples. It is important for you to not only be able to recognise such behaviour but to be able to rectify and eliminate it. Indeed, in law, you and your employer could be penalised if you fail to act in this way. You must ensure that you apply the requirements of regulation and law within the workplace and that your personnel fully understand and apply the standards that are required of them. Discrimination is unlawful, and you should ensure that you are fully prepared to deal with it in all its guises.

Legislation

An understanding of the following acts will assist in understanding the range of legislation that is provided to prevent discrimination in the work place.

The Equality Act 2010

The primary source of legislation which has now codified the previous array of anti-discrimination

laws are: The Equality Act 2010. It replaces several earlier acts which included (but was not limited to) the following:

The Sex Discrimination Act 1975.

The Race Relations Act 1976

The Disability Discrimination Act 2005

Equal Pay Act 1970

You cannot in fairness be expected to know the full content of The Equality Act, but you should be aware of your general responsibilities and what are the actions required of you. All the following are relevant to discrimination issues:

Direct sex discrimination, such as when a man is favoured over a woman (or vice-versa) or a nonmarried person is treated more favourably than a married person. In short, the test of discrimination is whether an individual would have been treated the same as others had their sex or marital status been the same as theirs. The Act also includes the fact that pregnancy cannot be used to discriminate against women who are on maternity leave; meaning that it may be discriminatory to exclude them from information concerning pay and promotions etc. in which they have a legitimate interest.

Indirect discrimination under the Act will encompass activities that may be more difficult to see. This may include such instances as work hours which would not allow women (who tend to be primary child-carers) to look after their children properly.

The Act also provides for equality in advertising for recruitment, recruitment itself and the activities that an employee is required to carry out. However, there are exceptions and concessions for certain types of employment where a gender specific role is necessary for example, on the grounds of decency or privacy.

Discrimination, victimisation or harassment can take various forms but clearly, nobody should be treated less favourably than anyone else because of their ethnic origin, race, nationality or colour.

Direct disability discrimination involves the act of treating someone less favourably than another who does not have that disability. Also, under this Act, disability discrimination can happen when an employer does not make reasonable adjustments to ensure that disabled people are not disadvantaged. Examples of such adjustments will include the provision of fittings in buildings such as ramps or of specialist office furniture.

Employment equality must be maintained despite any trait or belief held by employees. This means that employees cannot be discriminated against or treated less favourably than others under the specific regulations above. The regulations cover direct and indirect discrimination as well as harassment and victimisation.

The Human Rights Act 1998.

This Act is quite wide-ranging as it requires UK law to be compatible with the European Convention on Human Rights. As such, the Act enshrines various rights including the right of religious belief, privacy and life. Under these broader headings there are various other rights which can be claimed by complainants or victims.

To most people, this array of laws and regulations can be intimidating and confusing and there are often cases where managers advise against any actions which they fear will contravene them. Whilst it is a requirement to conform with the law and regulation, and your organisation's responsibility, you must ensure that you can conduct security operations properly within their framework.

Managing Discrimination in the Workplace

Most large organisations have policies or procedures in place. These are designed to protect their staff, employees and visitors from discrimination, victimisation and harassment and which has been produced by legal departments in accordance with the regulations and acts listed above. Of course, all personnel will need to be familiar with such company procedures and regulations. If your company does not have a legal department or an appropriate policy in place, it should be considered as a matter of urgency. Notes

However, the most detailed procedures will be useless if they are neither understood nor implemented by the workforce. If you were the person responsible for your workforce, there must follow a responsibility placed upon you to ensure that compliance is embedded throughout the workforce. In fact, if you do not ensure compliance and manage the issue, you could find that you are subject to prosecution or sanction.

Therefore, you should ensure that you not only explain the standards of behaviour required of your personnel at all levels but also that you monitor and enforce such standards always. The following are some areas on which you should concentrate to ensure compliance and to avoid discriminatory practices:

Know the Law - The rules and regulations listed above are easily available and there are various sources from which you can obtain information about them. You must know what constitutes discrimination, victimisation and harassment and what you are required to do by law. The Equality and Human Rights Commission provides plentiful and detailed guidance on the law and how it affects the workplace.

Know your Workforce - Your workforce will be made up of people from varied backgrounds, each with their own beliefs. It is most important that you understand that the views, beliefs, background and tensions amongst your staff will affect the way that they work together and deal with their customers. You must be aware of any potential incidences of discrimination and you should encourage a culture of tolerance of diversity. You should also ensure that there is a clear procedure for reporting and highlighting incidences of discrimination.

Policy and Action Plan - You should ensure that you have in place a policy for Equal Opportunities which clearly states your organisation's position on this matter and which is signed off at the highest level.

To back up the policy there should also be an Action Plan which, according to the Equality and Human Rights Commission will provide clear direction on the following:

What will be done to achieve the goals laid down in the policy?

Which senior person is responsible for each action — this is important as accountability will contribute greatly to achieving goals? Deadlines and targets for achieving the goals — again, setting deadlines and targets provide not only timescales and required standards but also ensure a degree of accountability. How breaches of the policy will be tackled and rectified?

How success or failure will be measured?

How, and how often, progress will be reviewed?

Increase Awareness Most cases of discrimination in the workplace are due not only to ingrained intolerance but also to a lack of understanding of the cultures, beliefs and orientations of individuals and groups of people. Such deficiencies can be overcome by a programme of increasing awareness throughout the workforce. You should encourage staff to understand other cultures and beliefs through a programme of workshops and training for supervisors and managers to ensure that they can combat discrimination. There should also be clear guidance given to the workforce about the effects of intolerance and the penalties which may face them if they contravene the law.

Act - You need to ensure that in the event of any discrimination taking place in the workplace that you take appropriate action. This action must be commensurate with the problems that arise in the workplace and can range from informal interviewing to resolve conflicts, to a full and formal disciplinary process should the need arise. You must also ensure that you record in writing any incidents and ensure that such records are available for further action or scrutiny if required. Reporting must be timely, and it is important to ensure that your staff know what type of action they can expect to have taken on their behalf, or against them and the timescales for resolution.

Because such actions require your staff to confront their own prejudices and to modify their behaviour, you should be prepared to meet resistance and sometimes hostility. It is essential that you overcome such resistance and that you do all that is within your power to confront and manage change in perceptions and behaviour. You should also actively support victims of discrimination and ensure that the systems that your organisation has in place to comply with the law and regulation, are orientated towards providing such support.

Regulatory Bodies

The Equality and Human Rights Commission, is the UK's regulatory body responsible for protecting the rights of individuals and groups against discrimination, victimisation and harassment. It has extensive legal powers and acts to enforce legislation and to support victims within the workplace and in society at large.

The Commission formed in 2007, incorporates the previous Equal Opportunities Commission, Commission for Racial Equality, and the Disability Rights Commission. It has also taken responsibility for the other aspects of equality: age, sexual orientation and religion or belief, as well as human rights. Therefore, the Equality and Human Rights Commission is the authoritative source of regulation and guidance for this subject and related issues.

Having identified the targets and the types of potential discrimination, write an outline plan of action for dealing with the problem in your workplace Once completed, compare it with your organisation's current plan and describe improvements which could be made.

References

The link below will take you to the Office of Public Sector Information's 1.1K Statute Law Database, which will allow you to access and view the legislation covered in this unit. It is recommended that you look at these pieces of legislation and if you have not addressed the legal implications of your security department's operations, that you do so as soon as possible: http://www.legislation.gov.uk/

The changing nature of the law within the UK makes it very difficult to provide reliable and detailed guidance on the law within this unit. It is therefore recommended that if you wish or need to find accurate guidance you should also seek out the following reference books, available from online retailers:

Blackstone's Police Manual: Crime

Blackstone's Police Manual: Evidence and Procedure

Blackstone's Police Manual Volume 4: General

Police Duties

Employment Law - Deborah J Lockton

Workplace Law Handbook (www.workplacelaw.net)

All these references are regularly updated (usually annually) reflecting the changes in law.

You should note that legislation is often updated and therefore accessing this information should not be a 'one-off' activity you must remain aware of any potential changes to the legal framework within which you operate.

Conclusion

The law is complicated, but the responsibilities of the police and of citizens are clearly defined. Although the legal constraints that do apply are enshrined in law, the role of private security and of the police has become less defined, particularly in some of the roles that the police have moved away from. The roles of police and private security are complementary, in that whilst the police concentrate on offences and offenders, private security practitioners are more orientated toward protecting assets from loss.

The legal constraints that are placed upon private security are no different to those placed on other citizens. However, private security officers will sometimes find themselves in situations where they are required to respond but must tailor that response to legal requirements. Private security officers need to act reasonably, and to be aware of the circumstances surrounding an incident to which they are required to respond. Also, they need to understand the law and the implications and liabilities concerned with contravening the law.

Investigations, either by the police, or managed by private security managers, need to be conducted correctly and sequenced effectively. The management of the whole process needs to be meticulous and accurate. Evidence must be secured, documented correctly and preserved, in order that it may be presented in an appropriate manner either in an investigation report or as court evidence. Investigation, evidence collection and marking are a specialist skill and although you may not be directly involved you may well be required to oversee the process. Therefore, it is incumbent upon you to at least familiarise yourself with the outline processes. It is usually most beneficial for an investigation to be conducted by a consultant or contractor who will have a full grasp of procedural and ethical issues.

The culmination of evidence collection and investigations will normally be a hearing or court appearance. Lack of preparation by witnesses will jeopardise the whole investigation and damage credibility. You should therefore ensure that you, your organisation and your specialist security staff are aware of court and judicial processes and the implications of poor preparation.

Managing discrimination in the workplace is not only something that should be done, it must be done to provide equality but also to comply with the law. It is incumbent upon all personnel at all levels of an organisation to recognise that discrimination is wrong and to ensure that all possible measures are taken to eliminate it. Managers and supervisors have a pivotal role to play in leading and initiating change and response throughout the workforce by raising awareness and making the workplace a more equitable place in which to operate.

Finally, it should be clear that the responsibility for good response to an incident is yours. If managers fail to provide appropriate instructions or guidance to their people, they personally may be held responsible for any failings. To avoid such a situation, you must know what can and cannot be done in the name of security. However, always remember that there are many agencies and organisations which can assist you.

Using the notes in this workbook, and perhaps through discussion with your HR department, describe what you believe is the legal position on discrimination in the following scenarios:

1. A male security officer is refused assignment to a client's site as his hair is considered too long; it extends past his shoulders.

2. A female security officer is frequently late for work due to problems with child minders. There is a suggestion that she be replaced by a security officer with no children.

3. A security officer applicant is refused employment by a company with a large site requiring foot patrols because his obesity prevents him from walking more than 200m without becoming out of breath.

4. A Muslim security officer insists on being allowed prayer breaks during assignment without being docked pay. His supervisor disagrees, arguing that he can pray on Fridays.

5. A security officer is fired because he has been convicted of travelling on public transport without a valid ticket. The offence has nothing to do with his workplace.