

Best practice guide

Counter- terrorism security for business premises



Pool Re
SOLUTIONS
Building resilience against terrorism risk

Contents

Physical security

Personnel security

IT infrastructure and information security

Good housekeeping

Corporate profile and specialised business processes

Risk management and emergency procedures



Foreword

Each business sector faces its own unique challenges with varied levels of risk associated with the nature of their business, their profile, their people or their location. The best practice counter-terrorism security guide for business premises is a collaborative work between Pool Re and protective security professionals who have drawn on their extensive experience and on the best practice to be found within Government and relevant professional bodies.

Where appropriate, links to these have been embedded within the guide to direct users to further guidance and support.

The guide has been provided by Pool Re for the use by its members and the members' clients and is just one small part of the range of solutions Pool Re have to offer.

The guide is designed to underpin the Vulnerability Self-Assessment Tool (VSAT) which is available through the Pool Re website. VSAT

is one of the routes to obtaining a Loss Mitigation Credit (LMC), which may enable you to receive a discount on the cost of your insurance premium, provided you meet the necessary criteria.

Key aspects of security architecture are explained in terms of their benefits and potential impact on business. The Guide is not exhaustive in covering every possible aspect of security. But it does provide the guidance needed to understand and put in place the core elements of security whilst signposting the user to where they can find further support.

Regardless of your security knowledge or experience, the contents of this guide will be useful to you.

arl Partners & Pool Re

Throughout this guide there are links to additional information denoted by **bold blue text which can be accessed by simply clicking where it appears** on the relevant pages.



Physical security

This section considers both the range of equipment and the technology used to protect your site. Physical security measures will usually be the first line of defence against any potential intruders and are also the most visible. Ideally, physical security measures will deter, detect, and delay any potential intruders while the appropriate response is coordinated and delivered. Installation, maintenance, management, training and operational policies are also key elements in ensuring these security measures continue to provide the layers of protection necessary for your business. The section covers a broad range of issues. It explores both the types of physical security measures that could be in place and how they might be supported and integrated into the overall security architecture and day-to-day business processes.

Perimeter security 8

Perimeter intrusion detection systems (PIDS) 10

Lighting 11

CCTV (Including Video Analytics) 12

Intruder Detection Systems (IDS) 16

Access control 18

Security guarding and patrolling 20

Facial recognition 22

Penetration Testing 23

Glazing 24

Vehicle Access 26

Drones 30

Conclusion 32

Physical security

Perimeter security

A well-defined perimeter, whether this is a fence line or the fabric of your building, establishes 'rules' which effectively communicate the existence of a private place and that access rights are required. It also demonstrates that the site is owned and managed, which creates the perception that the occupiers and users are aware, alert and prepared to challenge potential intruders. If you have extensive grounds, perhaps including woodland or areas of waterfront, ensure you have clearly marked where your boundary and responsibilities begin and apply the same rules throughout your property. The adoption of this approach generates further benefits to the security of the site and how it is viewed by those who may seek to gain access but it will require a sustained level of effort to maintain it.

If your perimeter has significant gaps and areas where it is in disrepair, then it presents a range of opportunities for intruders to enter your site undetected and for them to escape easily after committing a crime. A state of disrepair also suggests that your site is not well managed and that there may well be security deficiencies elsewhere across the site.

Those who seek to commit crime will almost always conduct a degree of assessment and hostile reconnaissance as they look for vulnerabilities to exploit. A poorly defined and maintained perimeter suggests that the site is not well-managed and that staff are not alert to, or concerned with, the threat of crime.

Effective signage at established access points supports the positive image of a site being professional, well-managed and safe. At times of emergency, people can quickly identify escape routes and emergency services can respond more effectively. The ability to close off entrances at times of heightened threat is a further security benefit which can deter and deflect potential attackers. Ensure you comply with other legislation such as fire regulations.

Physical security

Perimeter intrusion detection systems (PIDS)

If your perimeter is defined by a fence or wall, then Perimeter Intrusion Detection Systems will assist in enhancing your first line of defence. PIDS can provide significantly enhanced protection to a perimeter, especially on sites where there are extensive fencing runs and where fence line checking is challenging. A range of systems is available from basic features such as a cut sensor, vibration sensing, audio, infrared, pressure and video analytics. These functions can be embedded within a CCTV platform and therefore require careful design, planning and implementation to ensure optimum performance. Integration with an appropriate lighting environment is also important here.

Whatever system you have deployed, it must be capable of detecting an attempted breach before the breach is fully achieved, then send an alert to a monitoring station. That alert must generate a response to the incident which has the capability to neutralise the threat before lasting or significant intrusion or damage can be achieved. If this response capability is not able to meet that standard, then your PIDS will offer no more protection than an audible 'bells only' alarm and the absence of an integrated response will quickly be identified through hostile reconnaissance.

Lighting

A good lighting regime provides an enhanced working environment, enables people to move around your site with confidence and for your staff to spot any unusual activity.

When strategically designed, security lighting can perform an attractive dual function and can assist with other security systems such as CCTV. However, if the lighting is not uniform then areas where there is poor or even no visibility can exist, and those areas can become known and could be exploited by those wishing to move onto your site undetected.

Such areas can be created temporarily by equipment failure so lighting equipment should be supported by a management and maintenance regime. Any damage

and defects to your lights should be identified and rectified quickly.

If you have external areas around your site, then your lighting will assist in forming a 'Protected Area' around your site's important areas which will enable enhanced levels of surveillance by your staff and your security personnel. These areas might include any residential blocks or units and other facilities such as plant, equipment, storage, heating and ventilation, emergency access and vehicle access points. A uniform level of low light across these areas is easily achieved and makes it difficult for intruders to hide or pass through unnoticed. The 'Protected Area' should be supported by other security initiatives, such as security patrols and perimeter checking.

Physical security

CCTV (Including Video Analytics)

Well-designed CCTV systems with strategically positioned cameras represent an effective security tool which can be of significant benefit to any integrated security regime. Investment in correctly sited CCTV that is monitored and trained on the important aspects of your site means that those areas can be better protected and resources better tasked when incidents occur. Ensure your CCTV system is properly maintained and if it is extended, refurbished or replaced then use an established Operational Requirement (OR) process to optimise the design, installation, management and operation. A structured CCTV OR process ensures you develop a statement of your overall security need and defines your CCTV requirements. The OR allows you to specify exactly what you want out of your CCTV installation without having to understand the full technical specifications necessary to achieve those aims. All CCTV system

installations, whether they are new build, extensions or upgrades, should be defined in this way, so your recommended installer knows what system capabilities have to be attained. As a customer, you have a written record of your requirements and if these are not met then you are in a strong [position to require the installer to make the necessary adjustments.](#)



Having a CCTV system capable of producing images of a person at a minimum of 50% of the screen height will enable those images to meet the Home Office 'RECOGNISE' Standard.

Achieving this resolution allows security personnel and investigative authorities the opportunity to recognise a suspect, day or night, who may have visited your site on previous occasions or has been observed at other locations under suspicious circumstances. Producing a description of a suspect

and supporting it with a quality image is a major step in detecting and preventing crime of any nature. CCTV systems of this standard can also be of great assistance in locating lost or vulnerable individuals and for the collection of other details. Higher resolution systems are available and a mix of capability can be deployed across a single system with the right equipment.

The CCTV system should be integrated with other disciplines such as the internal and external lighting and grounds' maintenance. Do not forget to include any temporary works which, without careful planning, can disrupt parts of your coverage and capability. In winter months or after spells of heavy rain and wind you should conduct a check of the external cameras for damage and debris, making sure that the lens covers are clean. The CCTV industry benefits from constant innovation and component upgrades so keep up

to date with improvements and look out for opportunities to install cost effective extra capability.

Video analytics is a collective term for a broad range of software programmes designed to enhance your CCTV system performance. Capability has soared in recent years, but generally video analytics programmes could be described as oversold and underused. Programmes offer a portfolio of elements which bolt on to your digital system and include the ability to apply virtual perimeters, virtual enclosures and criteria for movement detection.

These allow you to develop specific alerting conditions, such as applying time limits on alerts, direction of travel across perimeter lines, direct and random movement filters and even the ability to screen out body masses above or below a certain size, which can help to reduce false alarms especially in areas where

Physical security

CCTV (Including Video Analytics) continued

there is wildlife movement. As with all alarm and alert functions there is a requirement to support them with a monitoring and response capability as these optimise the benefit any video analytics provide. Ensure your CCTV personnel are properly trained in the use of the system and review the way in which the system is being used as part of an ongoing maintenance programme to keep the alerting criteria relevant to your security requirements. This should keep alerts to within a manageable number and reduces the likelihood of alerts being overlooked, disregarded, overwhelming or disruptive to business processes.

The monitoring of a CCTV system is an integral element, important in maximising the contribution that CCTV makes to your overall security regime. On site monitoring by your own, trained personnel allows early recognition of developing security (and other) incidents by people

who know and have an interest in your site because they work there. Local knowledge is valuable in understanding how your site operates, who should be there and recognising when something may not be quite right. Ensure your personnel are properly trained and motivated and make best use of all the options available to keep that motivation at a high level. Options such as staff rotation, camera tours, automatic camera parking, blank screen technology and the overall monitoring environment should all be considered.

Staff who have been trained to operate your CCTV system will be able to maximise the benefits it brings and quickly understand any limitations. A capable CCTV operator is a valuable asset who can significantly contribute to the integration of your CCTV with other security elements. Ensure that their training and accreditation are kept

i up to date and seek out their views on site vulnerabilities and how your systems and policies could be improved or affected by change.

There is no set time for the retention of CCTV images. However, industry best practice guidance suggests that recorded CCTV imagery should be securely retained for a minimum of 31 days. For some CCTV networks this can result in a huge amount of data that needs to be stored. You can introduce initiatives to optimise your data storage through simple changes such as reduced frame rates at times of inactivity and the use of motion sensors. Be aware that if there is an incident at your site or in the field of view of your cameras then the local authorities may seize your recordings' database and even some of your equipment. So, make sure you have backup and duplicate storage to give your network some resilience. They will also keep you

operating in the event of certain system faults arising, which over time will be inevitable.



Physical security

Intruder Detection Systems (IDS)

Intruder detection systems (IDS) are very often the base level electronic protection measures deployed to support physical measures such as doors, gates, locks and barriers. As with any automated alert system, the way in which IDS interact with other elements of your security regime is key to their effectiveness. In principle they should provide a deterrence and should alert quickly enough to allow security responders to reach the point of intrusion before intruders have managed to gain entry. Monitoring is important, audible or 'bells only' systems are of little concern to the determined attacker. Use an Operational Requirement (OR) to develop your security needs and to define the system and support elements, as well as the maintenance regime that best suits your environment.

An alarm system contributes to the 'Detect' and possible 'Deter' aspect of protective security measures. Within most city centres the police will strive to respond within 20 minutes to an alarm activation; in most cases this can be achieved in less than 10 minutes. But you will need to coordinate and liaise with your local police force to ensure that they can respond within an acceptable time frame.

Remote Signalling Systems, known as Type A alarm systems, automatically generate a police response in line with the National Police Chiefs Council's alarm policy, which consists of a 'double knock' alarm system. For example, the breaking of glass may trigger one aspect of the alarm, which, if followed by the activation of an internal motion sensor (Intruder Detection System,

IDS), provides confirmation that an intruder is present. It must be noted that there is a strict policy around false activations and should an alarm provide three false activations within 12 months, then the police response may be removed.

All alarm systems must be registered and allocated a police Unique Reference Number (URN). Moreover, for the police to issue a URN, the alarm system must be connected to a recognised Alarm Receiving Centre (ARC) and/or a Remote Video Response Centre (RVRC). The installation and the services provided by the installing company and the ARC should be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body.

The Redcare system is a widely deployed standard from British Telecom (BT). Redcare is a Secured

by Design approved product and as such has gained the Police Preferred Specification status and attaining [the highest grade \(Grade 4\) of the new European Standard 50131](#).



Physical security

Access control

All employers carry a responsibility and a duty of care to ensure the safety of their personnel and any visitors to their sites. Even if you do not allow members of the public to enter your site, it is likely that they can move freely around the perimeter and could access other premises adjacent to you, but which are outside your control. Potential intruders will exploit any access they can obtain to adjacent buildings from which to launch an intrusion or an attack onto your site. So, you will need to have effective plans, policies and mitigation measures in place to guard against that eventuality.

An Access Control system should ideally have Networked IP based technology which can be integrated with doors, speed gates and lift consoles and managed within a dedicated security office.

Your chosen solution must provide a number of basic core functions, such as: anti-tail gating (which should

include an alarm activation if a card is used first on any access control point by bypassing the first point of contact); pass-back detection (used on same access control reader multiple times); lock-bypass; zoning or role-based access (specific to tenant floors for example); a biometric option for increased security; and fail secure (people can exit during an emergency but not enter) which ensures that the fire alarm cannot be used as a means to override the access control to gain unlawful entry. An Access Control system also enhances the employees' safety by preventing them from re-entering a building that might be on fire to collect personal possessions. A 'Fail Secure' system will not hinder an emergency response in the event of a fire.

Biometrics incorporated into the Access Control system are generally used for high security facilities and incorporate functions such as voice recognition, fingerprint or retinal scanners and facial recognition.

Some form of battery back-up or other Uninterrupted Power Supply supported by a detailed service level agreement should also be incorporated within the system. An integrated Access Control system should also have the ability to 'Zone' your site and provide an audit that provides a record of who used which door and more importantly who tried to use a door that they are not authorised to use which can also trigger an alarm for security purposes.

i An integrated Access Control [system will also provide the means to conduct a 'Dynamic Lockdown'](#).

Clear signage will also send a message that your site is well-managed, and that security is taken seriously. The lack of clear signage can make it difficult to discourage unauthorised visitors or provide a coherent rationale for their eviction. Some intruders will deliberately test your security resilience by seeing just how far they can intrude onto your

site, then use your lack of signage as a justification. Your staff will lack confidence in challenging intruders when there is no policy to support them, making it more difficult for them to challenge potential malicious activity. Identify where signage is lacking and address any shortfall with additional signage as required. Keep signs well maintained and back up the policy with a challenge culture.

Unauthorised access should not be easy to achieve most of the time if your signage and privacy policy is working correctly. Sometimes however, these efforts can still be circumvented deliberately or innocently by members of the public and well-meaning staff. Staff awareness and a challenge culture should always be encouraged to limit the time any unauthorised person spends in a private area before they are detected and escorted away. If this sort of intrusion is happening too often, you may need to strengthen your access control policies.

Physical security

Security guarding and patrolling

Trained security professionals can deliver a high level of protection to your site and significantly enhance your appearance as a safe and secure environment. They have a positive effect on your employees and on any clients and visitors who will feel confident and encouraged to attend and remain at your site, whilst potential attackers will feel uncomfortable in a setting where there is a high likelihood of detection. Having your own dedicated security team has always been regarded as the best solution as they are part of your staff and can be more loyal than, for instance, a contracted security team. In-house security teams do not require licensing under the SIA Act. However, many companies ensure that all security personnel are trained and registered. If, however, you do

not register your security team, the law requires CCTV operators to be licenced if they use CCTV that covers any aspect of public space.

Dedicated perimeter patrols are a significant element in protecting your perimeter and are highly visible to people as they enter your site and to anyone who may be observing from outside your property. Extending these patrols across your entire site delivers many benefits and signals to potential intruders that their chance of detection is present throughout your estate.

If you have extensive grounds or many floors or levels in buildings to cover, then you should deploy sufficient staff to conduct these patrols effectively and efficiently and consider dividing your estate into separate patrolling areas.

On larger sites it will become necessary to direct patrolling staff from a central point and provide them with the means to communicate so that they don't become isolated and can be quickly redeployed to attend an incident.

However, all that benefit is lost if you only patrol out of hours. Security personnel need effective and ongoing training to keep their skills current and compliant with legislation. In the UK the most prominent professional organisation is the Security Industry Authority (SIA), which provides training and accreditation. Any weaknesses in your security presence and their patrolling will be highlighted through hostile reconnaissance and exploited. The business functions of your site will greatly influence the type of crimes committed against it.

If people are the target, then out of hours patrols will be of little benefit. But if physical assets, such as cash and equipment need protection then this type of patrol may assist. Be aware that many security companies have a number of contracts so they may spend little time at your site and their patrol patterns may become predictable. As with earlier answers, these deficiencies may be reinforced by using other measures, such as alarms and CCTV; but there may still be opportunities to circumvent or divert security assets in order to create or exploit a weakness.

[Click for further guidance on training and accreditation.](#)



Physical security

Facial recognition

Facial recognition is a biometric software application, which sits within an existing CCTV system and is capable of uniquely identifying or verifying a person by comparing and analysing patterns based on the person's facial contours. Facial recognition is mostly used for security purposes.

Whilst the use of facial recognition by the police has been deemed lawful by the courts, it is nonetheless an intrusive tool with human rights

and public rights and public confidence implications that will have to be considered. Use by the private sector is becoming more widespread but is as yet untested in the courts and for further guidance please select [more information 1](#) or [more information 2](#). For information on [surveillance camera codes click here](#).



Penetration Testing

Penetration testing is an integral part of any security regime. However, the use and effectiveness of a penetration test is often misunderstood. Prior to commencing any form of testing, you need to consider whether your existing security posture has ever been reviewed; and if so, whether you implemented all the required enhancements/replacements or training that your review identified. A penetration test is most effective as a quality assurance measure to test the effectiveness of your physical security and security policies. Remember that when you commission a penetration test, it is your test and as such you will

need to set out clear objectives and parameters. These should include areas that you want to test and importantly any areas that you want to keep out of scope for reasons of confidentiality or health and safety. It is strongly recommended that all such penetration tests are conducted with the inclusion of an 'Umpire' who works with you and the testing team. An Umpire can ensure that the test is controlled, is safe and can intervene to prevent the test being confused with a real event. A successful penetration test should result in no penetration being gained.

Physical security

Glazing

Within the urban environment and especially in the commercial sector where buildings are designed to be open, inviting and full of light, the use of glass as a construction element and decorative feature is very widespread. Unfortunately, glass is a contributory factor in up to 95% of injuries sustained in an explosion. The use of laminated glass or protection systems such as Anti-shatter Film (ASF) is recognised across the protective security world as an effective measure in reducing this level of injury.

ASF has a finite life and will degrade over time due to wear and tear and the effects of pollution and sunlight. Physical damage will increase this problem and may make a section of ASF unreliable, which won't actually become apparent until a blast occurs or the window is broken. Therefore, testing is necessary, so

be prepared for sections to fail the test periodically and expect large sections to fail around a similar time as their installation date approaches. Incorporate their replacement cost into your projected expenditure and maintenance budgets so they can be replaced quickly.

Entrance areas and public facades are often where this type of glazing is most common, and these are also the most vulnerable to attack or to damage from collateral effects. Toughened safety glass does not perform well in a blast situation and should not be considered safe unless it has been enhanced with ASF. Protective films can provide additional benefits, such as making the private areas less visible to the outside and helping to control the building's environment through improved insulation and protection from the sun.

It is important to ensure that all windows and apertures, including those easily accessible from a low level are fitted with locking mechanisms (if they are not fixed sealed units) as these are an easy route into a building. Even at the most basic level of security, it must be possible to both close and lock shut these features. If they are located in concealed or very quiet areas and particularly if they could provide access to important, sensitive or private areas then consider how they could be better protected by using grilles, bar sets or other physical measures, such as alarms. It may be possible to brick/block some up. Where this is not possible then ensure your staff are compliant with a policy of keeping such windows locked shut when rooms are unoccupied and provide your visitors with similar security

advice. Consider your compliance with health and safety and any fire or other relevant regulations before compromising any ventilation or emergency access options.

Physical security

Vehicle Access

Vehicles feature highly in the commission of many types of crime and can be used for a variety of purposes including the transportation of the perpetrators, their equipment and the proceeds of their activity. A vehicle is also a means of effecting a forced entry and for concealing a device and delivering it close to or into your premises. Trojan vehicles, those which are made to appear trustworthy, perhaps through branding or a cover story, have been used to gain entry through access-controlled points. Sometimes your staff may be forced to carry out an act against you when they are placed under duress and this may include using their own vehicle to transport people or equipment past a control point. Vehicles therefore present a range of opportunities and permitting their access on to your site, particularly if they can be brought close to occupied buildings, requires careful management. Properly managed and effective access controls of your parking facilities will help to reduce the

opportunity for them to be used and abused, either in the commission of crime or as a location from which a terrorist related event can be initiated. There are a range of controls that can be used, from a manned entry point where a physical check can be made of someone's permission to access the site; to an automated system that can include barriers that are activated by some form of electronic pass enhanced through the use of CCTV covering the entry point. However, no system is perfect. For instance, following an authorised vehicle through an access control measure, known as tailgating, is relatively easy to achieve and creates a vulnerability in your security.

You should have a record of which vehicles, together with the vehicle's registration number, type make and colour, belong to which members of staff. A parking permit should be issued and displayed where it can be seen and checked by the security

staff whenever the vehicle is onsite. Staff should be instructed to comply with your parking rules and regulations and that they must set an example to any visitors and clients. These rules must apply to all staff regardless of their position or seniority within the organisation. Visitors should also be allocated parking permits that should be date stamped and should be handed in when they leave your site. Colour coding can also be used to help your security staff identify a visitor's vehicle on sites where there are large numbers of cars parked.

Any parking policy that includes the issuing of staff and visitor parking permits will only be effective if it is supported and enforced by a patrolling regime. Both staff and visitors should be informed about the policy and made aware that any concerns relating to their vehicle will be brought to their attention. Ideally, your patrolling regime should avoid becoming predictable and should be conducted at different times of the day and frequently

enough so as to avoid leaving any long gaps during which a vehicle could be parked unnoticed.

The Centre for the Protection of National Infrastructure (CPNI) recommend that the minimum "Stand Off" that should be achieved between a vehicle and a building should be 30 metres. "Stand Off" or the lack of it is a major vulnerability which may, depending on the site's construction, layout and location in relation to other features, be very difficult or even impossible to create. However, most problems can be mitigated to some degree and it is likely that you will have some opportunity to reduce the risk of a Vehicle Borne Improvised Explosive Device (VBIED) being left in a vehicle right beside or in close proximity to your buildings. Identify the areas of potential vulnerability, explore how they might be reduced or at least how the threat of a VBIED could be pushed further away from your buildings. The principles of Crime Prevention Through Environmental Design (CPTED) www.cpted.com

Physical security

Vehicle Access continued

ected.net. could help you identify some options. Every metre counts so even a small gain is worth the effort. Do not overlook waterborne access or underpasses. Consider also the features of your building and the landscape at the points where vehicles can be left. Are there entrances here, large areas of glazing, rooms where people congregate such as restaurants, bars, and function rooms? Are people accommodated in this area of the building? It may be possible to relocate some of these areas away from the potential point of threat. As mentioned earlier, ASF and laminated glazing systems may be an option. You may be able to use your own

i vehicles to effectively **block the areas off, even as a temporary fix.**

In addition, you may have a requirement to incorporate full time vehicle searching. However, this is only viable at sites where there is a small volume of vehicular traffic or there are multiple access points as the time taken to successfully search

and 'clear' a vehicle for entry can quickly cause queues to develop at your control point, especially during peak times. Note that congestion can in itself represent an additional threat and create another vulnerability. Given the costs and logistics associated with full time vehicle searching, this level of search regime is usually only associated with those sites that require a high level of security.

If you have any underground facilities, these will present a very real security problem as they have been a preferred route for VBIEDs to devastating effect.

The arrangement of these spaces can contain the effects of blast causing more severe damage locally, with larger devices causing partial or even total structural collapse. In town and city scenarios where land and space is at a premium, the development of sites with underground parking has been seen by developers, planners and architects as a solution, allowing them to use space above ground for more

attractive facilities, such as restaurants, bars, terraces and retail sites.

This use of space creates a potential for large numbers of vehicles to be located immediately below areas of your site where people congregate. Your underground areas need to be protected by a robust access control policy which minimises the opportunity for unknown vehicles to access them. Policies should include the ability to implement additional security measures at times of heightened threat. Wherever possible, this should allow the complete closure of underground parking, even if only temporarily.

In addition to facilitating staff or visitor vehicles you may also have delivery vehicles in attendance. If so, these types of vehicle require a different approach. The best practice guidance is to manage deliveries away from the main activity areas and not to allow delivery vehicles into underground areas at all. Existing conditions may make this difficult to achieve. A good

alternative is to agree a policy to use only trusted suppliers and make deliveries by appointment, with drivers calling ahead and confirming names, vehicle registration numbers and arrival times beforehand. At rural and isolated locations where you could have more space, you may be able to develop a system of accepting deliveries at the edge of your site, away from vulnerable areas. You can then utilise your own, trusted vehicles to finalise the delivery on site.

As a consequence, having an effective enforcement regime that differentiates between authorised and unauthorised vehicles having access to your site and which takes effective remedial action will act as a deterrent to those who may be looking to cause you harm. And it will reduce the likelihood of people trying to exploit your parking facilities for their own purposes.

Examine and review your enforcement policy to ensure it provides flexibility to cater for a range of circumstances.

Physical security

Drones

Drones, also referred to as Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aircraft Systems (RPAS), vary in size from larger 'Military' platforms that operate without a pilot being on-board to much smaller ones, often referred to as Hobby Drones, which are commercially available from numerous retailers.

The capabilities in terms of distance and flying time and the 'Pay Load' they can carry vary greatly. Small commercially available drones can carry between 0.3 to 2kg in weight. From a terrorism perspective, this restricted payload will dictate what attack options could be considered. For example, a drone with 2kg of homemade explosive would have little effect on a large building, whereas if the same drone was flown into a crowded place, the

impact would be more significant. A drone carrying 2kg of noxious chemicals could be more impactful if it was used as a dispersal device. Small commercially available drones also have a very limited flying time of around 20-30 minutes on average and may also be further limited depending on the skill of the operator.

Risk mitigation measures remain immature. While several technologies exist for countering drones, none represent a panacea. Furthermore, private bodies in the UK are not currently authorised to deploy 'effectors' to deal with hostile drones. Jamming either a frequency or the GPS (common on most drones) could have a broader, disruptive impact on the wider community and as a consequence are not permitted by law.

Drones have caused widespread disruption within the UK, specifically around airports. However, it must be remembered that the use of drones is still limited. With the advances in technology, longer flight times, greater capacity to carry heavier loads, the threat from drones could be significant to your organisation.

From an insurance perspective, attacks involving drones are much more likely to result in business interruption losses than damage to property. With relatively small payloads, commercial drones are unlikely to be used to deliver large explosive payloads. However, their inherent mobility means attacks could cause disruption over large areas, with potentially significant business interruption losses arising from post-incident investigations and clean-up.

As of the 30th November 2019, anyone responsible for operating a drone or unmanned aircraft weighing between 250g to 20kg, will have to register as an operator with the Civil Aviation Authority (CAA). They will then need to pass an online theory test before obtaining an operator ID.

However, this recent change in legislation will not prevent drones being used in the commission of terrorist acts. It should, however, reduce the potential for the nuisance use of drones, as seen at airports or other sporting events. Any drone registered can be traced back [to the operator under the new CAA registration scheme](#). If drones are deemed a credible threat to your organisation, then [you should consider some of the mitigating options](#) that you could deploy.



Physical security

Conclusion

For most organisations, Physical Security measures will provide both the first line of defence to any potential intruders and will also provide their most visible commitment to their approach to security. Having a robust security architecture in place will go a long way to deterring those who may have malicious intent. However, your site will need to have a layered approach that provides the site with defence in depth so that it cannot only deter but detect, delay and respond to any potential intruders before they have the opportunity to cause any harm or damage. This section considered both the range of equipment and technology that can be used by your company but also provided pointers to examine how well the security systems have been installed, maintained, managed and integrated with the site's security staff. In order for the physical security measures to work, all of these aspects must be operating effectively and efficiently.



Personnel security

This section considers the measures employed to recruit, train and deploy the company's staff, including its security personnel. It will also help you consider how staff should be managed, how they should be supported and equipped; how they are trained and motivated and where failures or weaknesses in the personnel management regime may create vulnerabilities or opportunities for organisational harm.

Understanding how to nurture and encourage loyalty and integrity as part of the company's security culture is a key element in personnel security. Having the right culture will not only enhance the overall security regime and the protection of all company assets but it will also deliver a number of other business benefits. Note, however, that the advice provided here is generic in nature and in line with UK best practice and employment law.

Pre-Employment Screening 36

Training 38

Policies and Procedures 42

Conclusion 46

Personnel security

Pre-Employment Screening

There are many reasons to support the use of pre-employment screening as a measure to check prospective staff credentials. It is very common for false claims to be made in job applications to secure employment or a higher wage than the actual skill set would attract. The wider implications mean that an individual employed to represent your company may not be able to do so at the standard you expected, with a potential for embarrassment and reputational harm. Employment means access to information, premises, systems and assets and so an employee who has lied to gain these permissions may have more sinister outcomes in mind. Today, most companies in the UK, unless required to by law, will only provide a reference that confirms a former employee's employment dates so you may not get any insights into a prospective employee's performance or behaviours. Ensure your screening methods are up to date

and place a requirement on your personnel to inform you of relevant changes in their circumstances which may affect their employability. The use of external personnel supplied through agencies or third-party contracts is very widespread across multiple business sectors. It is important that your personnel security measures relating to employment screening are applied as robustly to externally sourced personnel as they are to your own staff. Your organisation must have clear guidelines on how to manage all personnel issues relating to external personnel because any performance issues with them will have to be addressed with the third-party provider.

Even if screening is a policy that you have required from your third-party providers for some time, you will need to check that it is still being applied by them. All companies look to manage their costs efficiently and

your third-party providers' decisions will not always be in your best interests. Be sure that your external suppliers are not undermining your stated policy requirements deliberately or otherwise, especially where they themselves may have sub-contracted your requirement to another supplier of their choice. Remember that access rights and permissions to your estate, systems, resources and data are the primary goals of those looking to cause harm and placing an individual into your business through an external supplier is a well-used tactic by those with malicious intent. Consider and review your requirement for third party personnel especially where the roles afford access to critical assets, sensitive material or other important features of your business. As best practice these areas of employment should be provided to your own trusted personnel wherever possible.

Personnel security

Training

Induction training is one of the first opportunities an employer has to train employees in site specific procedures and covers a range of required and optional inputs. It should include site safety and site security and take place as soon as employment starts. This approach promotes an inclusive attitude as it makes the employee feel valued and better equipped to contribute to the company's performance and success. A sense of ownership and responsibility is vital in nurturing and developing a security culture which is the basis of any effective security regime. All employees, including contracted staff, temporary and agency staff should be included.

Training in the implementation of emergency procedures and response plans is of paramount importance if you wish to protect your workforce, colleagues, clients and visitors from harm in the event

of a major incident or where there is a threat which affects your site.

Research has shown conclusively that well-constructed plans which are properly and regularly exercised greatly enhance the reaction of personnel at times of threat. This improves their response, reduces death and injury and the longer-term effects of exposure to extreme circumstances, such as Post-traumatic Stress Disorder (PTSD). It follows too that reputational harm is not only minimised but, depending upon the type of incident, reputation could even be enhanced by a well-executed response plan. Ensure your training is conducted regularly and that any amendments that are made to your plans are then exercised, tested and rehearsed fully. Make sure all your plans are tested and that there are various training options, such as table-top exercises, quizzes and live play

scenarios. Make these as interesting as possible and avoid repetitive training which tends to lead to disinterest and complacency.

Your training should also include Hostile Reconnaissance as it is often associated with terrorism, but in fact it is conducted for many types of crime, including low level acquisitive crime such as shoplifting. People with hostile intent have a range of desired outcomes. These often include the requirement to escape after successfully committing their act. In the first instance they will conduct reconnaissance to identify the vulnerabilities of your site so as to identify the weak points which can be exploited. The reconnaissance phase may include online research, site visits, photography and filming, approaching security staff and employees with questions, sometimes even setting off

alarms or deliberately invoking a security response. All of these are opportunities for your staff and security personnel to identify potential intruders at an early stage and so training in the methods used in reconnaissance is a key security element. Training on how to detect Hostile Reconnaissance should be part of the training provided to your staff as should the need to challenge anything and anyone that is out of the ordinary and to report any suspicious activity. A straightforward and polite challenge to a potential intruder is often enough to deter them from your site and you may not even know that you have prevented or deflected a future incident. A challenge and reporting culture should be embedded in your security regime as an essential element for all your personnel, even if they do not have a primary security role. Security is everybody's responsibility and

Personnel security

Training continued

suspicious activity can happen at any time and at any location on your site. Consequently, any member of staff may be the first to notice it, so they have the opportunity to challenge it at the earliest point. The correct approach is key, usually a non-confrontational enquiry or an offer to provide assistance is more than enough to deter a potential intruder and avoids the possibility of creating confrontation with someone who is genuinely lost or requires assistance and could be a customer. Clearly the response needs to reflect the intruder's behaviour, the type of activity, when and where it is occurring and the intruder's initial reaction to the challenge. A low-level challenge can be escalated quickly to include a response or attendance by your security personnel, contact with the emergency services, or even the initiation of emergency plans. Make sure your training

covers a series of different scenarios and that staff understand their roles, responsibilities and the expectations placed upon them, including what they should not do.

Security briefings are also an excellent opportunity to reinforce the need for vigilance, the need to report suspicious activity and to reinforce a positive security culture. Security must be viewed as everyone's responsibility, so using security briefings as an inclusive practice keeps your personnel informed, up to date and confident in the delivery of a secure place of work. It is also an ideal platform to discuss new incidents, emerging suspicious activity and odd occurrences which may be easier to understand with additional input from other personnel who can provide more detail and a clearer picture of what is actually happening.

Because security must be considered to be everyone's responsibility, you should provide any visitors with a general site security briefing. It should include, for instance, information on how to report any suspicious activity to a member of your staff, as well as provide guidance on any potential hazards and potential dangers and advice on how to respond to an emergency incident.

Use inputs from local emergency services' personnel on a regular basis as they add authority and integrity to your briefings, as well as reinforcing a good professional relationship. For useful information on the terrorist threat [visit poolre.co.uk](https://www.visitpoolre.co.uk)



[co.uk](https://www.visitpoolre.co.uk)

Personnel security

Policies and Procedures

The link between good Human Resource practices and security is often overlooked.

So, a company that invests in its people and provides continuous professional development will generate a greater sense of loyalty, engagement and ownership which are important elements in the delivery of a good and effective security culture. Whilst there is always a risk that staff who have benefited from additional training and the acquisition of further qualifications at the company's expense might be poached by a competitor, many companies have now introduced conditions on their employees regarding the cost of the training and impose a fee or a penalty on staff who leave employment before an agreed date.

As a general rule, personnel will remain in employment longer and perform better in an environment where they feel valued and

supported. A positive environment promotes confidence in the company and the management and is reflected in the quality of business delivery and in customer relations. It also encourages the reporting of suspicious activity as employees who feel a sense of ownership and responsibility for the well-being of their company are more likely to take steps when they see potential harm. A regular appraisal scheme is a useful platform for staff to air their views and discuss potential difficulties. If effectively managed, these appraisals can also allow for changes in attitude and behaviour to be picked up as they develop over time.

Having invested in the various aspects of pre-employment screening mentioned above, it is strongly recommended that you record the details of all non-staff coming to your site, such as visitors or contractors. Signing in and out is part of a rule-setting process which

informs those coming to your site that they are accounted for and accountable for their behaviour on site. When correctly applied, a signing in policy will include the verification and authentication of the visitor's identity using some form of photo identity, confirmation of the appointment and the person they are visiting and the purpose of their visit. For the potential intruder it is another hurdle to overcome.

Visitor badges can be colour coded according to the days of the week and the visitor's access rights, (whether they should be accompanied, for instance), can also be clearly labelled. Badges should be dated, numbered and should bear the name of the visitor. The details should be recorded in a register, (whether handwritten or electronic), and held on site. Company staff who are visiting from another site should be required to sign in. In the event of an emergency, the register will


be the first place that emergency responders will look at in order to understand who is on site, so there should be strict compliance with signing out and the surrender of badges to prevent any confusion. The register can prove to be a helpful post-incident investigation tool when it is necessary to examine who accessed your site and when. Senior visiting staff should not enjoy inappropriate exemption from this policy. It is also important to ensure all badges are handed in before the person leaves.

In today's business world there is an increasing need for staff to travel abroad for a variety of purposes. These could include the need to explore and develop new opportunities, to assess existing workplaces or to develop business and professional relationships with clients and colleagues. Many of these destinations are not as safe as the UK and staff can be confronted with a variety of threats

Personnel security

Policies and Procedures continued

ranging from disease, political upheaval, environmental disasters, road traffic incidents, terrorism and personal accidents to war and crime. Training staff in how to plan and prepare for these threats allows them to travel with confidence and significantly reduces the chances of them becoming targets or victims, whilst increasing their capability to withstand, survive and return safely from a hostile environment or survive a dangerous incident. If your organisation sends your staff to these environments, then a duty of care is created and whether you have adequately discharged that duty will be examined if harm, injury or death occurs on such a journey. A comprehensive package needs to be threat and destination specific. It is also valuable to support any advice and training provided to the member of staff with a debrief on their return to review the quality of your advice prior to travel and to

provide any insights and learning points that can be taken from their trip. These might include issues encountered with accommodation, routes and travel methods in country; or perhaps some tips on where to go for certain types of food, which public places to avoid and comments on local customs and dress codes. All of these can be used to fine tune the advice, training and policy documents related to your TRM package. [Click here for more information.](#) 

At the conclusion of a period of employment, where the employee is leaving the organisation either permanently or for an extended period, an exit interview should be completed to ensure that all of the employee's access rights, passes, keys and codes are recovered and deactivated. The interview need not be too comprehensive but may serve as an opportunity to

understand the employee's reasons for leaving, which may alert you to any underlying malicious intent. Employees can be reminded of the importance of surrendering access rights and that they will be expected to comply with any non-disclosure agreements and to respect the company's operating and security policies. If they are due to return to your employment, they should undertake induction training before commencing duties.

[For further advice click here.](#) 

Personnel security

Conclusion

Employees play a critical role in protecting an organisation from harm. Without the employees full, committed and willing participation, all of the security systems, measures and procedures that may have been put in place will be potentially vulnerable. Neglect, ignorance and indifference are the most common causes for a security breach in any organisation. Having the right organisational culture in place is crucial, not least because it will also minimise the risk of the insider threat, which is often the cause for the most damaging security breaches any organisation can suffer.



IT Infrastructure and Information Security

IT Infrastructure and Information Security is a critical enabler for any business in today's digital and networked world. With the exponential growth in cyber related crime, your company's IT can also prove to be a key vulnerability.

IT security, more than any other, is a specialised discipline that requires the ability to respond to a constantly evolving threat. As an example, current, robust anti-malware protection will defend the IT network against some malware but will not provide any protection from other cyber attack vectors, such as a Distributed Denial of Service attack, the Insider Threat, brute force or even just a weak password policy. This section will consider the general level of IT security. It is not designed to provide detailed advice on the entire IT network, nor does it explore all the potential cyber related threats your company may face nor advise the company on all the protective measures that may need to be considered. This section will therefore only examine whether the essential elements have been put in place to protect the IT infrastructure. And whether they are in line with established best practice principles, providing your company with enough information to understand where the principal IT Security vulnerabilities may lie.

Security Standards 50

Security is a Management Responsibility 51

Passwords 55

Encryption 56

Virtual Private Network (VPN) and Two Factor Authentication 57

Anti-Malware 58

Information Security 62

Cloud Storage 64

Firewalls 66

IT Penetration Testing 67

Risk Assessments 68

IT Business Continuity Plan 70

Back-Ups 72


Conclusion 74

IT Infrastructure and Information Security

Security Standards

There are a number of recognised IT security standards such as ISO27001; SANS Institute's CIS Critical Security Controls; or one of the Government's recommended approaches such as Cyber Essentials, Cyber Essential Steps, 10 Steps to Cyber Security. Boards are tempted to adopt credible standards more through a desire to demonstrate compliance for accountability purposes. And different businesses and their CROs and CISOs will have their preferences as to which standard they adopt because of the level of assurance they believe the various standards offer them and their Boards. In reality, however, any framework or standard is only effective if it has been fully

operationalised, fully understood and used as an active management tool by the business. You will need to do more than simply get accreditation. You must interpret, customise and apply the different components required by each standard according to your assessed risk and business needs.

For further guidance on what accreditation entails, [please click here](#) 

Security is a Management Responsibility

Management - A dedicated information security manager should have the responsibility and capability to manage all aspects of your company Information Security. Because of their level of access to your IT systems, the security manager should have an enhanced level of vetting to that of your other employees. The information security manager's responsibilities should include: who has access to what information; which software, malware and firewall products are installed; where equipment is purchased; who maintains it; where and how it is disposed of and all manner of other issues affecting staff training, data security, data management and asset control. Your IT security policies must cater for a range of different threats and it is unwise to rely upon a single policy to provide protection across multiple disciplines. Ideally you should have a suite of policies including, but not necessarily limited to: Passwords,

Firewalls, Back-ups, Bring Your Own Device (BYOD), Social Media, Secure Configuration, Access, Data Classification and Acceptable Use.

Don't forget, your IT infrastructure also includes smartphones, smartwatches, tablets and laptops, removable media, and the use of personal equipment at the workplace.

Cybercrime is growing and evolving at an exponential rate, so as new technologies and new protection systems come into being, so new tactics are developed to circumvent them. System intrusion is very commonplace, with a huge range of potentially harmful and damaging consequences. System intrusion can occur and go unnoticed for a prolonged period of time during which a lot of valuable data can be lost. Failure to have at least basic safeguards in place will not reflect well on the business in any post event investigation and may result

IT Infrastructure and Information Security

Security is a Management Responsibility continued

in significant reputational damage. Putting in place the requisite safeguards may require specialist knowledge and expertise.

In today's world, most businesses will require their staff to access the business's IT systems.

Your organisation should employ a dedicated IT security manager who has the specialist knowledge necessary to understand and adequately address the threats to your computerised systems. It is best practice to have a clearly defined IT Security Policy that will enable your business to address security risks in a consistent manner. The policy should set out your business' approach to security, make it clear who is responsible for implementing the policy and for monitoring compliance; and make it clear to your employees what their responsibilities are and what any potential sanctions might be in the event of their non-compliance.

Failure by your employees to adhere to the IT Security Policy could result in your business becoming vulnerable to a cyber enabled attack. Deliberate acts of non-compliance and clear failures in the application of the policy by employees must be addressed quickly and, if necessary, with consequences for the individuals concerned. Obvious areas of concern include: the use of personal devices at work especially if they have automatic wireless connection; with social networking, the downloading of unauthorised software, the taking of photographs and storing other media presenting some real difficulties. Devices that have been enabled with near field communication can be accessed and exploited remotely by a Third Party to compromise your IT systems. Remember to provide your staff with regular briefings on the evolving nature of the threat to reinforce the need for good IT security. You should have a process

in place to ensure that your IT Security Policy is reviewed on a regular basis and any changes and the reasons for those changes must be communicated to your staff before implementation.

... but IT security is also an employee responsibility.

Your staff also have a critical role to play in maintaining the integrity and the security of your IT systems. Without their full cooperation and their compliance with your security policies, your IT systems are potentially vulnerable. Keeping your staff informed of the correct procedures and of their responsibilities and explaining the reasons why compliance is important are essential steps in delivering IT security. Without that knowledge, your staff may view aspects of the policy as tiresome and restrictive, which could result in attempts to ignore them. Maintain a policy of active engagement with

your staff and ensure that any new security elements are introduced with the appropriate supporting information and training. In addition, employees leaving an organisation take with them considerable knowledge about the business's operations, assets and security vulnerabilities. This knowledge can present a risk to your organisation, particularly as the circumstances surrounding an employee's departure are not always amicable. A formal and thorough procedure for all staff departures will ensure appropriate actions are taken to protect the organisation, without unduly disrupting the employer-employee relationship. You should also ensure that the policy is applied to any agency and subcontracted personnel, including IT technicians.

You will also need to consider the user access rights within your IT network. Administrator access rights allow users to adjust settings, install and remove software,

IT Infrastructure and Information Security

Security is a Management Responsibility continued

run maintenance programmes, make changes to your hardware installations and download/upload data. All of these activities have the potential to create and introduce threats and vulnerabilities to your network and devices. Hackers can use inappropriate administrator and access rights to implement these changes and their activity will go unnoticed until those changes take effect. Your policy must be clear and robust, only allowing rights according to the user's role and responsibility.

Be aware that users will always want more access than they really need so support this policy with information about why it is being applied and the consequences of network failures.

Passwords

All staff should have their own usernames and passwords for each account and device. NEVER share passwords. It is accepted good practice to have a strongly constructed password using unpredictable information and a broad range of alphanumeric and special characters. Using the same password, or close variations of it, for numerous applications and accounts could make you vulnerable to a hacker or someone using specialist software designed to hack passwords.

The routine changing of passwords is not recommended, unless the accounts to which they apply have been hacked, in which case they should be changed immediately. You should also immediately change your password if another account or website for which you use the same login details has been hacked.

It can be very difficult to remember a lot of passwords but never fall into the trap of writing all your passwords in a book or on a document on your computer. This is like leaving the key under the mat. There are software programmes that will securely store your passwords, but you will still need a robust password to lock this and your computer. These very strong passwords should always be something you can remember and never written down. When using a password management software: first, install a password manager. Second, get all your existing passwords into it. Third, little by little fix all your weak and duplicate passwords.

If you must write passwords down in order to remember them, encrypt them in a way that is familiar to you but makes them indecipherable to others.

IT Infrastructure and Information Security

Encryption

The first line of defence for the protection of your data is to ensure that you have the appropriate physical security measures in your office to protect your IT. These have been addressed in the Physical security section. However, you should also consider the use of encryption and strong passwords to protect the data that is stored on your devices on your IT. As a consequence, even if your computer, for instance, is stolen it will be difficult for anyone to gain access to the data. If in the future your company decide to access data whilst on the move, the use of encryption and strong passwords

is even more important as it is more difficult to ensure that laptops, mobile devices, removable hard drives etc are kept secure. For mobile devices and Apple products, Remote Data Destruction Software is available and will give you the ability to remotely delete all data on your device if it is not recoverable.

Virtual Private Network (VPN) and Two Factor Authentication

When connecting to the internet, be aware that if you are using a Wi-fi hotspot it may not be secure. You should consider the use of a virtual private network (VPN) so that when you connect to the internet using a Wi-fi hotspot your data will be encrypted. In so doing, even if a hacker manages to position himself in the middle of your connection, your data will be protected. Many companies, including banks and software as a service provider offer a two-step authentication method. It might include a number generating keypad or receiving a code by text or email. It is highly recommended

that if you have the option to use two-factor authentication then it is used. Most online banking will have this option.

IT Infrastructure and Information Security

Anti-Malware

As a business you should have a standing policy to update your anti-malware programmes with the latest versions and software patches as soon as they become available. Reputable product developers are constantly monitoring and learning from attack methodology and adjusting and adapting their products to protect them from emerging threats. Your systems should be configured to apply these updates as soon as they become available. Hackers will be looking to develop new methods to defeat any new anti-malware programme and may do so very quickly.

However, failure to introduce the latest anti-malware programmes will leave you vulnerable to the most unsophisticated of hackers and much more vulnerable to criticism and the attendant reputational damage in the event of any breach.

Awareness training in the types of cyber attack

- Training should be provided at least once a year to make staff aware of the dangers of email scams to help them be vigilant of cybercrime. Cybercrime is not new but is still on the increase and you should aim to provide training at least once a year to keep your staff briefed on the evolving threat and techniques used by cyber criminals. Criminals are using a variety of different techniques to obtain sensitive information such as usernames, passwords, bank and credit card details. They disguise themselves as trustworthy companies using SMS, Skype and the telephone; but their preferred method is by email using a technique known as Phishing. Phishing is the fraudulent practice of sending

emails purporting to be from reputable companies in order to trick you into revealing personal information, such as passwords and credit card numbers. Phishing is one of the largest causes of cybercrime. It is easy to execute and can produce the results with very little effort.

Without listing all of the specific types of attack, here are some things to look out for:

- The email contains spelling and grammatical errors.
- The sender's email address doesn't match with the organisation's website address.
- The email is sent from a completely different address or a free webmail address.
- The email does not use your proper name but uses a non-specific greeting like "dear customer".

- A sense of urgency; for example, "act immediately as your account may be closed".
- Uppercase text in the email is used to highlight the urgency to the recipient.
- Check the website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the company that appears to have sent it.
- The email appears to come from a friend, but the content is out of character.
- The entire text of the email is contained within an image rather than the usual text format.

IT Infrastructure and Information Security

Anti-Malware continued

- The image contains an embedded hyperlink to a bogus site.

If you have any doubts of the origin of the email; do not click on any links in the email. Do not reply to the email or contact the senders and NEVER open any attachments unless you are 100% sure this has come from a genuine source. If you have suspicions of the validity of the email, simply contact the company or person using a phone number or email address that you know is genuine and ask them to confirm that the email is genuine. If, however, you have clicked on the link your anti-malware should protect you from any malware but never enter any of your details and close the webpage.

If you think you may have compromised the safety of your details, contact the relevant

company, e.g. the bank, and inform them and change your password immediately.

If you have any doubts about a caller on the telephone and have the slightest inkling that it might be fraudulent, hang up the phone wait for a dial tone and call the number of the company/bank on a number that you know to be genuine. Do not use the number that is given to you by the person on the phone.

For further help and guidance on [scam emails click here](#) and on [Phishing by clicking here](#).



IT Infrastructure and Information Security

Information Security

Your company needs to be aware of what information/data is critical to the business in order to determine what safeguards are required. As part of your IT Risk Assessment and before you can establish what level of security is right for your business, you will need to review the data you hold and decide how critical it is to your business. Consider how valuable, sensitive or confidential, the information might be. Consider what damage the business might suffer, both financially or reputationally, or what distress could be caused to individuals if there was a security breach. Remember, there are a range of threats to your business that include rogue employees, careless staff, third party suppliers, organised crime, hackers and activists. And there are strict regulatory and compliance regimes concerning the protection of sensitive personal data to which you must adhere, and which may carry significant financial penalties if you breach them.

- Consider some of the following scenarios and think about the impact they may have on your business:
- Data theft, loss or data breach – Current and former employees, people with whom you do business or hackers who might, either accidentally or maliciously, compromise your pricing
- information, details concerning your clients including their personal and banking details.
- Software failure – like your business database or another application.
- Accidental or deliberate data deletion or corruption – it's all too easily done if proper security measures are not in place.
- You can never be totally safe from attacks, however most of them can be prevented or detected with simple security practices by you and your staff.

Personal media devices represent a significant security vulnerability. Modern devices have sophisticated processors with the ability to handle, store and deliver large amounts of data at high speeds across multiple platforms. Users are often unaware of much of the devices' functionality and how to control it, so users are also unlikely to understand how these devices can present an opportunity to a capable cyber attacker. Hacking is commonplace and allows a person to access a device without the user being aware and with no obvious activity being displayed upon it. Certain programmes can remotely switch on the video and audio monitoring or recording functions or enable remote access to computer networks thereby allowing sensitive data to be read, downloaded, altered, corrupted or destroyed. The consequence will be damage to your business systems and your reputation. Much social importance is placed on users having constant

access to their devices and restrictions in the workplace may be unpopular. Consider where these devices might make you vulnerable and how you can implement changes to reduce that vulnerability.

Work with your staff to ensure they understand the rationale for any policy changes and any new restrictions and manage their introduction to reduce the impact on your staff. Sudden and significant changes will cause disruption and will result in non-compliance from some employees.

IT Infrastructure and Information Security

Cloud Storage

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than on a local server or a personal computer.

Although storing data in the cloud seems simple and secure, you will encounter risks that you might not be fully aware of. It is important that you consider the security of the data that you hold in the cloud and put in place some simple safeguards. Again, the use of encryption and strong passwords are essential. Consider using two-factor authentication, which is where the provider will send you a password by SMS or email; or the use of a token from a keypad device.

You will need to ensure there is a secure connection from your computer to the cloud. If you are using one of the popular providers

like Google, Dropbox, Microsoft 365 etc they will all provide a high level of security of data in transit. However, if you are using a Software as a Service (SaaS), for example a customer relationship management (CRM) software to keep track of your customers, you will need to ensure the data is transmitted securely. Look for a padlock symbol or the HTTPS on the provider's website or ask your provider.

Be aware of your country's data protection regulations as some jurisdictions do not allow personal data to be stored outside of that country. For the UK, personal and sensitive personal data must not be transferred to any country or territory outside the European Economic Area (EEA). You will need to ensure that your cloud provider can guarantee this. You will also need to ensure that any help desk service on

which you might call to access any personal or sensitive personal data is also located within the EEA.

You should also be aware that if your data is held offshore a foreign law enforcement agency may have the power to require your cloud provider to give them access to your data or disrupt the availability of that data.

 For [ICO guidance click here](#).

IT Infrastructure and Information Security

Firewalls

Firewalls are the first line of defence against all manner of cyber threats and intrusions and can be placed on software, hardware or both. A firewall is a network security device which establishes a barrier between your internal, trusted network and external, untrusted networks such as the internet. It monitors incoming and outgoing network traffic, allowing or blocking that traffic depending upon a set of network security rules. At the most basic level, your system must be protected by a Proxy Firewall, although this protection will be limited. A 'Stateful Inspection Firewall' will monitor all activity from the opening of a connection until it is closed and allows administrator set filters to be applied. It will also use information from previous connection activity, but protection is still rather limited. A Unified Threat Management firewall (UTF) provides improved protection by adding in intrusion prevention and malware functionality. It may also have additional services such as cloud management. Currently,

most companies now deploy a Next Generation Firewall (NGFW) to block today's threats, such as advanced malware and application layer attacks.

An NGFW should include:

- Standard firewall capabilities
- Integrated intrusion prevention
- Application awareness and controls to spot and block untrusted applications
- Upgrade paths
- Techniques and options to address evolving threats.

For better protection, you can deploy a threat focused NGFW. This allows you to know which assets are most vulnerable, to quickly respond to threats and attacks, detect evasive and suspicious activity more efficiently, reduce the time taken from threat detection to resolution and streamline your admin and unification with other IT security and general security policies. Review your firewall performance and rules regularly to ensure they remain relevant, efficient and justified.

IT Penetration Testing

Penetration testing is an integral part of any IT security regime. However, the use and effectiveness of a penetration test is often misunderstood. Prior to commencing any form of testing, you need to consider whether your existing IT security posture has ever been reviewed; and if so, whether you implemented all the required enhancements/replacements or training that your review identified. A penetration test is most effective as a quality assurance measure to test the effectiveness of your IT security and security policies. Remember that when you commission a penetration test, it is your test and

as such you will need to set out clear objectives and parameters and an agreed time frame. These should include areas that you want to test and importantly any areas that you want to keep out of scope for reasons of confidentiality. It is strongly recommended that all such penetration tests are conducted with the inclusion of an 'Umpire' who works with you and the testing team. An Umpire can ensure that the test is controlled, is safe and can intervene to prevent the test being confused with a real event. A successful penetration test should result in no penetration being gained into your IT system.

IT Infrastructure and Information Security

Risk Assessments

A full Risk Assessment that examines the threats to and the vulnerabilities of your IT infrastructure has most likely been undertaken. However, organisations that do not perform a Risk Assessment of their IT infrastructure are leaving themselves open to the possibility that their business could be disrupted as a result of their IT being damaged or even destroyed.

In order to conduct a Risk Assessment, you should consider each element of your IT infrastructure individually and establish how vital it is to your business. Think about everything you use on a daily basis including your servers, desktop and laptop computers, netbooks, telephone handsets, mobile phones, routers, switches, databases, software, business applications, custom software and anything else you might be using. For instance,

you might conclude that it would be nearly impossible to run your business without your website and internet connection, but that your printers are not essential. Consider who or what are the potential threats to your IT infrastructure (these could include fire, flooding, power failure, theft, accidental or malicious damage). Then consider how vulnerable your IT infrastructure might be to these threats. And finally, consider what the implications might be if any element of your IT infrastructure were damaged or lost, what the cost might be to your business both in terms of reputational damage and financial loss; and then the likelihood of that event occurring? You might want to think about some of the following examples:

- Theft or loss of hardware - could you cope without key equipment?

- Fire or excessive heat - what would happen in the event of a fire? How quickly could you replace damaged equipment, software and data?
- Water or excessive damp – IT equipment is sensitive to water and if your premises were flooded it is likely that you would have to replace everything.
- Equipment failure or damage – like a broken server or dropped laptop.
- Accidental or deliberate data deletion or corruption – it's all too easily done if proper security measures are not in place.
- Inability to access data (DoS attack, power failure, hardware failure).
- Inability to take payment - PDQ failure, till system failure.

Depending on your assessment of the potential risk, you will need to establish the appropriate mitigating measures to minimise that risk. Make sure that all your staff are aware of these measures and that they are communicated to all of your staff on a regular basis. Some of the mitigating measures might be as simple as requiring your staff to use a pen and a form until a new printer is purchased; or having an account with an IT supplier who can do an emergency replacement of your laptops or screens.

IT Infrastructure and Information Security

IT Business Continuity Plan

Plan for IT – As a business it is essential to have a business continuity plan in the event of any information loss or disclosure that is tested on an annual basis. Testing the Integrity of your backup data is essential so that when disaster strikes you can restore your data quickly and, importantly, you can access the data and not lose it permanently. There are several ways to ensure that the data is accessible, but the ideal way is to restore the whole data backup onto a new computer and ensure all the data is available and has not been corrupted. Just setting the backup to run or just checking that the odd file is available will not provide you with any assurance that all of your data has been saved.

Disclosure or a breach may mean that someone other than the authorised user has gained access to your data. This might be personal data or commercially sensitive data. You must ensure that there is a process in place to limit the damage caused by any disclosure. Your staff must be aware of this process, who they need to inform in the event of a breach and the actions required to contain the issue. Helpful guidance is given by the UK's Information Commissioner's Office. Once you have done a full Risk Assessment and examined the threats to the vulnerabilities of your IT infrastructure you will need to ensure that the mitigating strategies actually work by conducting tests.

Simulating fire or water damage is obviously not practical but you can test to see if you could continue to work effectively if some of your IT Infrastructure was not available. Test to see if you can still operate efficiently from your location without critical items and how long it would take to replace a computer monitor or laptop for example.

Testing a power failure, to ensure the backup power is available, is simple if using an Uninterruptible Power Supply (UPS). Ensure you have backed up all your work and that nothing could be damaged or lost if the test does not work. Then, simply switch off the power at the wall socket or pull the power supply. The UPS should supply power with

no interruptions. If you are reliant on backup generators these should be tested on a regular basis by a qualified person.

Specialist companies can provide Penetration Testing which will simulate an attack on your IT Infrastructure. Getting help from a specialist company will help you understand the extent to which an attacker can access your confidential information, corrupt your data's integrity or impact your ability to operate efficiently. For additional [ICO guidance click here](#).



IT Infrastructure and Information Security

Back-Ups

It is important to do regular backups to prevent the loss of data. Software can be reinstalled. But your data could be lost forever for a number of reasons: hardware failure; accidental file deletion; theft; fire; flood; accidental damage; malware infections; and file deletion during operating system upgrades.

The first time data is backed up, a full backup will be carried out. Subsequent backups need only be incremental - where only files that have been changed or added since the last backup are stored. Most modern backup processes select which mode to use automatically. There are two main methods of backing up your data. Removable/Portable Hard Drives or online/cloud. When choosing between them, you will need to consider ease of use, speed, and price or a combination of both. Do not use USB memory

sticks, recordable CDs or DVDs to back up your data. Although these may appear to be inexpensive and convenient methods, they share limited capacity and are also easily lost or stolen. CDs and DVDs are also very slow to transfer your data.

Removable/Portable Hard Drives - A Removable/Portable hard drive is a fast, efficient way of backing up all of your data. Removable/Portable hard drive can simply plug into or connect to your computer via your wireless network. These drives can then be removed and stored in a safe off site. It is important to test that the data you have backed up on your portable hard drive can be recovered if needed. You should test this by using a different computer to ensure that the back-up is compatible – and recoverable – in the event of the loss of your existing computer.

Online/Cloud Backup - The use of online backup is a very convenient, secure and low-cost option. There is virtually no limitation on storage space so you can backup data from one or two documents or the entire contents of your computer. Some providers supply limited storage free of charge, but generally the cost of backups increases proportionally to the amount of data involved. There are many providers of online backup. These include internet service providers (ISPs), internet security software vendors and companies such as Apple with the iCloud, Dropbox and many others.

Be aware of your country's data protection regulations as some jurisdictions do not allow personal data to be stored outside of that country. In the UK for example, all personal data must be stored with the European Economic Area.

IT Infrastructure and Information Security

Conclusion

Cyber related crime is growing exponentially. It includes not only financial loss, but also the loss of intellectual property, the loss of proprietary information, such as client data and pricing information, reputational harm and loss of confidence. And, depending on the commercial sector, cyber related crime can also include interference and even sabotage by third party and state sponsored actors. This section has considered those issues that will provide your company with a general IT health assessment and whether the essential elements to protect your IT infrastructure in line with best practice principles have been put in place. Given the growing complexity of the cyber threat and the speed with which it is evolving, it has become increasingly difficult to protect the entirety of any IT enterprise. Focus and effort are better placed on understanding what are the core, critical business functions and the information within the organisation that must be protected. Depending on the results, your company will want to address any vulnerabilities that have been identified and may also want to conduct a more detailed cyber specific review that is in line with those functions and that information that are business critical.



Good housekeeping

Good housekeeping is about how you manage and maintain your buildings, your grounds and your equipment. These influence how your site is perceived and has an impact upon its attractiveness as a target. Well-maintained and well-run sites create a positive impression of an environment that is professional in its attitude to safety and security and which will prove hostile to those looking to cause harm. In contrast, a poorly maintained or managed site can appear to be in a state of disrepair or even disuse, where safety and security are not priorities, thereby encouraging exploration and incursion by those looking for opportunities to cause harm or damage. This section looks at your housekeeping, maintenance and repair policies and considers how these can support and enhance your site security when done well or undermine it when poorly executed.

Maintenance 78

Storage Areas 82

Good housekeeping

Maintenance

It is good practice to have a policy for the effective and timely maintenance of all your grounds, buildings and facilities. Well-maintained facilities present an image of a well-run business which takes pride in how it is viewed by the world. Onlookers will associate this image with good business practice and a good security culture. So, your maintenance programme will influence how your site is viewed if it is the subject of any hostile reconnaissance. If your staff are diligent in keeping your site clean and in good order, then they will find it easier to spot changes in its condition, which might include damage, attempts to breach the perimeter, or more structured acts designed to test your security responses.

The early detection of any such acts will send a clear message to potential intruders that the site is well-managed and protected and the risk of more serious harm is reduced. Work with neighbouring businesses to collaborate on broadening this approach into a wider area if other sites nearby are not as diligent.

Having a security-oriented maintenance regime is a significant element of your overall security policy. Staff need to be encouraged to report issues they encounter, and the appropriate culture can be achieved through training, awareness and inclusion. Providing positive feedback to those who identify, report and address issues they find reinforces the culture and strengthens feelings of ownership

and responsibility, as staff see that their concerns are heard, acted upon and considered valuable.

Even anonymous reporting can help reinforce the culture if staff can see that reporting is acted upon.

Timely and decisive action to rectify issues affecting security, maintenance and efficient site operation enhances staff awareness, vigilance and promotes a sense of ownership. These in turn reinforce your policies and send a clear message to everyone that lapses and failures will not be tolerated. If your company leave these issues unaddressed, for even short periods of time, then you will undermine the staff's confidence that these issues are taken seriously. Take steps to improve your response before

standards decline. If some issues stay unresolved, then compliance with your reporting and maintenance policies could evaporate quickly as staff lose confidence in the management's attitude which could in turn have a negative effect on the staff's behaviour in other ways. Take action now to introduce a strong ethos of compliance and response, but also look to understand why these were absent in the first place to reduce the risk of a similar failure elsewhere.

Contractors and maintenance personnel require access to all parts of your building and, depending on their role, significant networks and items of equipment. Their access affords them the opportunity to undertake a vast range of activity

Good housekeeping

Maintenance continued

which may harm or undermine your business or create an opportunity for others to do so. Malicious acts could occur spontaneously or over time, some will be subtle, and others will be in plain sight.

Any member of staff can become influenced by a range of external factors and those who are trusted can alter their views or ideals without displaying any obvious outward signs. Your company's approved list should contain details of all contractors and maintenance personnel, including cleaning and catering staff and any others who are not directly employed by your company. Your company policy should be reviewed regularly and when individuals move away, or particular services or companies are no longer required those individuals

should be deleted from the list. Ensure your company has a set of robust and appropriate criteria for approving new additions. See advice on Personnel Security for further information.

As a general rule, your company should be in control of the maintenance schedule for your site. Your staff should determine when, how and by whom it is done. However, if other organisations have access to your site in order to service their equipment, they will not necessarily disclose their maintenance schedule nor share the details of their maintenance staff unless your company has set in place the necessary protocols. As a consequence, staff who are unknown to your company may be on your site and be less concerned

about your safety and security and who may inadvertently undermine your security regime. Moreover, they may work for an organisation whose risk appetite is very different to your own and which may be at a greater risk of an attack. Without the ability to monitor and strictly control who has access to your site, you may inadvertently create a vulnerability that could result in an attack on their equipment or staff. An attack which results in any damage or harm which has been facilitated by access to your site will result in your company suffering reputational damage and possibly being sued by the organisation which has incurred the loss. Examples of sites where there may be more than one company that has equipment it must maintain include: utilities, TV, radio and some military, aviation and emergency

services' communications centres. Your company should ensure that your staff are always aware of who is accessing your site at any time and for whatever reason and have the ability to check on an individual's credentials with their parent organisation.

Good housekeeping

Storage Areas

It is advised that a designated room or cloakroom should be made available for the temporary storage of visitors' personal effects. Concealing illicit items and improvised explosive devices in parcels and bags is a very common methodology which has been used with devastating results. Stores are a regular feature for most sites, but they need to be carefully managed, so they are not seen as an opportunity for attack. Locating them in well-staffed areas such as a reception reduces the chances of unauthorised access and for items to be placed there. It also provides

greater reassurance to visitors that their property is safe and less likely to be stolen or tampered with. Best practice is to pass items intended for temporary storage through a scanning system which has been assessed to operate effectively in detecting a range of items and materials. Commercial 'off the shelf' (COTS) equipment, such as that used in the aviation industry, is ideal for this purpose but be aware that systems are costly to purchase, take up considerable space and require operator training, regular maintenance and calibration for them to remain reliable.



Corporate profile and specialised business processes

This section considers how your corporate profile or that of other organisations with which you have a relationship might attract negative interest from a range of protest and special interest groups. These may in turn look to target your company with a view to damaging your company's reputation or disrupting the continued operational effectiveness of your business. The section also explores how the presence and use of hazardous materials as set out in Schedule 1 to the Planning (Hazardous Substances) Regulations 2015 which can pose unique security challenges and impact the safety and security of your site. It is important to understand if your company has a national or corporate identity which attracts or could attract protest or unwanted attention from those with extremist, environmental or other views that are opposed to your company.

Protest Movements 86

The Use of Hazardous Substances 90

Conclusion 92

Corporate profile and specialised business process

Protest Movements

In modern society there is a broad range of protest movements that include Extreme Right Wing (XRW), Extreme Left Wing (XLW), Animal Rights (AR), Environmental or other Political views. Their activity can range from lawful protest through to criminal behaviour, site incursions, cyber-attacks, physical assaults and aggressive protests. These can disrupt the smooth functioning of your business, create fear and uncertainty in the workforce and generate unhelpful publicity that can be reputationally damaging. If possible, your business should explore whether the issues that are of concern to the protest group are ones that are in your power to address and if there are ways in which you might be in a position to reduce either the extent to which your business is adversely

associated with those issues or how you might reduce their significance.

Opening a dialogue with the protest group can often lead to a successful outcome but much will depend on their willingness to engage. It is also important to talk with the local authorities and the emergency services as they will probably have useful insights that can help you shape your engagement strategy. You will also have to conduct a full threat and risk assessment so that you can put in place the appropriate security architecture to protect your staff, your critical assets and your reputation from attack. The security architecture will be based on the five main disciplines contained within VSAT®: Physical Security; Personnel Security; Information and Cyber Security; Good Housekeeping; and

Risk management and Emergency Procedures.

Your company is not the only factor which can influence attitudes of extremist action groups or prompt them to take more aggressive protest action. Your business processes and those of your affiliates, your third-party suppliers and organisations providing your labour force are all potential sources of grievance to those looking to justify action beyond a lawful protest. It is important that your company understands where these broader aspects of your business may have the potential to create ill feeling. Sources and suppliers of your raw materials, your contracted workers, recruitment and retention policies, wage levels, welfare, waste management and environmental

impact are all examples of the enormous range of activities your business will encompass and any one of these could be the catalyst for harmful protest and extremist action. Your company should ensure the integrity of these activities and apply legal, ethical and recognised business principles to them all. New ventures and significant changes should be similarly scrutinised, and contracted suppliers of any resource should be performing to the same standards as part of a structured agreement with your company.

Your company should have the appropriate response plans to deal with protest activity which should be reinforced by working closely with the local authorities and the emergency services. If your business

Corporate profile and specialised business process

Protest Movements continued

is never unoccupied, owing to a 24/7 business need or production facilities, this should mean there is reduced opportunity for any unlawful activity. However, on occasion, operating 24/7 can introduce a bias on the need for productivity at the expense of security. As a consequence, weaknesses in your security architecture may emerge and your site could be revealing vulnerabilities to those who are searching for ways to attack you or to commit crime for their own or another's benefit.

Security is a collaborative discipline which should be ever present and should involve all of your personnel across all roles and responsibilities. Ensure you have an appropriate level of properly trained security personnel onsite at all times. Encourage and nurture a security culture across the entire workforce and ensure your security strategy complements your business at all times, whatever your required levels of productivity.



Corporate profile and specialised business process

The Use of Hazardous Substances

Another critical aspect to understanding your corporate profile is to establish whether you use any hazardous substances as defined by the list of substances and controlled quantities set out in [Schedule](#)

i [1 to the Planning \(Hazardous Substances\) Regulations 2015](#)

Hazardous chemicals can represent a significant level of potential harm to your site for a variety of reasons. Stringent health and safety regulations contribute to the security of these materials but some factors, such as isolated storage facilities can sometimes create a security vulnerability. It is often the case that production pressures cause these control measures to be circumvented, resulting in hazardous chemicals being left unattended and vulnerable to theft. Hazardous chemicals can have properties which are useful to those looking to cause harm or to create fear and so large quantities on your site may attract

the attention of people looking to acquire such materials, whether for use at your venue or elsewhere. Acids and solvents feature as precursors in the production of many homemade explosives and even small quantities of just a few hundred millilitres can be attractive to a bomb maker. When large quantities are in regular use then smaller quantities become less significant, opening up opportunities for acquisition over a period of time to go unnoticed. Your site should have specially constructed secure storage areas protecting hazardous materials. Where vulnerabilities regarding unauthorised access or lack of control are discovered, an immediate security review should be undertaken. Seek professional advice to avoid inappropriate or even dangerous storage of chemicals with other chemicals and materials which could result in a violent reaction, explosion or fire.

In addition, items such as fuel or other flammable material carry an inherent risk of fire and explosion following spillage or any errors and accidents in routine handling. Fuel stores can be targeted by those intending to cause harm or disruption because fuel so readily ignites and produces spectacular flames. In many countries fuel is expensive, and, in some areas, it is also in limited supply, making it a target for theft from storage facilities, distribution networks and transport vehicles. In the process of stealing fuel, health and safety is not a major concern and so the risks of uncontrolled spillage and fire are increased, thereby increasing the risk of fire spreading to other parts of your site depending upon where and how the spillage occurs. Your fuel storage sites, and distribution networks should be protected by bunds and appropriate fire suppression systems, with access

control measures applied to manage access and to limit it to those with an operational need. Be aware that health and safety rules in relation to managing the fire risk can actually conflict with security requirements, especially where fuel tankers are operated. You must ensure that both disciplines are fully understood, and a balance of security and safety is achieved. You should also be informed about any fuel storage facilities which are outside of your control but located nearby, because an incident at an adjacent facility may well have significant impact upon your own operations.

If such facilities exist nearby, then approach and work with your neighbours and the emergency services to ensure your safety and security requirements are working collaboratively.

Corporate profile and specialised business process

Conclusion

This section looked at how your corporate profile could impact negatively on your security. There may, depending on the nature of your business and/or where it is located, be little or nothing that is within your company's power directly to change or adjust your corporate profile so that any risks and vulnerabilities that have been identified could be mitigated completely. However, having identified them, any risks might potentially be mitigated by reinforcing your approach to the other sections contained within the assessment.



Risk management and emergency procedures

All businesses are required, as part of their duty of care to their employees and their visitors, to have in place a suite of risk management and emergency response plans. It is also sound business practice to have in place an effective business continuity plan that will enable a business to minimise the consequences of and recover as quickly as possible from any interruption caused by an unexpected event. Creating an effective and proportionate response begins with an understanding of the potential threats your business may face, their likelihood and how they may impact upon you. This section will consider these issues and the extent to which you have effective risk management, emergency and business continuity plans in place.

Risk Assessments 96

Emergency Response Plans 98

Emergency Management Plan 100

Business Continuity Plan 102

Search Plans 104

Mailrooms 106

Terrorism Threat Levels 109

Other Police Resources 110

Conclusion 114

Risk management and emergency procedures

Risk Assessments

A security specific, terrorism threat driven risk assessment forms the foundation on which to design and assemble an effective and proportionate protective security plan. A terrorism threat driven risk assessment should identify the types of threat which may impact upon your business, either directly or indirectly. A clear understanding of the associated risks, based on their likelihood and impact and how you may be vulnerable to them will allow you to plan your counter measures effectively, thereby ensuring you have a protective security plan that

is sustainable, affordable and fit for purpose. Your terrorism threat driven risk assessment must be managed as a 'live' process that should be reviewed annually in line with the evolution of the terrorist threats both to your business and also to the safety and security of everyone within your working environment.



Risk management and emergency procedures

Emergency Response Plans

It is essential that businesses today have detailed emergency response plans that contain a range of procedures including evacuation, invacuation and dynamic lockdown.

- **Emergency Evacuation:** The immediate controlled exit from a building.
- **Emergency Invacuation:** Where keeping everyone inside the building is the safest option.
- **Dynamic Lockdown:** Where the threat/hazard has entered the building and there is a need to seal off the threat by locking the building down internally to prevent it from spreading.

The ability to recognise an emergency situation and then to respond to it quickly and effectively is of paramount importance. Research has shown that having an effective emergency plan will significantly reduce the amount of harm and damage an emergency incident will cause and will improve the

business's ability to recover quickly. An effective emergency plan will also reduce the impact an incident could have on your employees who may otherwise suffer from physical and mental health related issues, poor performance and poor attendance. Even if your business is affected by an incident or an attack, your reputation may actually be enhanced by the way in which you responded effectively and efficiently rather than undermined because you didn't have a plan. Plans need to be well constructed and aligned to your risks, regularly trained, reviewed and communicated effectively across the whole of your organisation.


In the UK the inclusion of a robust and effectively communicated Fire Emergency Evacuation Plan (FEPP) is a mandatory requirement under the terms laid out within the Health and Safety at Work Act 1974 and many other countries have similar regulations. Employers also have a responsibility to ensure a Personal

Emergency Evacuation Plan (PEEP) is designed into fire procedures to accommodate the needs of disabled employees, customers and visitors. A similar approach should also be adopted for the design and implementation of Emergency Response Plans (ERPs). The planning and implementation of robust and sustainable emergency response plans are essential elements for meeting your duty of care towards your staff, visitors and customers.

Your emergency plans should be designed to meet the types of risk identified through the security threat assessment referred to in the previous section. It is no longer acceptable to rely on an emergency fire plan to cover all the eventualities relating to emergency incidents or situations.

 For additional [HSE information click here](#)

Emergency plans and procedures must be designed to provide people with an enhanced opportunity to move away from sources of danger relating to the full spectrum of threats, including crime, accidents, terrorism, acts of aggression and natural disasters. You may also want to consider the use of mobile phone apps that enable you to track the precise location of all of your staff. Thereby enabling you to account for them during an emergency incident and potentially send them instructions on how best to respond.

The procedures you put in place should be as familiar to all staff as the emergency fire procedures and must be [tested and rehearsed at regular intervals throughout the year.](#) 

For further government guidance on [Dynamic Lockdown click here.](#) 

Risk management and emergency procedures

Emergency Management Plan

An Emergency Management Plan (EMP) is an essential part of any emergency response planning and enhances the safety and security of any organisation. The EMP deals specifically with the operational management of any incident, event or occurrence that fits within the definition of an emergency. An emergency will relate to any threat to people, infrastructure or business function within your organisation or business and can range from acts of terrorism to natural disasters.

The question has addressed terrorism specifically and an effective EMP will enable your organisation to take control of the situation quickly in order to:

- Provide staff, visitors and emergency responders with the confidence to act.
- Minimise the overall impact of the incident, event or occurrence.
- Formulate a proportionate and effective response to the situation.
- Establish command, control & communication to enhance the response.
- Address immediate priorities aligned to health, safety and security.
- Provide leadership & reduce fear, panic and confusion.
- Close the incident and return the organisation to normal operations as soon as possible.

In essence, an EMP allows trained personnel to quickly establish effective leadership, command and control of a potentially serious situation that could have negative effects on people, infrastructure and organisational processes. The Emergency Management Plan (EMP) should not however be mistaken for a Business Continuity Plan (BCP). Additional information can be accessed below:

 [Business Continuity Institute \(BCI\) - emergency planning](#)

[British Standards Institute \(BSI\) - business continuity](#)

[Centre for the Protection of National Infrastructure \(CPNI\) - business continuity planning](#)

Risk management and emergency procedures

Business Continuity Plan

A Business Continuity Plan (BCP) should, ideally, conform to ISO 22301. It is an essential part of an organisation's response and resilience planning and should set out how the business will operate following any serious incident that may impact on the core and supporting business functions and how you return to 'business as usual' in the quickest possible time afterwards. Your plan should not be specific to terrorist incidents and can apply to any significant disruption such as a major fire, flooding or a 'Force Majeure' event. It should set out the agreed arrangements for bringing events under control, the necessary resources for maintaining critical business functions and the staff required for coordinating actions.

The BCP also needs to be clearly presented, avoiding vague internal references and abbreviations, and structured in such a way that people can quickly find and understand what is expected of them. Effective Business Continuity Plans will differ depending on the business but all BCPs should include:

- A specific threat, vulnerability and risk profile for the business
- An understanding of possible and likely impact from risks
- Desired responses to any incident and how these will be achieved
- Preparation and initial planning considerations
- A communication plan
- A resilience strategy and an anticipated timeline
- Longer term planning considerations
- BCP roles, appointments, training and equipment.

BCPs should not become complex or reliant upon individual personalities and should be rehearsed and tested annually by those who will be expected to play a part in the plan's implementation. In the UK the following guidance is available:

 [BSI Group](#)
[CPNI](#)

Risk management and emergency procedures

Search Plans

When required, an effective Search Plan is a valuable process which can be initiated quickly and, if properly trained and rehearsed, executed with a minimum of disruption and delay. A Search Plan will most likely be implemented as a response to a threat that an explosive device or other potentially harmful item has been hidden or placed at your site. It can also be effective in helping to recover lost property or locate lost children or vulnerable persons who may have become ill or disorientated whilst at your premises. In the UK the police service will expect you to conduct a search of your site before police personnel are deployed there.

Disgruntled and former employees, business competitors, protest groups, disaffected individuals and those with mental health issues have all used the placement of device(s)

as a tactic to cause disruption, fear and harm to the business they have chosen to target. The threat itself is often a hoax, with the disruption caused by a site evacuation being the desired outcome.

Unfortunately, no such threat can be considered a hoax until it has been checked out.

A Search Plan will allow for a structured and rapid check of your building or buildings and quickly establish if there is a need for an evacuation or other emergency response. A hoax situation can be identified and resolved in a short period and the hoaxer will not be rewarded with the sight of a full emergency response. If you do not rehearse and review your plans, ideally at least once a year, then you cannot expect them to run smoothly

in an emergency. Your search personnel will not be confident in their roles which may result in them making mistakes which could in turn mean a genuine device is not located. Devise and implement a training and rehearsal regime as a matter of priority. Ensure you build resilience into your Search Plan through regular training, with several people responsible for each defined search area to cater for absences through holiday, illness, training and secondment. If you re-organise, re-develop or extend your facilities you will need to review and amend your Search Plan. Following any changes to your plan, you must test and review the amended plan to eliminate any errors and optimise its effectiveness.

Risk management and emergency procedures

Mailrooms

Best practice in mail handling is to operate a dedicated mailroom facility which is located away from your critical assets and away from your staff and busy areas of your business. Ideally this will be a standalone building which is completely isolated from the rest of your site and should be located at the perimeter, allowing for the delivery of items without the need for external third-party delivery vehicles to enter your site at all. If you have large quantities of mail then these can be distributed around your site after screening, using internal 'trusted' vehicles and/or mail bags/mail carts. If necessary, these can be further protected by numbered security tags applied at the mailroom and removed by the intended recipient at the point of final delivery. Should your site be the unfortunate recipient of explosive,

hazardous or incendiary devices which are then opened or initiated then the damage should be limited to your mail room only and the effect on the rest of your site and your business should be limited.

Dedicated mailrooms must incorporate safety and security elements that cater for a whole range of potential hazards. Air conditioning/air handling equipment must be housed separately from other site systems and there must be the ability to switch it off from within the mailroom and from a control room or using separate switchgear outside the mailroom. The ability to switch off the air conditioning/air handling equipment is essential in order to limit the spread of a contaminating agent or noxious substance. When such items have been identified, there needs to be a designated space where they can be placed

securely and which can be accessed by specialist responders, such as Explosive Ordnance Disposal (EOD) personnel who may deploy with their specialist equipment. Mail handling personnel must be provided with appropriate personal protective equipment and washing/changing facilities to minimise the effects of a contaminant upon them and the likelihood of them spreading a contaminant elsewhere. A dedicated mailroom should operate efficiently as a specialist environment and when properly designed is a valuable addition to your safety and security, especially at large and high security venues.

All staff who are expected to handle mail should be trained to PAS 97:2015 standard. Any organisation which receives unscreened mail, including internal items and parcels, directly at its premises is potentially vulnerable to the threat from explosive, incendiary or

other harmful devices or materials arriving by post or courier. Large organisations receive and handle thousands of items each day, often several times a day, and screening all of these represents a major commitment to ensuring continued safety. Trained mail handlers should be able to recognise the common indicators for suspicious mail, including unusual odours, irregular package shapes or protrusions, staining, leakage, poor spelling or partial names and addresses and excessive postage charges. If your venue handles large amounts of mail, then handlers will need to be provided with suitable commercial off the shelf (COTS) screening equipment and you should ensure it has been properly accredited for its performance by an independent testing authority.

Most systems offer a variation of X-Ray examination, but be aware that systems which have been

Risk management and emergency procedures

Mailrooms continued

deployed to detect a range of materials, such as explosives, will compare scanned items to an internal library or database of known materials, limiting their detection capabilities to the contents of their library, which may not be up to date. Scanning equipment is also costly, requires specialist maintenance and calibration, takes up a significant amount of space and personnel will need specific training to operate it efficiently. Operator fatigue is a limiting performance factor too, so you will need to deploy enough trained personnel to rotate them often if you want to minimise the risk of suspicious items being missed. Operator training must include a response plan so there are clear instructions on what to do when different types of suspicious mail are identified.

The plan must include the ability to contact the emergency services and any EOD team that may

cover your location. Keep your training content up to date and be aware of developments in delivery methodology such as the use of drones. Drone technology is increasingly being used as a commercial delivery platform by major organisations, particularly online retailers, and is likely to feature in your mail and parcel delivery in the future if it hasn't done so already. Drones can carry parcels of several kilos in weight so this is an area of concern and should not be left unaddressed. Ensure your own staff are not utilising your business address for the delivery of personal parcels, again a particular problem arising from online shopping, as this can also represent an unnecessary risk. More information [from CPNI can be found here](#).



Terrorism Threat Levels

The threat from terrorism is serious, but it is important to keep it in perspective. The main threat comes principally from DAESH (also known as ISIL), Al Qaeda, and groups and individuals who can be directed, encouraged or inspired by them. The type and level of threat is complex and ranges from crudely planned but potentially well executed "lone wolf" style attacks to sophisticated networks pursuing ambitious and coordinated plots that are designed to cause mass casualties. There are, however, other terrorist threats that emanate from Extreme Right Wing organisations and Northern Irish Republican Terrorists. The threat level for the UK is determined by the Joint Terrorism Analysis Centre (JTAC) and ranges from Low to Critical where a terrorist attack is highly likely in the near future. More information about the terrorism threat from [PoolRe can be found here](#).



The threat levels are now defined as follows:

- Low - an attack is highly unlikely (changed from "unlikely")
- Moderate - an attack is possible but not likely
- Substantial - an attack is likely (changed from "a strong possibility")
- Severe - an attack is highly likely
- Critical - an attack is highly likely in the near future (changed from "expected imminently")

See here further guidance on the threat levels and on the [terrorist threat from MI5](#).



Risk management and emergency procedures

Other Police Resources

Project ARGUS which is a counter terrorism testing and exercising initiative, delivered by [Counter Terrorism Security Advisers and Counter Terrorism Awareness Advisers. NaCTSO.](#)

Taking the opportunity to attend a session will enable you to gain a better understanding of the threat from terrorism and of simple security measures that can be taken to protect a business or an organisation.

Participants from business and other organisations are asked to consider their preparedness for a terrorist attack through a series of simulated multi-media scenarios. The aim is to identify measures to help their organisation to prevent, manage and recover from a terrorist incident.

Project ARGUS explores what is likely to happen in the event of a terrorist attack. It highlights the importance of being prepared and

having the necessary plans in place to help safeguard staff, visitors and assets. All events include a module on a terrorist firearm or weapons attack.

The events are free of charge and last for approximately three hours. They are interactive and require some audience participation. An expert group will be in attendance at most events consisting of members from the emergency services, local authority and other specialist agencies to answer any queries. [There are currently nine Project ARGUS topics.](#)

ACT Strategic is a new initiative which aids businesses to explore ways of preventing, managing, and recovering from a terrorist attack. ACT Strategic is aimed at those responsible for writing policies and procedures or strongly influencing them. Events are aimed at 20-30 delegates from a range of organisations and business sectors.

i Delegates are asked to have completed the [ACT E-learning package](#) and have knowledge of their organisation's emergency response plans (incident management plan, recovery and business continuity plan) and the authority to affect changes or reviews of those plans (i.e. heads of department, security managers or emergency planners). To find out more [visit the gov.uk website.](#)

i ACT Awareness is an e-Learning training opportunity that has been developed by NaCTSO to help businesses better understand and mitigate terrorist methodology and to protect our cities and communities from [the threat of terrorism \[NaCTSO\]](#).

The following eLearning Modules are available through ACT Awareness:

- Introduction to Terrorism
- Identifying Security Vulnerabilities
- How to Identify and Respond to Suspicious Behaviour
- How to Identify and Deal with a Suspicious Item
- What to do in the Event of a Bomb Threat
- How to Respond to a Firearms or Weapons Attack
- Summary and Supporting Materials

Risk management and emergency procedures

Other Police Resources continued

Stay Safe Film - Run, Hide, Tell, reminds us all of the terrorist threat we face in the UK and abroad. Police and security agencies are working tirelessly to protect the public, but it is also important that communities remain vigilant and aware of how to protect themselves if the need arises. National Counter Terrorism policing is providing advice to the public on the steps they can take to keep themselves safe in the rare event of a firearms or weapons attack.

The police service has released the short public information film called 'Stay Safe: Firearms and Weapons Attack' which sets out the key options for keeping safe should the worst happen. You can watch the film on the [National Police Chiefs' Council YouTube account](#).

Protect your organisation from a range of threats with SCaN training from NaCTSO and Centre for the Protection of National Infrastructure (CPNI).

See, Check and Notify (SCaN) aims to help businesses and organisations maximise safety and security using their existing resources. Your people are your biggest advantage in preventing and tackling a range of threats, including terrorism, criminal activity and protest.

SCaN helps ensure that individuals or groups seeking to cause your organisation harm are unable to get the information they need to plan their actions. It also empowers your staff to know what suspicious activity to look for and [what to do when they encounter it](#).



Risk management and emergency procedures

Conclusion

All businesses need to minimise the impact of an unexpected emergency and to recover from that emergency so as to resume normal operations as quickly as possible within what is commonly referred to as your 'Outage time'. These can only be achieved if you have first identified the potential threats to your business and how these can impact it; and second, put in place the requisite planning, preparation and training. To support these, you must also have the right organisational culture that recognises and values the importance of and the need for contingency planning; and the governance structure that ensures that people are responsible and accountable for the organisation's contingency plans. This section looked at these issues to help you consider the extent to which you have effective risk management, emergency and business continuity plans in place.



VSAT

Pool Re Offering

You are invited to participate in the use of the Vulnerability Self Assessment Tool (VSAT®). It is designed to help you self-assess your security in line with UK best practice as suggested by the Government's leading protective Security Agencies.

The tool is available for use (free of charge) to those Policyholders whose portfolios aggregate to a Material/ Property Damage declared value sum insured of £50m or above, and do not consist primarily of domestic properties (PDHs/Flats). If you are in doubt as to whether you meet the eligibility criteria, please discuss with your insurance broker or insurer.

Once you have completed the self-assessment process, you will be awarded a risk assessment score expressed as a Red Amber Green (RAG) rating and you will receive an online report that provides you with practical advice on the mitigating measures you can put in place to reduce any risks and vulnerabilities identified. The RAG rating will be commuted to a score and you may be eligible for a Loss Mitigation Credit (LMC) that will qualify you for a discount on your insurance. The results are entirely confidential and will remain so until you decide to share them with your insurer. Once shared with your insurer, they will assess the report and confirm whether a discount should be applied to your insurance premium. For further details, please consult your insurer or go [direct to VSAT](#)

Powered by VSAT®

arl Partners Ltd
www.arlpartners.co.uk

Additional information

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378443/28_09_CCTV_OR_Manual2835.pdf

<https://www.sia.homeoffice.gov.uk/Pages/licensing-cctv.aspx>

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

<https://videosurveillance.blog.gov.uk/tag/facial-recognition/>

<https://www.gov.uk/government/organisations/surveillance-camera-commissioner>

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

<https://www.redcare.bt.com>

<https://www.gov.uk/government/publications/developing-dynamic-lockdown-procedures>

<https://www.securityindustry.org/>

<https://www.cpni.gov.uk/system/files/documents/40/20/Integrated%20Security%20Guide.pdf>

<https://register-drones.caa.co.uk>

<https://www.cpni.gov.uk/counter-unmanned-aerial-vehicles>

<https://www.gov.uk/foreign-travel-advice>

<https://www.cpni.gov.uk/pre-employment-screening>

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

<http://www.actionfraud.police.uk/scam-emails>

<http://www.actionfraud.police.uk/fraud-az-vishing>

<https://ico.org.uk/media/about-the-ico/documents/1042330/cloud-computing-guidance-for-organisations.pdf>

<https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches>

<http://www.legislation.gov.uk/ukxi/2015/627/schedule/1/made>

<https://www.gov.uk/guidance/emergency-response-and-recovery>

<https://www.gov.uk/government/publications/developing-dynamic-lockdown-procedures>

<http://www.hse.gov.uk/toolbox/fire.htm>

https://www.thebci.org/training_provider/emergency-planning-college.html

<https://www.bsigroup.com/en-GB/iso-22301-business-continuity/>

<https://www.cpni.gov.uk/business-continuity-planning>

<https://www.bsigroup.com/en-GB/iso-22301-business-continuity/>

<https://www.cpni.gov.uk/business-continuity-planning/>

<https://www.poolre.co.uk/risk-awareness-resources/>

<https://www.mi5.gov.uk/threat-levels>

<https://www.cpni.gov.uk/system/files/documents/3f/b7/Introduction-to-PAS-97-2015.pdf>

<https://www.gov.uk/government/organisations/national-counter-terrorism-security-office>

<https://www.gov.uk/government/publications/project-argus/project-argus>

<https://www.gov.uk/government/news/act-awareness-elearning>

<https://www.gov.uk/government/news/act-strategic>

<https://www.gov.uk/government/news/act-awareness-elearning>

<https://www.youtube.com/watch?v=CYPyZ3ErFy0>

<https://www.gov.uk/government/news/security-training-package-empowers-staff-to-see-check-and-notify-scan>