Counter Terrorism Protective Security Advice

for your business outside of the UK

Foreign & Commonwealth Office

produced by

NaCTSO

National Counter Terrorism Security Office

foreword

Foreign & Commonwealth Office

The Foreign and Commonwealth Office – 'the FCO' or 'the Foreign Office' for short – is the United Kingdom's Government department responsible for promoting British interests overseas and supporting our citizens and businesses around the globe.

The FCO does this by pursuing an active and activist foreign policy, working with other countries and strengthening the rules-based international system in support of our values to:

- Safeguard Britain's national security by countering terrorism and weapons proliferation, and working to reduce conflict.
- Build Britain's prosperity by increasing exports and investment, opening markets, ensuring access to resources, and promoting sustainable global growth.
- Support British nationals around the world through modern and efficient consular services.

NaCTSO
National Counter Terrorism Security Office

The National Counter Terrorism Security Office (NaCTSO), on behalf of the Association of Chief Police Officers, Terrorism and Allied Matters (ACPO TAM), works in partnership with the Security Service to reduce the impact of terrorism in the United Kingdom by:

- Protecting the UK's most vulnerable and valuable sites and assets.
- Enhancing the UK's resilience to terrorist attack.
- Delivering protective security advice across the crowded places sector.

NaCTSO aims to:

- Raise awareness of the terrorist threat and the measures that can be taken to reduce risks and mitigate the effects of an attack.
- Co-ordinate national service delivery of protective security advice through the Counter Terrorism Security Adviser network and monitor its effectiveness.
- Build and extend partnerships with communities, police and government stake holders.
- Contribute to the development of the Counter Terrorism policy and advice.

contents

one introduction

This guide provides protective security advice to those who own, operate, manage or work within various businesses outside of the UK including Hotels, Restaurants, Bars, Shopping Centres, Tourism and Transport. It is aimed at those premises where there may be a risk of a terrorist attack either because of the nature of the business, its location, or the number of people who work there. These premises will be referred to as **'your business'** throughout this guide.

It is accepted that the concept of absolute security is almost impossible to achieve in combating the threat of terrorism, but it is possible, through the use of this guide, to reduce the risk to as low as is reasonably practicable.

Terrorist attacks world wide are a real and serious danger. The attacks indicate that terrorists continue to target crowded places as they are usually locations with limited protective security measures, and therefore afford the potential for mass fatalities and casualties. Furthermore, these incidents identify that terrorists are prepared to use vehicles as a method of attack, to ensure delivery of a large improvised explosive device (I.E.D.) as close to their target as possible.

Your type of business worldwide has been subject to terrorist attacks on several occasions, so it is possible that you could be involved in a terrorist incident. This might include having to deal with a bomb threat or with suspicious items left in or around your premises, or delivered to your premises.

In the worst case scenario your staff and customers could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and co-ordinated terrorist attack, and this would have a detrimental effect on your reputation.

It is recognised that there is a need to maintain a friendly and welcoming atmosphere within your business and the surrounding area, so it is important to state that this guide is not intended to create a 'fortress mentality'. There is however a balance to be achieved where those responsible for security are informed that there are robust protective security measures available to mitigate against the threat of terrorism, e.g. protection from flying glass and vehicle access controls into crowded areas, goods and service yards and underground car parks.

Terrorism can come in many forms, not just a physical attack on life and limb. It can include interference with vital information or communication systems, causing disruption and economic damage. Some attacks are easier to carry out if the terrorist is assisted by an 'insider' or by someone with specialist knowledge or access. Terrorism also includes threats or hoaxes designed to frighten and intimidate your staff.

two managing the risks

Managing the risk of terrorism is only one part of a manager's responsibility when preparing contingency plans in response to any incident in or near their premises which might prejudice public safety or disrupt normal operations.

Basic principles regarding the risk assessment process involves making logical assumptions about the likelihood of a threat and its impact, should current security measures fail to protect it. Though it is not possible to predict all possible threats to your business, by working through a range of potential scenarios and consequences it becomes possible to make informed judgements about the priorities for your business.

It is advised that you carry out the following:

- Carry out adequate **risk assessments** and put suitable measures in place to manage those identified risks, even where they are not of your making and are outside your direct control. Then be alert to the need to conduct prompt and regular reviews of those assessments and measures in light of new threats and developments.
- **Co-operate and co-ordinate** safety arrangements between owners, managers, security staff, tenants and others involved with the business, including the sharing of incident plans and working together in testing, auditing and improving planning and response. **The commercial tensions which naturally arise between landlords and tenants, and between neighbouring organisations that may well be in direct competition with each other, must be left aside entirely when planning protective security.**
- **Ensure adequate training, information and equipment** are provided to all staff, and especially to those involved directly in safety and security.
- Put proper procedures and competent staff in place to deal with incidents which might cause **imminent and serious danger** and/or, require evacuation of the premises.

Business continuity

Business continuity planning is essential in ensuring that your business can cope with an incident or attack and return to **'business as usual'** as soon as possible. An attack on a crucial contractor or supplier can also impact on business continuity. You can develop a basic plan, which can be implemented to cover a wide range of possible actions. For example, part of the plan will cover evacuation procedures, but the principles will be generally applicable for fire, flooding, or bomb threat incidents. This is particularly relevant for smaller enterprises that may not have the resources to withstand even a few days financial loss.

Reputation and goodwill are valuable, but prone to serious and permanent damage if it turns out that you gave a less than robust, responsible and professional priority to best protecting people against attack. Being security minded and better prepared reassures your customers and staff that you are taking security issues seriously and could potentially deter an attack.

Do you know who your neighbours are and the nature of their business? Could an incident at their premises affect your operation? There is limited value in safeguarding your own premises in isolation. Take into account your neighbours' business plans and those of the local authorities with responsibility for security.

A number of organisations have adopted good practice to enhance the protective security measures in and around their premises. This document identifies and complements such good practice.

This guide recognises that your business may differ in many ways including, size, location, staff numbers, layout and operation and that some of the advice included in this document may have already been introduced at some locations.

For specific advice relating to your business, contact your local government and local business associations including local authorities responsible for security. Also refer to Useful Contacts on page 62.

It is essential that all the work you undertake on protective security is progressed in partnership with your local authorities as appropriate, and with your neighbours.

It is worth remembering that measures you may consider for countering terrorism will also usually be effective against other threats, such as theft and burglary. Any extra measures that are considered should integrate wherever possible with existing security.

With regard to protective security, the best way to manage the hazards and risks to your business is to start by understanding and identifying the threats, vulnerabilities and resulting business impact.

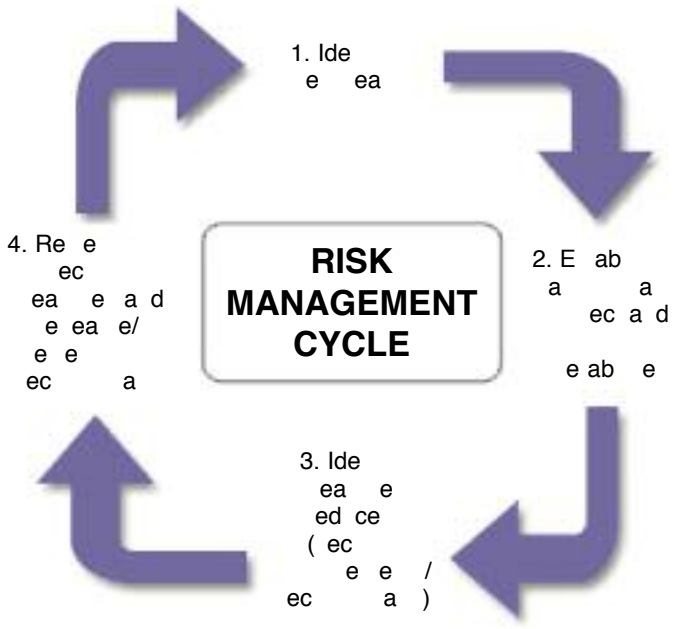
This will help you to decide:

- What security improvements you need to make.
- What type of security and contingency plans you need to develop.

For some businesses, simple good practice - coupled with vigilance and well exercised contingency arrangements - may be all that is needed.

If, however, you assess that you are vulnerable to attack, you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable.

The following diagram illustrates a typical risk management cycle:



Step One: Identify the threats.

Understanding the terrorist's intentions and capabilities - what they might do and how they might do it - is crucial to assessing threat. Ask yourself the following questions:

- What can be learnt from local government, local business associations including local authorities responsible for security and the media about the current security climate, or about recent terrorist activities? See Useful Contacts on page 62.
- Is there anything about the location of your premises, its visitors, sponsors, contractors, occupiers and staff, or your activities that would particularly attract a terrorist attack?
- Is there an association with high profile individuals or organisations which might be terrorist targets?
- Do you have procedures in place and available for deployment on occasions when VIPs attend any events at your location?
- Does your location mean you could suffer collateral damage from an attack or other incident at a 'high risk' neighbouring premises?
- What can your local government and local business associations, including local authorities, responsible for security tell you about crime and other problems in your area?
- Is there any aspect of your business or activities that terrorists might wish to exploit to aid their work, e.g. plans, technical expertise or unauthorised access?
- Are the building / floor plans for your premises published or publicly available?
- Do you communicate information about the threat and response levels to your staff?

Step Two: Decide what you need to protect and identify your vulnerabilities.

Your priorities for protection should fall under the following categories:

- People (staff, visitors, customers, contractors, general public)
- Physical assets (buildings, contents, equipment, plans and sensitive materials)
- Information (electronic and paper data)
- Processes (supply chains, critical procedures) - the actual operational process and essential services required to support it.

You know what is important to you and your business. It may be something tangible - for example, the data suite where all your transactions are recorded, the IT system or a piece of equipment that is essential to keep your business running. You should already have plans in place for dealing with fire and crime, procedures for assessing the integrity of those you employ, protection from IT viruses, and measures to secure parts of the premises.

Review your plans on a regular basis and if you think you are at greater risk of attack, perhaps because of the nature of your business or the location of your premises, then consider what others could find out about your vulnerabilities, such as:

- Information about you that is publicly available, e.g. on the internet or in public documents
- Anything that identifies installations or services vital to the continuation of business in your premises

- Any prestigious targets that may be attractive to terrorists, regardless of whether their loss would result in business collapse
- You should have measures in place to limit access into non - public areas of your premises; and vehicle access control measures into goods and service areas.

As with Step One, consider whether there is an aspect of your business or activities that terrorists might want to exploit to aid or finance their work. If there are, how stringent are your checks on the people you recruit? Are your staff security conscious?

It is important that your staff can identify and know how to report suspicious activity. See hostile reconnaissance on page 19.

Step Three: Identify measures to reduce risk

An integrated approach to security is essential. This involves thinking about physical security, information security and personnel security (i.e. good recruitment and employment practices). There is little point investing in costly security measures if they can be easily undermined by a disaffected member of staff or by a poor recruitment process.

Remember, TERRORISM IS A CRIME. Many of the security precautions typically used to deter criminals are also effective against terrorists. So before you invest in additional security measures, review what you already have in place. You may already have a good security regime - on which you can build.

If you need additional security measures, then make them most cost-effective by careful planning wherever possible. Introduce new equipment or procedures in conjunction with building work. In multi-occupancy buildings, try to agree communal security arrangements.

Even if organisations / businesses surrounding your location are not concerned about terrorist attacks, they will be concerned about general crime - and your security measures will help protect against crime as well as terrorism.

Staff may be unaware of existing security measures, or may have developed habits to circumvent them, e.g. short cuts through fire exits. Simply reinstating good basic security practices and regularly reviewing them will bring benefits at negligible cost.

Step Four: Review your security measures and rehearse and review security and contingency plans.

You should regularly review and exercise your plans to ensure that they remain accurate, workable and up to date.

Rehearsals and exercises should wherever possible, be conducted in conjunction with all partners, emergency services and local authorities.

Make sure that your staff understand and accept the need for security measures and that security is seen as part of everyone's responsibility, not merely something for security experts or professionals. Make it easy for people to raise concerns or report observations.

IT SHOULD BE REMEMBERED THAT THE GREATEST VULNERABILITY TO ANY ORGANISATION IS COMPLACENCY.

three security planning

It is recognised that for many businesses, responsibility for the implementation of protective security measures following a vulnerability and risk assessment will fall on a security manager within the centre, who must have sufficient authority to direct the action taken in response to a security threat.

The security manager must be involved in the planning of the premises' perimeter security, access control, contingency plans etc, so that the terrorist dimension is taken into account. The responsible person must similarly be consulted over any new building or renovation work so that counter terrorism specifications, e.g. concerning glazing and physical barriers can be factored in, taking into account any local planning and safety regulations.

The person responsible for security of your business should already have responsibility for most, if not all, of the following key areas:

- The production of the security plan based on the risk assessment
- The formulation and maintenance of a search plan
- The formulation and maintenance of other contingency plans dealing with bomb threats, suspect packages and evacuation
- Liaising with the police, and the local authorities responsible for security
- Arranging staff training, including his/her own deputies and conducting briefings/debriefings
- Conducting regular reviews of the plans.

For counter terrorism advice and guidance that is site specific, the Security Manager should establish contact with the local government and business associations, and local authorities responsible for security. Also refer to Useful Contact page on page 62.

They may give advice to:

- Help you assess the threat, both generally and specifically
- Give advice on physical security equipment and its particular application to the methods used by terrorists
- Offer advice and assistance with risk assessments
- Identify vulnerabilities and advise on reducing them
- Identify appropriate trade bodies for the supply and installation of security equipment
- Offer advice on search plans

Creating your Security Plan

The Security Manager should aim to produce a plan that has been fully exercised, and which is regularly audited to ensure that it is still current and workable.

Before you invest in additional security measures, review what is already in place, including known weaknesses such as blind spots in any CCTV system.

When creating your security plan, consider the following:

- Details of all the protective security measures to be implemented including physical, information and personnel security
- Instructions on briefing content to security staff including the type of behaviour to look for
- Instructions on how to respond to a threat (e.g. telephone bomb threat)
- Instructions on how to respond to the discovery of a suspicious item or event
- A search plan
- Evacuation plans and details on securing the premises in the event of a full evacuation
- Your business continuity plan
- A communications and media strategy which includes handling enquiries from concerned family and friends.

Your planning should incorporate the seven key instructions applicable to most incidents:

1. **Do not touch suspicious items.**
2. **Move everyone away to a safe distance.**
3. **Prevent others from approaching.**
4. **Communicate safely to staff, business visitors and the public.**
5. **Use hand-held radios or mobile phones away from the immediate vicinity of a suspect item, remaining out of line of sight and behind hard cover.**
6. **Notify the police.**
7. **Ensure that whoever found the item or witnessed the incident remains on hand to brief the police.** **See Reporting Incidents on page 58.**

Effective security plans are simple, clear and flexible, but must be compatible with any existing plans e.g. evacuation plans and local fire safety strategies. Everyone must be clear about what they need to do in a particular incident. Once made, your plans must be followed, other than when exceptional circumstances dictate otherwise.

four physical security

Physical security is important in protecting against a range of threats and addressing vulnerability.

Put in place security measures to remove or reduce your vulnerabilities to as low as reasonably practicable bearing in mind the need to consider safety as a priority at all times. Security measures must not compromise public safety.

Your risk assessment will determine which measures you should adopt, but they range from basic good housekeeping (keeping communal areas clean and tidy) through mitigation against flying glass, CCTV, perimeter fencing, intruder alarms, computer security and lighting, to specialist solutions such as mail scanning equipment.

Specialist solutions, in particular, should be based on a thorough assessment – not least because you might otherwise invest in equipment which is ineffective, unnecessary and expensive.

Successful security measures require:

- The support of your senior management.
- Staff awareness of the measures and their responsibilities in making them work.
- A senior, identified person within your organisation having responsibility for security.

Security awareness

The vigilance of your staff (including cleaning, maintenance and contract staff) is essential to your protective measures. They will know their own work areas or offices very well and should be encouraged to be alert to unusual behaviour or items out of place.

They must have the confidence to report any suspicions, knowing that reports – including false alarms – will be taken seriously and regarded as a contribution to the safe running of the commercial centre.

Training is therefore particularly important. Staff should be briefed to look out for packages, bags or other items in odd places, carefully placed (rather than dropped) items in rubbish bins and unusual interest shown by strangers in less accessible places.

See Hostile Reconnaissance on page 19.

Access control

An efficient reception area is essential to controlling access, with side and rear entrances denied to all but authorised people.

Keep access points to a minimum and make sure the boundary between public and private areas of your building is secure and clearly signed. Ensure there are appropriately trained and briefed staff to manage access control points or alternatively invest in good quality access control systems operated by magnetic swipe or contact proximity cards supported by Personal Identification Number (PIN) verification.

See Access Control Guidance on page 24.

Security passes

Consider introducing a pass system if you do not already have one. If a staff pass system is in place, insist that staff wear their passes at all times and that the issuing is strictly controlled and regularly reviewed. Visitors to private areas should be escorted and should wear clearly marked temporary passes, which must be returned on leaving. Anyone not displaying security passes in private areas should either be challenged or reported immediately to security or management.

Screening and Patrolling

Random screening of hand baggage is a significant deterrent that may be a suitable protective security consideration for your premises.

The routine searching and patrolling of your premises represents another level of vigilance covering both internal and external areas. Keep patrols regular, though not too predictable (i.e. every hour on the hour). See Search Planning on page 29.

Traffic and parking controls

If you believe you might be at risk from a vehicle bomb, the basic principle is to keep all vehicles as far from your building as practical. Those requiring essential access should be identified in advance and checked before being allowed through. If possible, you should ensure that you have proper access control, careful landscaping, traffic-calming measures and robust, well-lit barriers or bollards. Ideally, keep non-essential vehicles at least 30 metres from your building.

See also Vehicle Borne Improvised Explosive Devices on page 38.

Doors and windows

Good quality doors and windows are essential to ensure building security. External doors should be strong, well-lit and fitted with good quality locks. It should also be remembered that glazed doors are only as strong as their weakest point – which may be the glass itself. Doors that are not often used should be internally secured ensuring compliance with relevant fire safety regulations and their security monitored with an alarm system. **This is particularly important where an external search / screening operation is present in order to prevent unauthorised entry and bypassing any search regime.**

- As a minimum, accessible windows should be secured with good quality key operated locks. See Useful Contact page on page 62 who may provide further advice on improving the security of glazed doors and accessible windows.
- Many casualties in urban terrorist attacks are caused by flying glass, especially in modern buildings, and glazing protection is an important casualty reduction measure.
- Extensive research has been carried out on the effects of blast on glass. There are technologies that minimise shattering and therefore casualties as well as the cost of re-occupation.

- Anti-shatter film, which holds fragmented pieces of glass together, offers a relatively cheap and rapid improvement to existing glazing. If you are building a new structure and are installing windows, consider laminated glass, but before undertaking any improvements seek specialist advice through the Useful Contact page on page 62, and visit www.cpni.gov.uk for further details.

Integrated security systems

Intruder alarms, Closed Circuit Television (CCTV) and lighting are commonly used to deter crime, detect offenders and delay their actions. All these systems must be integrated so that they work together in an effective and co-ordinated manner.

Intrusion detection technology can play an important role in an integrated security system, it can be as much a deterrent as a means of protection.

Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations, but only if the images are good enough to identify what happened and be used in any post incident investigation.

External lighting provides an obvious means of deterrence as well as detection, but take into account the impact of additional lighting on your neighbours. If it is carefully designed and used, external lighting will help security staff and improve the capabilities of CCTV systems.

Remember that CCTV is only effective if it is properly monitored and maintained.

See CCTV guidance on page 25.

five evacuation planning and protected spaces

As with search planning, evacuation should be part of your security plan. You might need to evacuate your business because of:

- A **threat received directly to your business**.
- A **threat received elsewhere** and passed on to you by the police.
- **Discovery of a suspicious item in your business** (perhaps a postal package, an unclaimed hold-all or rucksack).
- **Discovery of a suspicious item or vehicle outside your building**.
- **An incident** to which the police have alerted you.

Whatever the circumstances, you should tell the police as soon as possible what action you are taking.

The biggest dilemma facing anyone responsible for an evacuation plan is how to judge where the safest place might be. For example, if an evacuation route takes people past a suspect device outside your building, or through an area believed to be contaminated, external evacuation may not be the best course of action.

A very important consideration when planning evacuation routes in response to near simultaneous terrorist attacks is to ensure people are moved away from other potential areas of vulnerability, or areas where a larger secondary device could detonate.

The decision to evacuate may be yours, however the local authorities may also advise. In exceptional cases they may insist on evacuation, although they should always do so in consultation with your Security Manager.

A general rule of thumb is to find out if the device is external or internal to your premises. If it is within the building you may consider evacuation, but if the device is outside the building it may be safer to stay inside.

Planning and initiating evacuation should be the responsibility of the Security Manager. Depending on the size of your premises and the location of the building, the plan may include:

- Full evacuation outside the building.
- Evacuation of part of the building, if the device is small and thought to be confined to one location (e.g. a small bag found in an area easily contained).
- Full or partial evacuation to an internal safe area, such as a protected space, if available.
- Evacuation of all staff apart from designated searchers.

Evacuation

Evacuation instructions must be clearly communicated to staff and routes and exits must be well defined. People must be appointed to act as marshals and as contacts once the assembly area is reached. Assembly areas should be at least 500 metres away from the incident. In the case of most vehicle bombs, for instance, this distance would put them beyond any police or military cordons – although it would be advisable to have an alternative about 1km away.

It is important to ensure that staff are aware of the locations of assembly areas for incident evacuation as well as those for fire evacuation and that the two are not confused by those responsible for directing members of the public to either.

Grab bags

'Grab Bags' should be available in key locations, which contain essential equipment and information. All relevant contact information, the staff involved, tenants and other site information should be contained in an easily accessible format.

Suggested 'Grab Bag' contents:

Items you could consider including in a grab bag sometimes known as a battle or incident box.

Equipment:

- First aid kit (designed for major emergencies) consider large bandages, burn shields or cling film, large sterile strips, cold packs, baby wipes as well as standard first aid equipment.
- Torch and spare batteries or wind up
- Emergency and Floor plans (laminated)
- List of Contacts (laminated) staff etc
- Incident Log (consider dictaphone), notebook, pens, markers, etc
- Glow sticks
- Radio (wind up)
- High visibility jackets
- Loud hailer and spare batteries
- Hazard and cordon tape
- Plastic macs / foil blankets / bin liners
- Dust / toxic fume masks
- Water (plastic container) and chocolate/glucose tablets
- Computer back up tapes / disks / USB memory sticks or flash drives (see extra documents to be stored below)

Some extra items you could consider:

- Spare keys / security codes
- Mobile telephone with credit available, plus charger (wind up if possible).

- Disposable / small camera.
- Hard hats / protective goggles / heavy duty gloves

Documents which can be electronically stored if accessible, otherwise paper copy should be readily available:

- Business Continuity Plan - your plan to recover your business or organisation.
- Communication strategy, signage and messaging
- List of employees with contact details - include home and mobile numbers. You may also wish to include next-of-kin contact details.
- Lists of customer and supplier details.
- Contact details for emergency glaziers and building contractors.
- Contact details for utility companies.
- Building site plan, including location of gas, electricity and water shut off points.
- Latest stock and equipment inventory.
- Insurance company details.
- Local authority contact details.

See Useful Contact page on 62.

Make sure this pack or packs are stored safely and securely on site or at an accessible emergency location nearby. Ensure items in the pack are checked regularly, are kept up to date, and are working. Remember that cash / credit cards may be needed for emergency expenditure.

This list is not exhaustive, and there may be other documents or equipment that should be included for your business or organisation.

Car parks should not be used as assembly areas and furthermore, assembly areas should always be searched before they are utilised.

Disabled staff should be individually briefed on their evacuation procedures.

In the case of suspected:

Letter or parcel bombs

If in a premises, evacuate the room and the floor concerned and the adjacent rooms along with the two floors immediately above and below.

Chemical, Biological and Radiological Incidents (CBR)

Responses to CBR incidents will vary more than those involving conventional or incendiary devices, but the following general points should be noted:

- The exact nature of an incident may not be immediately apparent. For example, an Improvised Explosive Device (IED) might also involve the release of CBR material.
- In the event of a suspected CBR incident within a building, switch off all air conditioning, ventilation and other systems or items that circulate air (e.g. fans and personal computers). Do not allow anyone, whether exposed or not, to leave evacuation areas before the emergency services have given medical advice, assessments or treatment.
- If an incident occurs outside an enclosed temporary structure or building, close all doors and windows and switch off any systems that draw air into the structure/building.

Agree your evacuation plan in advance with the local emergency services and local authorities. Ensure that staff with particular responsibilities are trained, and that all staff are aware of your evacuation plan. Remember to let the local authorities know what action you are taking during any incident.

Security managers should ensure that they have a working knowledge of the heating, ventilation and air conditioning (HVAC) systems and how these may contribute to the spread of CBR materials within the building. (**Can you turn off your systems?**)

Protected Spaces

Protected spaces may offer the best protection against blast, flying glass and other fragments. They may also offer the best protection when the location of the possible bomb is unknown, when it may be near your external evacuation route or when there is an external CBR attack.

Since glass and other fragments may kill or maim at a considerable distance from the centre of a large explosion, moving staff into protected spaces is often safer than evacuating them onto the streets. Protected spaces should be located:

- In areas surrounded by full – height masonry walls e.g. internal corridors, toilet areas or conference rooms with doors opening inwards.
- Away from windows and external walls.
- Away from the area in between the building's perimeter and the first line of supporting columns (known as the 'perimeter structural bay').
- Away from stairwells or areas with access to lift shafts where these open at ground level onto the street, because blast can travel up them. If, however, the stair and lift cores are entirely enclosed, they could make good protected spaces.
- Avoiding ground floor or first floor if possible.
- In an area with enough space to contain the occupants.

When choosing a protected space, seek advice from a structural engineer with knowledge of explosive effects and do not neglect the provision of toilet facilities, seating, drinking water, lighting and communications.

Consider duplicating critical systems or assets in other buildings at a sufficient distance to be unaffected in an emergency that denies you access to your own. If this is impossible, try to locate vital systems in part of your building that offers similar protection to that provided by a protected space.

Communications

Ensure that staff know their security roles and that they or their deputies are always contactable. All staff, including night or temporary staff, should be familiar with any telephone recording, redial or display facilities and know how to contact your local police and security staff in or out of office hours.

It is essential to have adequate communications within and between protected spaces. You will at some stage wish to give the 'all clear', or tell staff to remain where they are, to move to another protected space or evacuate the building. Communications may be by public address system (in which case you will need standby power), hand-held radio or other

standalone systems. Do not rely on mobile phones. You also need to communicate with the emergency services. Whatever systems you choose should be regularly tested and available within the protected space.

Converting to open plan

If you are converting your building to open plan accommodation, remember that the removal of internal walls reduces protection against blast and fragments.

Interior rooms with reinforced concrete or masonry walls often make suitable protected spaces as they tend to remain intact in the event of an explosion outside the building. If corridors no longer exist then you may also lose your evacuation routes, assembly or protected spaces, while the new layout will probably affect your bomb threat contingency procedures.

When making such changes, try to ensure that there is no significant reduction in staff protection, for instance by improving glazing protection. If your premises are already open plan and there are no suitable protected spaces, then evacuation may be your only option.

six hostile reconnaissance

The ability to recognise those engaged in hostile reconnaissance could disrupt an attack and produce important intelligence leads.

Primary Role of Reconnaissance

- Obtain a profile of the target location.
- Determine the best method of attack.
- Determine the optimum time to conduct the attack.

Hostile reconnaissance is used to provide information to operational planners on potential targets during the preparatory and operational phases of terrorist attack planning.

Reconnaissance operatives may visit potential targets a number of times prior to the attack. Where pro-active security measures are in place, particular attention is paid to any variations in security patterns and the flow of people in and out.

What to look for.

- Significant interest being taken in the outside of your premises including parking areas, delivery gates, doors and entrances.
- Groups or individuals taking significant interest in the location of CCTV cameras and controlled areas.
- People taking pictures – filming – making notes – sketching of the security measures at your location. **Tourists should not necessarily be taken as such and should be treated sensitively, but with caution**.
- Overt/covert photography, video cameras, possession of photographs, maps, blueprints etc, of critical infrastructures, electricity transformers, gas pipelines, telephone cables etc.
- Possession of maps, global positioning systems, (GPS), photographic equipment, (cameras, zoom lenses, camcorders). GPS will assist in the positioning and correct guidance of weapons such as mortars and Rocket Propelled Grenades (RPGs). This should be considered a possibility up to one kilometre from any target.
- Vehicles parked outside buildings of other facilities, with one or more people remaining in the vehicle, for longer than would be considered usual.
- Parking, standing or loitering in the same area on numerous occasions with no apparent reasonable explanation.
- Prolonged static surveillance using operatives disguised as demonstrators, street sweepers, etc or stopping and pretending to have car trouble to test response time for emergency services.
- Simple observation such as staring or quickly looking away.
- Activity inconsistent with the nature of the building.

- Unusual questions – number and routine of staff / VIPs in residence.
- Individuals that look out place for any reason.
- Individuals that appear to be loitering in public areas.
- Persons asking questions regarding security and evacuation measures.
- Vehicles, packages, luggage left unattended.
- Vehicles appearing overweight.
- Persons appearing to count pedestrians / vehicles.
- Strangers walking around the perimeter of the commercial centre.
- Delivery vehicles arriving at premises outside normal delivery times.
- Vehicles emitting suspicious odours e.g. fuel or gas.
- Vehicle/s looking out of place.
- Erratic driving.
- Noted pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures, (bomb threats, leaving hoax devices or packages).
- The same vehicle and different individuals or the same individuals in a different vehicle returning to a location(s).
- The same or similar individuals returning to carry out the same activity to establish the optimum time to conduct the operation.
- Unusual activity by contractor's / delivery vehicles.
- Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or assault equipment, i.e. ropes, ladders, food etc. Regular perimeter patrols should be instigated months in advance of a high profile event to ensure this is not happening.
- Attempts to disguise identity – motorcycle helmets, hoodies etc, or multiple sets of clothing to change appearance.
- Constant use of different paths, and/or access routes across a site. 'Learning the route' or foot surveillance involving a number of people who seem individual but are working together.
- Multiple identification documents – suspicious, counterfeit, altered documents etc.
- Either non co-operation with police or security personnel, or more accomodating than usual.
- Those engaged in reconnaissance will often attempt to enter premises to assess the internal layout and in doing so will alter their appearance and provide cover stories.
- In the past reconnaissance operatives have drawn attention to themselves by asking peculiar and in depth questions of employees or others more familiar with the environment.
- **Sightings of suspicious activity should be passed immediately to your security management for CCTV monitoring and the event recorded for evidential purposes.**

Reconnaissance operatives may also seek additional information on:

- Width surveys of surrounding streets – exploring the range of tactical options available to deliver an explosive device.
- Levels of internal and external security – are vehicle/person/bag searches undertaken?

THE ROLE OF THE RECONNAISSANCE TEAM HAS BECOME INCREASINGLY IMPORTANT TO TERRORIST OPERATIONS.

Reconnaissance trips may be undertaken as a rehearsal to involve personnel and equipment that will be used in the actual attack.

seven good housekeeping

Good housekeeping improves the ambience of your premises and reduces the opportunity for placing suspicious items or bags and helps to deal with false alarms and hoaxes.

You can reduce the number of places where devices may be left by considering the following points:

- Avoid the use of litter bins around critical/vulnerable areas of the premises i.e. do not place litter bins next to or near glazing, support structures, most sensitive or critical areas and make sure they are covered by your CCTV and operators. Ensure that there is additional and prompt cleaning in these areas
- Review the management of all your litter bins and consider the size of their openings, their blast mitigation capabilities and location
- The use of clear bags for waste disposal is a further alternative as it provides an easier opportunity for staff to conduct an initial examination for suspicious items
- Review the use and security of any compactors, wheelie bins and metal bins used to store rubbish within service areas, goods entrances and near areas where crowds congregate
- Your business should have an agreed procedure in place for the management of contractors, their vehicles and waste collection services. The vehicle registration mark of each vehicle (and its occupants) should be known to the security staff or manager in advance
- Keep public and communal areas e.g. exits, entrances, lavatories, service corridors and yards clean and tidy
- Keep the fixtures, fittings and furniture in such areas to a minimum – ensuring that there is little opportunity to hide devices
- Lock unoccupied offices, rooms and store cupboards
- Ensure that everything has a place and that things are returned to that place
- Place tamper - proof plastic seals on maintenance hatches
- Keep external areas as clean and tidy as possible
- Pruning all vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any packages.

Additionally consider the following points:

Ensure that all staff are trained in bomb threat handling procedures or at least have ready access to instructions – and know where these are kept. See Good Practice Checklist - Bomb Threat in Appendix 'J'.

Review your CCTV system to ensure that it has sufficient coverage both internally and externally.

Ensure that fire extinguishers are identified as belonging to the premises and authorised for the locations they will be kept. Regular checks should be made to ensure that they have not been interfered with or replaced.

Your business managers should identify a second secure location for use as a control room as part of their normal contingency plans.

Security systems reliant on power should have an uninterrupted power supply (UPS) available which is regularly tested if it is identified that power loss could impact on the safety of the public.

See Good Practice Checklist - Housekeeping in Appendix 'B'.

eight access control

There should be clear demarcation between public and private areas, with appropriate access control measures into and out of the private side.

Risk assessment

Refer to 'managing the risks' on page 5 and decide the level of security you require before planning your access control system.

Appearance

The access control system to your private areas is often a strong indicator on how seriously you have planned a security regime for your premises and might be the first impression of security made upon visitors to your site.

Ease of access

Examine the layout of your system. Ensure that your entry and exit procedures allow legitimate users to pass without undue effort and delay.

Training

Ensure your staff are fully aware of the role and operation of your access control system. Your installer should provide adequate system training.

System maintenance

Your installer should supply all relevant system documentation, e.g. log books and service schedules. Are you aware of the actions required on system breakdown? Do you have a satisfactory system maintenance agreement in place? Is there a contingency plan you can implement at a moments notice?

Interaction

Your access control system should support other security measures. Consider system compatibility between access control, alarms, CCTV and text alert systems.

Compliance

Your access control system should be compliant with all local legislation.

Objectives

Are your security objectives being met? If necessary, carry out a further risk assessment and address any vulnerabilities accordingly.

Access control is only one important element of your overall security system.

REMEMBER! Whether driving a lorry or carrying explosives, a terrorist needs physical access in order to reach the intended target.

See Good Practice Checklist - Access Control and Visitors to you Business in Appendix 'C'

nine cctv guidance

CCTV can help clarify whether a security alert is real and is often vital in any post incident investigation.

You should constantly monitor the images captured by your CCTV system or regularly check recordings for suspicious activity ensuring at all times full compliance with all local legislation.

CCTV cameras should, if possible, cover all the entrances and exits to your premises and other areas that are critical to the safe management and security of your business.

With more organisations moving towards digital CCTV systems, you should liaise with your local authorities responsible for security to establish that your system software is compatible with theirs to allow retrieval and use of your images for evidential purposes.

Consider the following points:

- Ensure the date and time stamps of the system are accurate.
- Regularly check the quality of recordings.
- Digital CCTV images should be stored in accordance with local guidance.
- Ensure that appropriate lighting complements the system during daytime and darkness hours.
- Keep your recorded footage for at least 31 days.
- Ensure the images recorded are clear – that people and vehicles are clearly identifiable.
- Check that the images captured are of the right area.
- Implement standard operating procedures, codes of practice and audit trails.
- Give consideration to the number of camera images a single CCTV operator can effectively monitor at any one time.
- Do you have sufficient qualified staff to continue to monitor your CCTV system during an incident, evacuation or search?

See Good Practice Checklist – CCTV in Appendix 'D'

CCTV Maintenance

CCTV maintenance must be planned and organised in advance and not carried out on an ad hoc basis. If regular maintenance is not carried out, the system may eventually fail to meet its Operational Requirement (OR).

What occurs if a system is not maintained?

- The system gets dirty resulting in poor visiblity.
- Consumables wear causing poor performance.
- Major parts fail.
- Weather damage can cause incorrect coverage.
- Deliberate damage/environmental changes can go undetected.

ten small deliveries by courier and mail handling

Most businesses will receive a large amount of mail and other deliveries and this offers an attractive route into premises for terrorists.

Delivered Items

Delivered items, which include letters, parcels, packages and anything delivered by post or courier, have been a commonly used terrorist tactic. A properly conducted risk assessment should give you a good idea of the likely threat to your business and indicate precautions you need to take.

Delivered items may be explosive or incendiary (the two most likely kinds), or chemical, biological or radiological. Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality.

A delivered item will probably have received some fairly rough handling in the post and so is unlikely to detonate through being moved, but any attempt at opening it, however slight, may set it off or release the contents. Unless delivered by a courier, it is unlikely to contain a timing device. Delivered items come in a variety of shapes and sizes; a well made device will look innocuous but there may be telltale signs.

Indicators to Suspicious Deliveries/Mail

- It is unexpected or of unusual origin or from an unfamiliar sender.
- There is no return address or the address cannot be verified.
- It is poorly or inaccurately addressed e.g. incorrect title, spelt wrongly, title but no name, or addressed to an individual no longer with the company.
- The address has been printed unevenly or in an unusual way.
- The writing is in an unfamiliar or unusual style.
- There are unusual postmarks or postage paid marks.
- A Jiffy bag, or similar padded envelope, has been used.
- It seems unusually heavy for its size. Most letters weigh up to about 28g or 1 ounce, whereas most effective letter bombs weigh 50-100g and are 5mm or more thick.
- It is marked ‘personal’ or ‘confidential’.
- It is oddly shaped or lopsided.
- The envelope flap is stuck down completely (a harmless letter usually has an un-gummed gap of 3-5mm at the corners)
- There is a smell, particularly of almonds or marzipan.
- There is a pin sized hole in the envelope or package wrapping.
- There is an additional inner envelope, and it is tightly taped or tied (however, in some organizations, sensitive or ‘restricted’ material is sent in double envelopes as standard procedure).

Chemical, biological or radiological materials in the post

Terrorists may seek to send chemical, biological or radiological materials in the post. It is difficult to provide a full list of possible CBR indicators because of the diverse nature of the materials. However, some of the more common and obvious are:

- Unexpected granular, crystalline or finely powdered material (of any colour and usually with the consistency of coffee, sugar or baking powder), loose or in a container.
- Unexpected sticky substances, sprays or vapours.
- Unexpected pieces of metal or plastic, such as discs, rods, small sheets or spheres.
- Strange smells, e.g. garlic, fish, fruit, mothballs, pepper. If you detect a smell, do not go on sniffing it. However, some CBR materials are odourless and tasteless.
- Stains or dampness on the packaging.
- Sudden onset of illness or irritation of skin, eyes or nose. CBR devices containing finely ground powder or liquid may be hazardous without being opened.

What you can do:

- The precise nature of the incident (chemical, biological or radiological) may not be readily apparent. Keep your response plans general and wait for expert help from the local emergency services and local authorities responsible for security.
- Review plans for protecting staff and visitors in the event of a terrorist threat or attack. Remember that evacuation may not be the best solution. You will need to be guided by the local emergency services on the day.
- Plan for the shutdown of systems that may contribute to the movement of airborne hazards (e.g. computer equipment containing fans and air-conditioning units).
- Ensure that doors can be closed quickly if required.
- If your external windows are not permanently sealed shut, develop plans for closing them in response to a warning or incident.
- Examine the feasibility of emergency shutdown of air-handling systems and ensure that any such plans are well rehearsed.
- Where a hazard can be isolated by leaving the immediate area, do so as quickly as possible, closing doors and windows as you go.
- Move those directly affected by an incident to a safe location as close as possible to the scene of the incident, so as to minimise spread of contamination.
- Separate those directly affected by an incident from those not involved so as to minimize the risk of inadvertent cross-contamination.
- Ask people to remain in situ – though you cannot contain them against their will.

Planning your mail handling procedures

Although any suspect item should be taken seriously, remember that most will be false alarms, and a few may be hoaxes. Try to ensure that your procedures, while effective, are not needlessly disruptive. Take the following into account in your planning:

- Seek advice from your local authorities responsible for security on the threat to your business and on your defensive measures.
- Consider processing all incoming mail and deliveries at one point only. This should ideally be off-site or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of your business.
- Ensure that all staff who handle mail are briefed and trained. Include reception staff and encourage regular correspondents to put their return address on each item.
- Ensure all sources of incoming mail (e.g. mail, couriers, and hand delivery) are included in your screening process.
- Ideally, post rooms should have independent air conditioning and alarm systems, as well as scanners and x-ray machines. However, while mail scanners may detect devices for spreading chemical, biological and radiological (CBR) materials (e.g. explosive devices), they will not detect the materials themselves.
- At present there are no CBR detectors capable of identifying all hazards reliably.
- Post rooms should also have their own washing and shower facilities, including soap and detergent.
- Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual deliveries. Train them to open post with letter openers (and with minimum movement), to keep hands away from noses and mouths and always to wash their hands afterwards. Staff should not blow into envelopes or shake them. Packages suspected of containing biological, chemical or radiological material should ideally be placed in a double sealed bag.
- Consider whether staff handling post, need protective equipment such as latex gloves and facemasks (seek advice from a qualified health and safety expert). Keep overalls and footwear available in case they need to remove contaminated clothing.
- Make certain post handling areas can be promptly evacuated. Rehearse evacuation procedures and routes, which should include washing facilities in which contaminated staff could be isolated and treated.
- Staff who are responsible for mail handling should be made aware of the importance of isolation in reducing contamination.
- Prepare signs for display to staff in the event of a suspected or actual attack.

eleven search planning

Searches of your premises should be conducted as part of your daily good housekeeping routine. They should also be conducted in response to a specific threat and when there is a heightened response level.

It is recognised, that for the majority of your business sites, responsibility for the implementation of any search planning, following a vulnerability and risk assessment, will fall upon the Security Manager.

The following advice is generic for most business sites, but recognises that they are built and operate differently.

Search Plans

- Search plans should be prepared in advance and staff should be trained in them.
- The conduct of searches will depend on local circumstances and local knowledge, but the overall objective is to make sure that the entire area, including grounds, are searched in a systematic and thorough manner so that no part is left unchecked.
- If you decide to evacuate your premises in response to an incident or threat, you will also need to search it in order to ensure it is safe for re-occupancy.
- The local authorities responsible for security will not normally search business premises. They are not familiar with the layout and will not be aware of what should be there and what is out of place. They cannot, therefore, search as quickly or as thoroughly as a member of staff or on site security personnel.
- The member(s) of staff nominated to carry out the search do not need to have expertise in explosives or other types of device. But they must be familiar with the place they are searching. They are looking for any items that should not be there, that cannot be accounted for and items that are out of place.
- Ideally, searchers should search in pairs; to ensure searching is systematic and thorough.

Action You Should Take

Consider dividing your business premises into sectors. If the site is organised into departments and sections, these should be identified as separate search sectors. Each sector must be of manageable size.

Each sector search plan should have a written checklist - signed when completed - for the information of the Security Manager.

Remember to include any stairs, fire escapes, corridors, toilets and lifts in the search plan, as well as car parks, service yards and other areas outside. If evacuation is considered or implemented, then a search of the assembly areas, the routes to them and the surrounding area should also be made prior to evacuation.

Consider the most effective method of initiating the search. You could:

- Send a message to your search teams over a public address system (the messages should be coded to avoid unnecessary disruption and alarm).
- Use personal radios or pagers.

Ensure the searchers know what to do if they discover a suspicious item. Action will depend on the nature of the device and the location, but the general "golden rules" are:

1. **Do not touch or move suspicious items.**
2. **Move everyone away to a safe distance and prevent others from approaching.**
3. **Communicate safely to staff, visitors and the public.**
4. **Communicate what has been found to the Security Manager, using hand-held radios or mobile phones – only once out of the immediate vacinity of the suspect item, remaining out of line of sight and behind hard cover.**
5. **Ensure that whoever found the item or witnessed the incident remains on hand to brief the local police or local authorities responsible for security.**
6. **The Security Manager should liaise with the local police or local authorities responsible for security regarding safe evacuation distances.**

Exercise your search plan regularly. The searchers need to get a feel for the logical progression through their designated area and the length of time this will take. They also need to be able to search without unduly alarming any visitors or customers.

See good practice checklist – Searching in Appendix 'E'

twelve personnel security

Some external threats, whether from criminals, terrorists, or competitors seeking a business advantage, may rely upon the co-operation of an 'insider'.

This could be an employee or any contract or agency staff (e.g. cleaner, caterer, security guard) who has authorised access to your premises. If an employee, he or she may already be working for you, or may be someone newly joined who has infiltrated your organisation in order to seek information or exploit the access that the job might provide.

What is personnel security?

Personnel security is a system of policies and procedures which seek to manage the risk of staff or contractors exploiting their legitimate access to an organisation's assets or premises for unauthorised purposes. These purposes can encompass many forms of criminal activity, from minor theft through to terrorism.

The purpose of personnel security seeks to minimise the risks. It does this by ensuring that organisations employ reliable individuals, minimising the chances of staff becoming unreliable once they have been employed, detect suspicious behaviour, and resolving security concerns once they have become apparent.

This chapter refers mainly to pre-employment screening, but organisations should be aware that personnel screening should continue throughout the worker's term of employment. Further information regarding ongoing personnel screening can be found at www.cpni.gov.uk

Understanding and assessing personnel security risks

Organisations deal regularly with many different types of risk. One of them is the possibility that staff or contractors will exploit their positions within the organisation for illegitimate purposes. These risks can be reduced but can never be entirely prevented. Instead, as with many other risks, the organisation should employ a continuous process for ensuring that the risks are managed in a proportionate and cost-effective manner.

Pre-employment Screening

Personnel security involves a number of screening methods, which are performed as part of the recruitment process but also on a regular basis for existing staff. The ways in which screening is performed varies greatly between organisations; some methods are very simple, others are more sophisticated. In every case, the aim of the screening is to collect information about potential or existing staff and then use that information to identify any individuals who present security concerns.

Pre-employment screening seeks to verify the credentials of job applicants and to check that the applicants meet preconditions of employment (e.g. that the individual is legally permitted to take up an offer of employment). In the course of performing these checks it will be established whether the applicant has concealed important information or otherwise misrepresented themselves. To this extent, pre-employment screening may be considered a test of character.

Pre-employment checks

Personnel security starts with the job application, where applicants should be made aware that supplying false information, or failing to disclose relevant information, could be grounds for dismissal and may amount to a criminal offence. Applicants should also be made aware that any offers of employment are subject to the satisfactory completion of pre-employment checks.

Pre-employment screening checks may be performed directly by an organisation, or this process may be sub-contracted to a third party. In either case the company needs to have a clear understanding of the thresholds for denying someone employment.

Pre-employment screening policy

Your pre-employment screening processes will be more effective if they are an integral part of your policies, practices and procedures for the recruiting, hiring, and where necessary training of employees. If you have conducted a personnel security risk assessment then this will help you decide on the levels of screening that are appropriate for different posts.

Identity

Of all the pre-employment checks, identity verification is the most fundamental. Two approaches can be used:

- A paper - based approach involving the verification of key identification documents and the matching of these documents to the individual.
- An electronic approach involving searches on databases to establish the electronic footprint of the individual. The individual is then asked to answer questions about the footprint which only the actual owner of the identity could answer correctly.
- Pre-employment checks can be used to confirm an applicant's identity, nationality and immigration status, and to verify their declared skills and employment history.

Qualifications and employment history

The verification of qualifications and employment can help those applicants attempting to hide negative information such as a prison sentence or dismissal. Unexplained gaps should be explored.

Qualifications

When confirming details about an individual's qualification it is always important to:

- Consider whether the post requires a qualifications check.
- Always request original certificates and take copies.
- Compare details on certificates etc. with those provided by by the applicant.
- Independently confirm the existence of the establishment and contact them to confirm the details provided by the individual.

Employment checks

It is increasingly difficult to obtain character references, but past employers should be asked to confirm dates of employment. Where employment checks are carried out it is important to:

- Check a minimum of three but ideally five years previous employment.
- Independently confirm the employer's existence and contact details (including the line manager).
- Confirm details (dates, position, salary).
- Where possible, request an employer's reference from the line manager.

Financial checks

For some posts it may be justifiable to carry out financial checks, for example where the employee's position requires the handling of money. Interpreting the security implications of financial history is not straightforward and will require each organisation to decide where their thresholds lie (e.g. in terms of an acceptable level of debt).

There are a number of ways in which financial checks can be carried out. General application forms can include an element of self-declaration (for example in relation to County Court Judgements (CCJs)), or the services of third party providers can be engaged to perform credit checks.

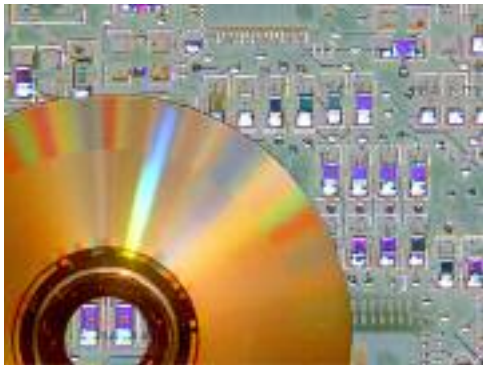
Contractor recruitment

Organisations employ a wide variety of contract staff, such as IT staff, cleaners, and management consultants. It is important to ensure that contractors have the same level of pre-employment screening as those permanent employees with equivalent levels of access to the company's assets, be they premises, systems, information or staff.

Contracts should outline the type of checks required for each post and requirements should be cascaded to any sub-contractors. Where a contractor or screening agency is performing the checks they should be audited (see the chapter 'Secure Contracting' for additional guidance on dealing with contractors via the CPNI website).

See Good Practice Checklist - Personnel Security in Appendix 'G'.

thirteen information security



The loss of confidentiality, integrity and most importantly, availability of information in paper or electronic format can be a critical problem for organisations. Many rely on their information systems to carry out business or nationally critical functions and manage safety and engineering systems.

Your confidential information may be of interest to business competitors, criminals, intelligence services or terrorists. They may attempt to access your information by breaking into your IT systems, by obtaining the data you have thrown away or by infiltrating your organisation. Such an attack could disrupt your business and damage your reputation.

Before taking specific measures you should:

Assess the threat and your vulnerabilities. See Managing the Risks on Page 5.

- To what extent is your information at risk, who might want it, how might they get it, how would its loss or theft damage you?
- Consider current good practice information security for countering electronic attack and for protecting documents.

For general advice on protecting against electronic attack visit www.cpni.gov.uk

Electronic attack

Attacks on electronic systems could:

- allow the attacker to steal or alter sensitive information
- allow the attacker to gain access to your computer system and do whatever the system owner can do. This could include modifying your data, perhaps subtly so that it is not immediately apparent, or installing malicious software (virus or worm) that may damage your system, or installing hardware to relay information back to the attacker. Such attacks against internet-connected systems are extremely common.
- make your systems impossible to use through 'denial of service' attacks. These are increasingly common, relatively simple to launch and difficult to protect against.

As soon as you entrust your information or business processes to a computer system, they are at risk. Electronic attacks are much easier when computer systems are connected directly or indirectly to public networks such as the internet.

The typical methods of electronic attack are:

Denial of service (DoS)

These attacks aim to overwhelm a system by flooding it with unwanted data. Some DoS attacks are distributed, in which large numbers of unsecured, 'innocent' machines (known as 'zombies') are conscripted to mount attacks.

As with other security measures; you should conduct a risk assessment to establish whether you might be at particular risk from an electronic attack. System security professionals can provide detailed advice.

Malicious software

The techniques and effects of malicious software (e.g. viruses, worms, trojans) are as variable as they are widely known. The main ways a virus can spread are through:

- Running or executing an attachment received in an Email.
- Clicking on a website received in an Email.
- Inappropriate web browsing which often leads to a website distributing malicious software.
- Allowing staff to connect removable memory devices (USB memory sticks, CDs etc.) to corporate machines.
- Allowing staff to connect media players and mobile phones to corporate machines.

Hacking

This is an attempt at unauthorised access, almost always with malicious or criminal intent. Sophisticated, well-concealed attacks by intelligence services seeking information have been aimed at government systems but other organisations might also be targets.

Malicious modification of hardware

Computer hardware can be modified so as to mount or permit an electronic attack. This is normally done at the point of manufacture or supply prior to installation, though it could also be done during maintenance visits or by insiders. The purpose of such modifications would be to allow a subsequent attack to be made, possibly by remote activation.

What to do

- Implement an acceptable use policy for staff concerning web browsing, Email, use of chat rooms, social sites, trading, games and music download sites.
- Acquire your IT systems from reputable manufacturers and suppliers.
- Ensure that your software is regularly updated. Suppliers are continually fixing security vulnerabilities in their software. These fixes or patches are available from their websites – consider checking for patches and updates at least weekly.
- Ensure that all internet-connected computers are equipped with anti-virus software and are protected by a firewall.
- Back up your information, preferably keeping a secure copy in another location.
- Assess the reliability of those who maintain, operate and guard your systems. Refer to the section on Personnel Security on page 31.
- Consider encryption packages for material you want to protect, particularly if taken offsite – but seek expert advice first.
- Take basic security precautions to prevent software or other sensitive information falling into the wrong hands. Encourage security awareness among your staff, training them

not to leave sensitive material lying around and to operate a clear desk policy (i.e. desks to be cleared of all work material at the end of each working session).

- Make sure your staff are aware that users can be tricked into revealing information which can be used to gain access to a system, such as user names and passwords.
- Invest in secure cabinets, fit locking doors and ensure the proper destruction of sensitive material.
- Where possible, lock down or disable disk drives, USB ports and wireless connections.
- Ensure computer access is protected by securely controlled, individual passwords or by biometrics and passwords.

Businesses can seek advice from the Government website – www.getsafeonline.org/

Examples of electronic attacks

- A former systems administrator was able to intercept e-mail between company directors because the outsourced security services supplier had failed to secure the system.
- A former employee was able to connect to a system remotely and made changes to a specialist electronic magazine, causing loss of confidence among customers and shareholders.

Disposal of sensitive information

Companies and individuals sometimes need to dispose of sensitive information. Some of the material that businesses routinely throw away could be of use to a wide variety of groups including business competitors, identity thieves, criminals and terrorists.

The types of information vary from staff names and addresses, telephone numbers, product information, customer details, technical specifications and chemical and biological data. Terrorist groups are known to have shown interest in the last two areas.

The principal means of destroying sensitive waste are:

Shredding

Shredding machines specified to DIN 32757 – 1 level 4 will provide a shred size of 15mm x 1.9mm suitable for medium to high security requirements.

Incineration

Incineration is probably the most effective way of destroying sensitive waste, including disks and other forms of magnetic and optical media, provided a suitable incinerator is used (check with your local authorities with responsible for security). Open fires are not reliable as material is not always destroyed and legible papers can be distributed by the updraft.

Pulping

This reduces waste to a fibrous state and is effective for paper and card waste only. However, some pulping machines merely rip the paper into large pieces and turn it into a paper maché product from which it is still possible to retrieve information. This is more of a risk than it used to be because inks used by modern laser printers and photocopiers do not run when wet.

There are alternative methods for erasing electronic media, such as overwriting and degaussing. For further information visit www.cpni.gov.uk

Before investing in waste destruction equipment you should:

- If you use contractors, ensure that their equipment and procedures are up to standard. Find out who oversees the process, what kind of equipment they have and whether the collection vehicles are double-manned, so that one operator remains with the vehicle while the other collects. Communications between vehicle and base are also desirable
- Ensure that the equipment is up to the job. This depends on the material you wish to destroy, the quantities involved and how confidential it is
- Ensure that your procedures and staff are secure. There is little point investing in expensive equipment if the people employed to use it are themselves security risks
- Make the destruction of sensitive waste the responsibility of your security department rather than facilities management.

See good practice checklist – Information Security in Appendix 'H'

fourteen vehicle borne improvised explosive devices (VBIEDs)

Vehicle Borne Improvised Explosive Devices (VBIEDs) are one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives to a target and can cause a great deal of damage.

Once assembled, the bomb can be delivered at a time of the terrorist's choosing and with reasonable precision, depending on defences. It can be detonated from a safe distance using a timer or remote control, or can be detonated on the spot by a suicide bomber.

As building a VBIED requires a significant investment of time, resources and expertise, terrorists will seek to obtain the maximum impact for their investment.

Terrorists generally select targets where they can cause most damage, inflict mass casualties or attract widespread publicity.

Effects of VBIED's

VBIED's can be highly destructive. It is not just the effects of a direct bomb blast that can be lethal, flying debris such as glass can present a hazard many metres away from the seat of the explosion.

What you can do

If you think your business could be at risk from any form of VBIED you should:

- Ensure you have effective vehicle access controls, particularly at goods entrances and service yards. Do not allow unchecked vehicles to park in underground service areas directly below or next to public areas where there will be large numbers of people or where there is a risk of structural collapse.
- Do what you can to make your premises blast resistant, paying particular attention to windows. Have the structures reviewed by a qualified security / structural engineer when seeking advice on protected spaces.
- Insist that details of contract vehicles and the identity of the driver and any passengers approaching your goods/service areas are authorised in advance.
- Consider a vehicle search regime at goods/service entrances that is flexible and can be tailored to a change in threat or response level. It may be necessary to carry out a risk assessment for the benefit of security staff who may be involved in vehicle access control.
- Establish and rehearse bomb threat and evacuation drills. Bear in mind that, depending on where the suspected VBIED is parked and the design of your building, it may be safer in windowless corridors or basements than outside if this facility is available.
- Consider using robust physical barriers to keep all but authorised vehicles at a safe distance, vehicle security barriers can be passive (eg. static bollards or planters) or active (sliding, swinging, rising gates or retractable blockers and bollards). If being procured for high security applications then only measures successfully tested to BSI PAS68 should be considered. BSI PAS68 is the impact test specification for vehicle security

barriers. Installations should not allow air gaps greater than 1.2m between adjacent barrier items. CPNI can provide a catalogue of successfully tested systems, and also produce advice for sites, architects and engineers on how to blend such items in to the street scene. Refer to the Security Advice section at the CPNI website www.cpni.gov.uk.

- Train and rehearse your staff in applying good security protocols, and in receiving and acting upon bomb threats. Key information and telephone numbers should be prominently displayed and readily available.
- Assembly areas must take account of the proximity to the potential threat. You should bear in mind that a vehicle bomb delivered into your building – for instance via service yards, underground car parks or through the front of your premises – could have a far greater destructive effect on the structure than an externally detonated device.
- It should be emphasised that the installation of physical barriers needs to be balanced against the requirements of safety and should not be embarked upon without full consideration of any local planning regulation and fire safety risk assessment.

See Good Practice Checklist – Access Control and Visitors to your Business in Appendix 'C'

fifteen chemical, biological and radiological (CBR) attacks

Much of the CBR-related activity seen to date has either been criminal, or has involved hoaxes and false alarms. There have so far only been a few examples of terrorists using CBR materials. The most notable were the 1995 sarin gas attack on the Tokyo subway, which killed twelve people, and the 2001 anthrax letters in the United States, which killed five people.

CBR weapons have been little used so far, largely due to the difficulty in obtaining the materials and the complexity of using them effectively. Where terrorists have tried to carry out CBR attacks, they have generally used relatively simple materials. However, Al Qaida and related groups have expressed a serious interest in using CBR materials. The impact of any terrorist CBR attack would depend heavily on the success of the chosen dissemination method and the weather conditions at the time of the attack.

As with other terrorist attacks, you may not receive prior warning of a CBR incident. Moreover, the exact nature of an incident may not be immediately obvious. First indicators may be the sudden appearance of powders, liquids or strange smells, with or without an immediate effect on people.

Good general physical and personnel security measures will contribute towards resilience against CBR incidents. Remember to apply appropriate personnel security standards to contractors, especially those with frequent access to your site.

Since the early 1990s, concern that terrorists might use CBR materials as weapons has steadily increased. The hazards are:

Chemical
Poisoning or injury caused by chemical substances, including ex-military chemical warfare agents or legitimate but harmful household or industrial chemicals.

Biological
Illnesses caused by the deliberate release of dangerous bacteria, viruses or fungi, or biological toxins such as the plant toxin ricin.

Radiological
Illnesses caused by exposure to harmful radioactive materials contaminating the environment.

What you can do

- Review the physical security of any air-handling systems, such as access to intakes and outlets.
- Ensure nominated staff know how to turn off and secure air conditioning systems.
- Improve air filters or upgrade your air-handling systems, as necessary.
- Restrict access to water tanks and other key utilities.
- Review the security of your food and drink supply chains.
- Consider whether you need to make special arrangements for mail or parcels, e.g. a separate post room, possibly with dedicated air-handling, or even a specialist off-site facility. See Mail Handling on page 26.
- **The Home Office advises organisations against the use of CBR detection technologies as part of their contingency planning measures at present. This is because the technology is not yet proven in civil settings.** A basic awareness of CBR threat and hazards, combined with general protective security measures (e.g. screening visitors, CCTV monitoring of perimeter and entrance areas, being alert to suspicious deliveries) should offer a good level of resilience.
- If there is a designated protected space available this may also be suitable as a CBR shelter, but seek specialist advice before you make plans to use it in this way.
- Consider how to communicate necessary safety advice to staff and how to offer reassurance. This needs to include instructions to those who want to leave or return to the building.

sixteen suicide attacks

The use of suicide bombers is a very effective method of delivering an explosive device to a specific location. Suicide bombers may use a lorry, plane or other kind of vehicle as a bomb or may carry or conceal explosives on their persons. These types of attack are generally perpetrated without warning. The most likely targets are mass casualty crowded places, symbolic locations and key installations. There is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the police.

When considering protective measures against suicide bombers, think in terms of:

- Using physical barriers to prevent a hostile vehicle from driving into your premises through main entrances, goods/service entrances, pedestrian entrances or open land.
- Denying access to any vehicle that arrives at your goods/service entrances without prior notice and holding vehicles at access control points into your site until you can satisfy yourself that they are genuine.
- Wherever possible, establish your vehicle access control point at a distance from the protected site, setting up regular patrols and briefing staff to look out for anyone behaving suspiciously. Many bomb attacks are preceded by reconnaissance or trial runs. Ensure that such incidents are reported to your local police or authorities responsible for security.
- Ensure that no one visits your protected area without your being sure of his or her identity or without proper authority.
- Effective CCTV systems may deter a terrorist attack or even identify planning activity. Good quality images can provide crucial evidence in court.

See Hostile Reconnaissance on page 19.

seventeen firearm & weapon attacks

Attacks involving firearms and weapons are still infrequent but it is important to be prepared to cope with such an incident.

The important advice below will help you plan.

In the event of an attack take these four actions:

Stay Safe

- **Under immediate GUN FIRE** – Take cover initially, but leave the area as soon as possible if safe to do so
- **Nearby GUN FIRE** - Leave the area immediately, if possible and it is safe to do so.
- Leave your belongings behind.
- Do not congregate at evacuation points.

COVER FROM GUN FIRE	COVER FROM VIEW
Substantial brickwork or concrete	Internal partition walls
Engine blocks of motor vehicles	Car doors
Base of large live trees	Wooden fences
Earth banks/hills/mounds	Curtains

REMEMBER - out of sight does not necessarily mean out of danger, especially if you are not in 'cover from gun fire.'

IF YOU CAN'T ESCAPE - consider locking yourself and others in a room or cupboard. Barricade the door then stay away from it.

If possible choose a room where escape or further movement is possible. Silence any sources of noise, such as mobile phones, that may give away your presence.

See

The more information that you can pass to police the better but NEVER risk your own safety or that of others to gain it. Consider using CCTV and other remote methods where possible to reduce the risk. If it is safe to do so, think about the following:

- Is it a firearms / weapons incident?
- What else are they carrying?
- Moving in any particular direction?
- Are they communicating with others?
- Exact location of the incident.
- Number and description of gunmen.
- Type of firearm -long-barrelled or handgun.
- Number of casualties / people in the area.

Tell

- **LOCAL AUTHORITIES** - contact them immediately by giving them the information shown under 'See'.
- Use all the **channels of communication** available to you to inform staff, visitors, neighbouring premises, etc of the danger.

Act

- Secure your immediate environment and other vulnerable areas.
- Keep people out of public areas, such as corridors and foyers.
- Move away from the door and remain quiet until told otherwise by appropriate authorities or if you need to move for safety reasons, such as a building fire.

Armed Response

In the event of an attack involving firearms or weapons, the priority for the armed response is to protect and save lives. Please remember:

- Initially they may not be able to distinguish you from the gunmen.
- Officers may be armed and may point guns at you.
- They may have to treat the public firmly. Follow their instructions; keep hands in the air / in view.
- Avoid quick movement towards the officers and pointing, screaming or shouting.

Plan

Consider the following when planning for a firearms / weapons incident

1. How you would communicate with staff, visitors, neighbouring premises, etc.
2. What key messages would you give to them in order to keep them safe.
3. Have the ability to secure key parts of the building to hinder free movement of the gunmen.
3. Think about incorporating this into your emergency planning and briefings.
4. Test your plan at least annually.

If you require further information then please liaise with your Local Authorities.

eighteen communication and security culture

You should consider a communication strategy for raising awareness among staff and others who need to know about your security plan and its operation. This will include the emergency services, local authorities and possibly neighbouring premises.

There should also be arrangements for dealing with people who may be affected by your security operation but who are not employees of your organisation (e.g. customers, clients, contractors, visitors).

It should be remembered that immediately following a terrorist attack, mobile telephone communication may be unavailable due to excessive demand.

Linked to communication, is the issue that all work environments possess their own unique internal culture that influences the way employees behave and interact. Though it might suit the day-to-day functions of the business, the existing culture may not be appropriate to secure the business against the potential threats it may face. In fact, it may even encourage behaviours that expose the business to a wider range of vulnerabilities than necessary.

Management should be seeking to ensure that the everyday actions and attitudes of staff effortlessly contribute towards the organisation's protective security. A security culture, therefore, is about encouraging all members of staff to respect common values and approaches towards security both inside or outside of the workplace.

One way to influence security culture is for Security Managers to meet with staff to discuss security issues and encourage staff to raise their concerns about security. Further information regarding security culture can be found at www.cpni.gov.uk.

Consideration should be given to the use of any intranet website or Email system to communicate crime prevention and counter terrorism initiatives.

All Security Managers should involve their local Police Counter Terrorism Security Adviser when considering improvements to a commercial centre and / or its environs.

See Good Practice Checklist – Communication and Security Culture in Appendix 'I'

good practice checklists

The following checklists are intended as a guide for your business managers to assist them in identifying the hazards and risks associated with counter terrorism planning.

They are not, however, exhaustive and some of the guidance might not be relevant to all business sites.

The checklists should be considered taking the following factors into account:

- Have you consulted your local authority responsible for security and the local fire and/or rescue service?
- Who else should be included during consultation?
- Which measures can be implemented with ease?
- Which measures will take greater planning and investment?

appendix a

Business Continuity

	Yes	No	Unsure
Do you have a Business Continuity Plan?			
Do you regularly review and update your plan?			
Are your staff trained in activating and operating your plan?			
Have you prepared an emergency 'Grab Bag' as explained on page 15?			
Do you have access to an alternative workspace to use in an emergency?			
Are your critical documents adequately protected?			
Do you have copies of your critical records at a separate location?			
Do you have contingency plans in place to cater for the loss/ failure of key equipment?			
Do you have sufficient insurance to pay for disruption to business, cost of repairs, hiring temporary employees, leasing temporary accommodation and equipment?			

appendix b

Housekeeping

	Yes	No	Unsure
Have you reviewed the use and location of all waste receptacles in and around your premises, taking into consideration their proximity to glazing and building support structures?			
Do you keep external areas, entrances, exits, stairs, reception areas and toilets clean and tidy?			
Do you keep furniture to a minimum to provide little opportunity to hide devices, including under chairs and sofas?			
Are unused offices, rooms and function suites locked?			
Do you use seals / locks to secure maintenance hatches, compactors and industrial waste bins when not required for immediate use?			
Do you screen all your mail and can you isolate your mail processing area?			
Are your reception staff and deputies trained and competent in managing telephoned bomb threats?			
Have you considered marking your first aid and fire fighting equipment as your business property and checked it has not been replaced?			

appendix C

Access Control and Visitors to Your Business

	Yes	No	Unsure
Do you prevent all vehicles from entering goods or service areas directly below, above or next to pedestrian areas where there will be large numbers of people, until they are authorised by your security?			
Do you have in place physical barriers to keep all but authorised vehicles at a safe distance and to mitigate against a hostile vehicle attack?			
Is there clear demarcation identifying the public and private areas of your business premises?			
Do your staff, including contractors, cleaners and other employees wear ID badges at all times when on the site?			
Do you adopt a 'challenge culture' to anybody not wearing a pass in your private areas?			
Do you insist that details of contract vehicles and the identity of the driver and any passengers requiring permission to park and work in your site are authorised in advance?			
Do you require driver and vehicle details of waste collection services in advance?			
Do all business visitors to your management and administration areas have to report to a reception area before entry and are they required to sign in and issued with a visitors pass?			
Are business visitors' badges designed to look different from staff badges?			
Are all business visitors' badges collected from visitors when they leave the premises?			
Does a member of staff accompany business visitors at all times while in the private areas of your premises?			

appendix d

CCTV

	Yes	No	Unsure
Do you constantly monitor your CCTV images or playback overnight recordings for evidence of suspicious activity?			
Do you have your CCTV cameras regularly maintained?			
Do the CCTV cameras cover the entrances and exits to your business premises?			
Have you considered the introduction of Automatic Number Plate Reader (ANPR) to complement your security operation?			
Do you have CCTV cameras covering critical areas in your business, such as server rooms, back up generators and cash offices?			
Do you store the CCTV images in accordance with the evidential needs of the police?			
Could you positively identify an individual from the recorded images on your CCTV system?			
Are the date and time stamps of the system accurate?			
Does the lighting system complement the CCTV system during daytime and darkness hours?			
Do you regularly check the quality of your recordings?			
Have you implemented operating procedures, codes of practice and audit trails?			
Is each CCTV camera doing what it was installed to do?			

appendix e

Searching

	Yes	No	Unsure
Do you exercise your search plan regularly?			
Do you carry out a sectorised, systematic and thorough search of your business premises as a part of routine housekeeping and in response to a specific incident?			
Does your search plan have a written checklist - signed by the searching officer as complete for the information of the Security Manager?			
Does your search plan include toilets, lifts, car parks and service areas?			
Have you considered a vehicle search regime at goods/service entrances that is flexible and can be tailored to a change in threat or response level?			
Do you conduct random overt searches of vehicles as a visual deterrent?			
Do sub-contractors and other service providers operating within the centre have their own search procedure with notification to management when complete?			
Have you considered a visitor search regime that is flexible and can be tailored to a change in threat or response level?			
Do you make use of your website/publications to inform contractors, visitors, of your searching policies as well as crime prevention and counter terrorism messages?			
Do you have a policy to refuse entry to any vehicle whose driver refuses a search request?			
Are your searching staff trained and properly briefed on their powers and what they are searching for?			
Are staff trained to deal effectively with unidentified packages found within the site?			
Do you have sufficient staff to search effectively?			
Do you search your evacuation routes and assembly areas before they are utilised?			

appendix f

Evacuation / 'Invacuation'

	Yes	No	Unsure
Is evacuation part of your security plan?			
Is 'invacuation' into a protected space part of your security plan?			
Have you sought advice from a structural engineer to identify protected spaces within your building?			
Do you have nominated evacuation / 'invacuation' marshals?			
Does your evacuation plan include 'incident' assembly areas distinct from fire assembly areas?			
Have you determined evacuation routes?			
Have you agreed your evacuation / 'invacuation' plans with the police, emergency services and your neighbours?			
Do you have reliable, tested communications facilities in the event of an incident?			
Have any disabled staff been individually briefed?			
Do you have a review process for updating plans as required?			

appendix g

Personnel Security

	Yes	No	Unsure
Full name			
Current address and any previous addresses in last five years			
Date of birth			
Full details of references (names, addresses and contact details)			
Full details of previous employers, including dates of employment			
Proof of relevant educational and professional qualifications			
Full (current) passport			
Driving license (ideally with photo)			
Birth Certificate – issued within six weeks of birth			
Credit card – with three statements and proof of signature			
Cheque book and bank card – with three statements and proof of signature			
Proof of residence – tax, gas, electric, water or telephone bill			

appendix h

Information Security

	Yes	No	Unsure
Do you lock away all business documents at the close of the business day?			
Do you have a clear-desk policy out of business hours?			
Do you close down all computers at the close of the business day?			
Are all your computers password protected?			
Do you have computer firewall and antivirus software on your computer systems?			
Do you regularly update this protection?			
Have you considered an encryption package for sensitive information you wish to protect?			
Do you destroy sensitive data properly when no longer required?			
Do you back up business critical information regularly?			
Do you have a securely contained back up at a different location from where you operate your business? (Fall back procedure)			
Have you invested in secure cabinets for your IT equipment?			

appendix i

Communication and Security Culture

	Yes	No	
Are security issues discussed / decided at Board level and form a part of your organisation's culture?			
Do you have a security policy or other documentation showing how security procedures should operate within your business?			
Is this documentation regularly reviewed and if necessary updated?			
Do you encourage all members of staff to respect common values and approaches towards security both inside or outside of the workplace?			
Do you regularly meet with staff and discuss security issues?			
Do you encourage staff to raise their concerns about security?			
Do you speak with neighbours to your commercial centre on issues of security and crime that might affect you all?			
Do you remind your staff to be vigilant when traveling to and from work, and to report anything suspicious to the relevant authorities or police?			
Do you make use of your website, to communicate crime and counter terrorism initiatives, including an advance warning regarding searching?			

appendix j

Bomb Threat

This checklist is designed to help your staff to deal with a telephoned bomb threat effectively and to record the necessary information.

Visit www.cpni.gov.uk to download a PDF and print it out.

Actions to be taken on receipt of a bomb threat:

Switch on tape recorder/voicemail (if connected)

Tell the caller which town/district you are answering from

Record the exact wording of the threat:

_____

_____

Ask the following questions:

Where is the bomb right now? _____

When is it going to explode? _____

What does it look like? _____

What kind of bomb is it? _____

What will cause it to explode? _____

Did you place the bomb? _____

Why? _____

What is your name? _____

What is your address? _____

What is your telephone number? _____

(Record time call completed:)

Where automatic number reveal equipment is available, record number shown:

_____

Inform the premises manager of name and telephone number of the person informed:

_____

Contact local authorities. Time informed: _____

The following part should be completed once the caller has hung up and the premises manager has been informed.

Time and date of call: _____

Length of call: _____

Number at which call was received (i.e. your extension number): _____

ABOUT THE CALLER

Sex of caller: _____

Nationality: _____

Age: _____

THREAT LANGUAGE (tick)

❒ Well spoken?

❒ Irrational?

❒ Taped message?

❒ Offensive?

❒ Incoherent?

❒ Message read by threat-maker?

CALLER'S VOICE (tick)

❒ Calm?

❒ Crying?

❒ Clearing throat?

❒ Angry?

❒ Nasal?

❒ Slurred?

❒ Excited?

❒ Stutter?

❒ Disguised?

❒ Slow?

❒ Lisp?

❒ Accent? If so, what type?_____

❒ Rapid?

❒ Deep?

❒ Hoarse?

❒ Laughter?

❒ Familiar? If so, whose voice did it sound like? _____

BACKGROUND SOUNDS (tick)

❒ Street noises?

❒ House noises?

❒ Animal noises?

❒ Crockery?

❒ Motor?

❒ Clear?

❒ Voice?

❒ Static?

❒ PA system?

❒ Booth?

❒ Music?

❒ Factory machinery?

❒ Office machinery?

❒ Other? (specify) _____

OTHER REMARKS

_____

_____

_____

_____

Signature

_____

Date _____

Print name

_____

What do the results show?

Having completed the various 'Good Practice' checklists you need to give further attention to the questions that you have answered 'no' or 'don't know' to.

If you answered 'don't know' to a question, find out more about that particular issue to reassure yourself that this vulnerability is being addressed or needs to be addressed.

If you answered 'no' to any question then you should seek to address that particular issue as soon as possible.

Where you have answered 'yes' to a question, remember to regularly review your security needs to make sure that your security measures are fit for that purpose.

reporting incidents

The aim of any observation is to be able to accurately report it to colleagues, management, local police and local authorities responsible for security.

The observer should be able to identify and describe both person and vehicle, so that third parties can imagine or recreate a general picture of the individual or vehicle described.

Observations

There are certain rules that should be followed when preparing a report such as:

- Always be honest. Do not invent or over-exaggerate sighting(s)
- Do not make assumptions
- Personal opinions regarding a criminal's purpose, activities or intentions can be included but must be clearly stated as such
- Report only the facts as seen, not to please supervisors or managers

SALUTE

A handy mnemonic for remembering key details when explaining an incident is SALUTE. This stands for:

- Situation: Who or what caught your attention?
- Activity: What was happening? What was the person or vehicle doing?
- Location: Where exactly was this?
- Unit: Who made the observation?
- Time: Time and date of the incident
- Equipment: Any specific equipment used such as a specific camera.

Remembering Observations

When trying to remember and describe a person after an observation use the following key words:

- Gender
- Race
- Age
- Hair colour
- Weight
- Build
- Height
- Special features (this may include scars, tattoos, disabilities)

Clothing is only important when describing a suspect person to another team member as an observation/event in unfolding, as clothes can be quickly and easily changed. Pay attention to inner clothes worn under the outer layer and to the shoes or trousers, as they are rarely changed.

Unless a business has a policy of doing so, the security officers should be encouraged not to attempt to use terminology they may have heard elsewhere, this will only serve to cause confusion to those who are not familiar with them.

Vehicle descriptions

When trying to remember and describe a vehicle after an observation use the following key words:

- Type
- Colour
- Size
- Year
- Number of doors
- Sunroof
- Registration number
- Type of aerial
- Distinguishing marks or features
- Number of occupants
- Weighted down
- Direction of travel

useful publications

Publications

Protecting Against Terrorism (3rd Edition)
This booklet gives general protective security advice from Centre for the Protection of National Infrastructure (CPNI). It is aimed at businesses and other organisations seeking to reduce the risk of a terrorist attack, or to limit the damage terrorism might cause. The booklet is available in PDF format and can be downloaded from www.cpni.gov.uk.

Personnel Security: Managing the Risk
This booklet has been developed by CPNI. It outlines the various activities that constitute a personnel security regime. As such it provides an introductory reference for security managers and human resource managers who are developing or reviewing their approach to personnel security. The booklet is available in PDF format and can be downloaded from www.cpni.gov.uk

Pre-Employment Screening
CPNI's Pre-Employment Screening is the latest in a series of advice products on the subject of personnel security. It provides detailed guidance on pre-employment screening measures including:

- Identity checking
- Confirmation of the right to work
- Verification of a candidate's historical personal data (including criminal record checks)

The booklet is available in PDF format and can be downloaded from www.cpni.gov.uk.

NaCTSO has produced a suite of booklets designed to meet the security and resilience needs of business. The information contained in these booklets is primarily for small and medium-sized businesses, but are relevant to any business. You can read all the booklets in order to cover all the important areas in a systematic way, or you can go to specific booklets if you need information on a particular topic. All of the booklets include clear diagrams which are easy-to-follow with links to useful websites and checklists. All of these will aid you in identifying and addressing your security and resilience needs.

Security – 'Secure in the Knowledge'
Thinking about security is good for your business. You have invested heavily in your business and you need to ensure it remains safe, secure and viable. The guidance provides information to help you improve your basic security and therefore protect your livelihood.

Resilience – 'Expecting the Unexpected'
Business resilience is a vital part of your business. Making it part of the way that you run your business, rather than having to 'firefight' any emergency, helps prepare you to offer 'business as usual' in the quickest possible time. Planned business continuity management, so that your staff, customers and suppliers are reassured that you have an effective policy and practice for managing the unexpected, helps build confidence in your business. This guide, (Expect the unexpected (522KB PDF)), will guide you in developing business continuity, helping you and your business to build resilience against any disaster.

'Counting The Cost'
Counting the cost provides guidance and information, primary for small and medium size businesses, that will help you to protect yourself.
It will enable you to:

- risk-assess the security and resilience needs of your business
- recognise threats and hazards
- understand better the role of insurance

This guide, (Counting The Cost (221KB PDF)), includes clear diagrams which are easy-to-follow with links to useful websites and checklists. All of these will aid you in identifying your security and resilience needs.

useful contacts

British Security Industry Association
Kirkham House
John Comyn Drive
Worcester
WR3 7NS United Kingdom
t: +44 (0) 845 389 3889
f: +44 (0) 845 389 0761
www.bsia.co.uk

ADS Group Limited
Salamanca Square
9 Albert Embankment
London, SE1 7SP United Kingdom
t: +44 (0)20 7091 4500
f: +44(0)20 7091 4545
www.adsgroup.org.uk

Fire Industry Association
Tudor House
Kingsway Business Park
Oldfield Road
Hampton, Middlesex
TW12 2HD United Kingdom
t:+ 44 (0) 20 3166 5002
f: +44 (0) 20 8941 0972
www.fia.uk.com

British Safety Industry Federation
93 Bowen Court
St. Asaph Business Park
St. Asaph, Denbighshire
LL17 OJE United Kingdom
t: +44 (0)1745 585600
www.bsif.co.uk

FCO (Foreign and Commonwealth Office)
www.fco.gov.uk

NaCTSO (National Counter Terrorism Security Office)
www.nactso.gov.uk

Centre for Protection of National Infrastructure (CPNI)
www.cpni.gov.uk

Home Office
www.homeoffice.gov.uk

local contacts

You may want to write here details of your local contacts.

Hospital
Telephone number
Address

Police
Telephone number
Address

Military
Telephone number
Address

Fire
Telephone number
Address

Ambulance
Telephone number
Address

Other local contacts for example, hotel association
Telephone number
Address

Other security and emergency services

notes

Produced by the National Counter Terrorism Security Office