SECURITY SERVICE
MI5


# PROTECTING AGAINST TERRORISM

# Top ten security guidelines

The following top ten protective security points summarise the guidance given in this booklet. Whether you are creating, reviewing, or updating your security plans, keep these key points in mind:

1. **Carry out a risk assessment** to decide on the threats you might be facing and their likelihood. Identify your vulnerabilities

2. If acquiring or extending premises, **consider security** at the planning stage. It will be cheaper and more effective than adding measures later

3. **Make security awareness part of your organisation's culture** and ensure security is represented at a senior level

4. **Ensure good basic housekeeping** throughout your premises. Keep public areas tidy and well-lit, remove unnecessary furniture and keep garden areas clear

5. **Keep access points to a minimum** and issue staff and visitors with passes. Where possible, do not allow unauthorised vehicles close to your building

6. **Install appropriate physical measures** such as locks, alarms, CCTV surveillance and lighting

7. **Examine your mail-handling procedures,** consider establishing a mailroom away from your main premises

8. When recruiting staff or hiring contractors, **check identities and follow up references**

9. Consider how best to protect your information and **take proper IT security precautions**. Examine your methods for disposing of confidential waste

10. **Plan and test your business continuity plans**, ensuring that you can continue to function without access to your main premises and IT systems.

This booklet is aimed at those who are responsible for the safety of others in businesses and in other organisations. It contains protective security advice derived from our role in advising organisations that own or operate key assets, services and systems which form part of the UK's critical national infrastructure.

# Contents

# Introduction

***Protecting Against Terrorism*** gives general protective security advice from MI5's National Security Advice Centre (NSAC). It is aimed at businesses and organisations seeking to reduce the risk of a terrorist attack, or to limit the damage terrorism might cause. The booklet is divided into three sections:

- **Section 1** deals with why you should consider protective security, with risk assessment, security planning and its implementation
- **Section 2** covers a range of security measures, from physical security and the protection of IT to staff selection and employment
- **Section 3** gives more specific information on the main type of bomb attacks, on how to protect against them and the recommended procedures to deal with bomb threats.

Further information may be found on **www.mi5.gov.uk**

***Protecting Against Terrorism*** supersedes ***Bombs – Protecting People and Property***, published by the Home Office in 1999. It is intended to give general advice and, as such, it is simply a starting point. If your organisation needs specialist advice tailored to its specific circumstances, contact the nationwide network of specialist police advisers known as Counter Terrorism Security Advisers (CTSAs) through your local police force. They are co-ordinated by the police National Counter Terrorism Security Office (NaCTSO), which is co-located with NSAC.

**Your CTSA can:**

- **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; your CTSA will be able to comment on its effectiveness as a deterrent, as protection and as an aid to post-incident investigation
- **Give advice on local installers of equipment**
- **Devise plans** and ensure their conformity with local arrangements, and the requirements of the police service and other emergency services
- **Offer advice** on search plans.

The work you undertake on protective security should be done in partnership with the police and your neighbours, if your community is to be secure. As well as safeguarding your business, the steps you take can make an important contribution to detecting terrorists.


# Section 1 | How to tackle protective security

## The importance of security planning

The bomb attacks in London in July 2005 demonstrated that the threat from terrorism is real and serious. Although actual attacks have so far been infrequent, it is possible that you may find yourself or your organisation caught up in a terrorist incident. This might include having to deal with a bomb threat or with suspect items sent through the post or left on the premises. In the worst case, you or your staff could be directly affected by a terrorist bombing.

Terrorism is not just about physical attack. It might take the form of attacks on vital information or communication systems, causing disruption and economic damage. Some attacks are easier to carry out if the terrorist is assisted either directly or indirectly by an 'insider', or by someone with specialist knowledge or access. Terrorism also includes threats or hoaxes designed to frighten and intimidate.

*Aftermath: wreckage of the Number 30 bus in Tavistock Square*

There are three strong business reasons why your organisation should plan to deter such acts, or at least to minimise their impact. They are:

- **Legal obligations**

In the event of an incident, your plans are likely to come under scrutiny. Health and safety at work regulations put the responsibility on the owner or occupier of the premises to provide a duty of care for staff and visitors. Although the police and other agencies can offer advice, it is up to the owner or occupier to seek out and act upon that advice. In any subsequent inquiries or court proceedings, you would need to show that you took the relevant legislation into account

- **Business continuity**

Ensure that your business is able to cope with an incident or attack and return to normality as soon as possible. This is particularly important for smaller businesses that may not have the resources to withstand even a few days without trading

- **Loss of reputation.**

In addition, make sure that your organisation has adequate insurance to cover terrorist threats – consult your insurance company or broker.

There is limited value in safeguarding your own business premises in isolation. Take into account your neighbours' plans and those of the emergency services, particularly if you are in a multi-occupancy building.

# Managing risks

If you think your organisation might be affected by a terrorist attack, you should apply appropriate protective security measures. Some institutions may be more at risk than others, especially if they have a higher public profile, but other factors can also play a part, such as the location of your business.

The diagram, right, illustrates a typical risk management cycle and the four steps you can take to protect your business.

## Step 1 Identify the threats

Ask yourself the following questions:

- What can be learnt from the Government and media about the current security climate and recent terrorist activities? (Visit **www.mi5.gov.uk** or refer to the *Useful contacts* section at the back of this booklet)
- Is there anything about the organisation, building or staff that might attract terrorist attack?
- Is there an association with high-profile individuals or organisations which might be terrorist targets?
- Could collateral damage occur from an attack on a high-risk neighbour?
- Is there anything terrorists might want to further their aims, e.g. materials, plans, technical expertise or access to other premises that might be targets?

## Step 2 Decide what you need to protect and identify your vulnerabilities

Priorities for protection should fall under the following categories:

- People (staff, visitors, contractors, customers)
- Physical assets (buildings, contents, equipment, plans and sensitive materials)
- Information (electronic and paper data)
- Processes (supply chains, critical procedures).

You know what is important to you and your business. You probably 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 hackers, 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 the business
- Any prestige targets that may be attractive to terrorists, regardless of whether their loss would result in business collapse.

As with Step 1, consider whether there is an aspect of your business or activities that terrorists might want to exploit to aid their work. If there are, how stringent are your checks on the people you recruit or on your contract personnel? Are your staff security conscious?

## Step 3 Identify the 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), each of which is covered in Section 2 of this guide. There is little point investing in costly physical

security measures if they can be easily undermined by a disaffected member of staff or by a lax recruitment process.

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.

If you need to introduce additional security measures, then make them more cost-effective by careful planning wherever possible. Introduce new equipment or procedures in conjunction with building work. In multi-occupancy buildings, shopping centres, high streets or business parks, try to agree communal security arrangements. Even if your neighbours 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.

### Step 4 Review your security measures and drills

You should conduct regular reviews and rehearsals of your security plans. This will help to ensure that they remain workable and up to date. You should be aware of the need to modify them to take account of any changes in your business. For instance, new building work, changes to personnel or revised health and safety procedures could have an impact on your plans.

Make sure that your staff understand and accept the need for security measures. Security should be seen as a common responsibility and not just something for security professionals. Make it easy for staff to raise concerns or report observations.

For more detailed information on risk assessment (including a check list to help identify the areas where your business may be vulnerable) refer to the publication ***Secure in the Knowledge***, which can be downloaded from **www.mi5.gov.uk**

## Creating a security plan

The risk management cycle described above requires the creation of a security plan. This is normally the responsibility of a Security Co-ordinator. If you do not already have a Security Co-ordinator, you should appoint one. In larger organisations the role should ideally be filled at board level and in smaller organisations it should similarly be a senior responsibility. Without a designated person with the proper authority to co-ordinate events, any security plan will not be fully effective. The Security Co-ordinator must be involved in planning and managing the building's interior security and external security, such as access control. It is also important that they are

consulted over any new building or renovation work (as in Step 3 of the risk management cycle on page 4).

## The Security Co-ordinator will have a number of key responsibilities:

- The production of a security plan based on the risk assessment
- Ensuring security measures are implemented and tested
- The formulation of other contingency plans dealing with bomb threats, suspect packages and possible evacuation
- Deciding when to re-occupy premises after they have been evacuated
- Liaising with the police, other emergency services and local authorities
- Arranging staff training, communication cascades and drills
- Conducting regular reviews of security measures and procedures.

**The Security Co-ordinator's first responsibility is the production of the security plan.** This should be produced in consultation with the emergency services, fully rehearsed and regularly updated. It should contain the following:

- Details of all the protective security measures to be implemented, covering physical, information and personnel security – these are covered in Section 2
- Instructions on how to respond to a threat (e.g. telephone bomb threat – see page 29)
- Instructions on how to respond to suspicious items or events
- A search plan
- Evacuation plans, including details on securing premises in the event of a full evacuation
- Business continuity plans
- A communications and media strategy which also 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 away to a safe distance
3. Prevent others from approaching
4. Communicate safely to staff, visitors and the public
5. Use hand-held radios or mobile phones away from the immediate vicinity of a suspect item
6. Notify the police
7. Ensure that whoever found the item or witnessed the incident remains on hand to brief the police.

# Business continuity planning

The focus of this booklet is on protective security – the practical steps you can take to reduce the risk of terrorism to your organisation and the physical impact should it occur. However, it is important to remember that protective security planning should go hand in hand with business continuity planning.

Business continuity planning is obviously not just driven by terrorism, but it would be critical to your business's survival if it was affected by a terrorist incident. And the benefits have an even wider impact. Every year nearly one in five businesses suffers a major disruption, and planning to deal with those disruptions is widely regarded as good business sense. Effective business continuity planning is critical to ensuring that the essential functions of your business can carry on despite an emergency.

Many businesses will already have plans to deal with sudden commercial risk. These may include events such as the failure of critical suppliers, an unexpected bad debt, industrial action or the discovery of a serious fault in a product or process. Planning for the aftermath of terrorist incidents is very similar.

*Buncefield depot explosion, 2005*

## Emergencies can jeopardise your organisation

For example, a major terrorist incident could have the following consequences:

- Damage to your buildings
- Loss of IT systems, records, communications and other facilities
- Unavailability of staff because of disruption to transport or their unwillingness to travel
- Loss of staff through death or injury
- Adverse psychological effects on staff, including stress and demoralisation
- Disruption to other organisations and businesses on which you may depend
- Damage to reputation
- Changes in the business demands placed on your organisation.

## You will need the right resources to maintain your critical business functions following a disruptive event

These are likely to include:

- Sufficient people with the necessary expertise and motivation to lead and manage the organisation
- Access to key records and IT systems
- Reliable means of communication, especially with your staff
- The ability to carry on paying staff, to ensure their safety and to provide them with welfare and accommodation
- The ability to procure goods and services
- The ability to respond to demands from the media.

## You should develop a business continuity plan in a systematic way

The booklet ***Expecting the Unexpected***, jointly published by the police National Counter Terrorism Security Office, London First and the Business

Continuity Institute, outlines five steps that you can follow to develop a business continuity plan:

1 **Analyse your business.** Working with the full support of senior management, you need to understand your business and the way it works, including which functions are essential and where vulnerabilities lie

2 **Assess the risks.** You need to understand what emergencies might affect your business and what impact they would have. By focusing on impacts rather than causes, you will make sure your plan allows you to deal effectively with an incident, no matter what the source

3 **Develop your strategy**. You will need to agree with senior management the organisation's appetite for risk. You can then decide which risks can be accepted, which risks can be reduced and which risks should be managed using business continuity planning

4 **Develop your plan.** You should then develop a business continuity plan covering the agreed areas. All plans look different, but they should be clear about roles and responsibilities, easy to understand and open for consultation and review around your organisation

5 **Rehearse your plan.** Rehearsal helps you to confirm that your plan will be connected and robust if ever you need it. Rehearsals are also a good way to train staff who have business continuity management responsibilities. Lessons from exercises can be used to refine your decisions in steps one to four.

## What you can do immediately

If you do not have a business continuity plan in place then consider how best to make your organisation more resilient while the plan is being developed. Designate a crisis management team led by senior staff, incorporate succession planning for key personnel and organise a robust telephone and/or e-mail cascade system for contacting staff outside working hours. Make sure copies of essential data or records are stored off-site and that IT systems can be accessed from other sites. Staff may continue to work from home if they have remote access to your IT systems. Ensure that you have robust banking and financial arrangements so that you can continue to make payments and sustain your business.

## Further advice

A wide range of advice on business continuity is available, much of it free. The Government's Preparing for Emergencies website (**www.pfe.gov.uk**) provides extensive information for business (including ***Expecting the Unexpected***) and links to key organisations. More detailed advice for business continuity professionals can be found at **www.ukresilience.info** and **www.mi5.gov.uk**. Other key contacts and publications are listed at the back of this booklet.

At the local level, the Civil Contingencies Act 2004 requires local authorities to provide advice and assistance to businesses in relation to business continuity management. Consult your local authority's website for further details.


# Section 2 | Protective security measures you should consider

## Physical security

Having conducted your risk assessment, you need to decide which physical security measures to adopt. In most cases they will range from basic good housekeeping (keeping communal areas clean and tidy) through CCTV, intruder alarms, lighting and computer security, 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 that is ineffective, unnecessary and expensive.

Contact your Counter Terrorism Security Adviser (CTSA) through your local police force at the start of the process. As well as advising you on physical security, they can direct you to professional bodies that regulate and oversee reputable suppliers. A reputable supplier can make a professional assessment of your requirements and recommend suitable products. Through the professional bodies, you can compare one provider with another. Before buying any security product, make sure you are clear about what it is designed to achieve and what guarantees and after-sales service you can expect.

As outlined in Section 1, in *Managing risks*, page 4, if you are part of a multi-occupancy building, shopping centre, high street or business park, make security a joint effort. For example, common access control procedures can be agreed or CCTV cameras sited for maximum overall benefit. This can both increase effectiveness and greatly reduce costs, while ensuring that health and safety regulations, fire prevention requirements and building consents are met. Remember that costs may be reduced if changes coincide with new building or refurbishment work, but do not let this delay the introduction of necessary equipment and procedures.

## Basic housekeeping

Basic good housekeeping reduces the opportunity for planting suspect packages and helps deal with false alarms and hoaxes. You can reduce the number of places where devices may be left by:

- Keeping public and communal areas – exits, entrances, reception areas, stairs, halls, lavatories, washrooms – clean and tidy
- Keeping the furniture in such areas to a minimum – ensuring that there is little opportunity to hide devices
- Locking unoccupied offices, rooms and store cupboards
- Ensuring that everything has a place and that items are returned to that place
- Considering the removal of litter bins or replacing them with clear bags
- Putting plastic seals on maintenance hatches
- Keeping external areas as clean and tidy as possible
- Pruning all vegetation and trees, especially near entrances, to assist in surveillance and preventing concealment of packages.

## Security awareness

The vigilance of your staff (including cleaning and maintenance staff) is key to your protective measures. They will know their own offices or work areas and should be encouraged to look out for unusual behaviour or items out of place. They must have the confidence to report any suspicions, knowing that reports will be taken seriously even if they turn out to be false alarms. Staff must also know who to report to and their contact details. Training is therefore particularly important. Staff should be briefed to look out for packets, 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.

## Access routes

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. Invest in good quality access controls such as magnetic swipe identification cards or ‘proximity’ cards which are readable from a short distance.

## Security passes

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

## Screening

The random screening of hand baggage is a significant deterrent and you have the right to refuse entry to anyone who does not allow you to search their possessions. However, body searches may be carried out only with the agreement of the person being searched. Routine searching and patrolling of premises represents another level of screening covering both internal and external areas. Keep the patrols regular, but not too predictable.

## Traffic and parking controls

If you believe you might be at risk from a vehicle bomb, the basic principle is to keep all vehicles at a safe distance. 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.

## Doors and windows

Good quality doors and windows are essential to ensure a building's security. External doors should be strong, well-lit and have good quality locks. You may want to consider alarms as well. Doors that are not often used should also have internal bolts and remember that, if you have glazed doors, they are only as strong as their glazing. All accessible windows should have good quality key-operated locks.

Many casualties in urban terrorist attacks are from 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 casualties, as well as the costs 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 installing new windows, consider laminated glass, but before undertaking any improvements seek specialist advice through your police CTSA or visit **www.mi5.gov.uk** for further details.

## Integrated security systems

Intruder alarms, 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 is as much a deterrent as a means of protection. If police response to any alarm is required, your system must be compliant with the Association of Chief Police Officers' (ACPO) security system policy (**www.acpo.police.uk**). For further information, contact the Alarms Administration Office at your local police headquarters.

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 court.

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

If you contract in staff who operate CCTV equipment, they must be licensed by the Security Industry Authority (SIA). This only applies if the CCTV equipment is deployed into fixed positions or has a pan, tilt and zoom capability and where operators:

- Proactively monitor the activities of members of the public whether they are in public areas or on private property
- Use cameras to focus on the activities of particular people either by controlling or directing cameras to an individual's activities
- Use cameras to look out for particular individuals
- Use recorded CCTV images to identify individuals or to investigate their activities.

Since 20 March 2006, contract CCTV operators must carry an SIA CCTV (Public Space Surveillance) licence – it is illegal to work without one. Your security contractor should be aware of this and you should ensure that only licensed staff are supplied.


*SIA licence for CCTV operators (example)*

# Managing staff securely

## 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 specifically in order to seek information or exploit the access that the job might provide.

Much of the following advice simply reflects good basic recruitment and employment practice. During the recruitment process you should ask each candidate to:

- Confirm their full name, date of birth and address with a supporting official document such as a full current passport or British photo driving licence. Other useful identifying documents are P45, credit card with statements, birth certificate, cheque book and bank card with signature and bank statements (account documentation from any UK financial institution is particularly useful as they will usually have made their own identity checks before opening an account). Ask to see recent utility bills confirming the given address. Do not accept as proof of identity any duplicate or photocopied documents, an international driving licence, an old British visitors passport or a birth certificate issued more than six weeks after birth
- Give their National Insurance number or other government-issued unique personal identifying number such as a National Health Insurance number
- Give evidence of academic or professional qualifications. Take up any references from schools, colleges, universities and previous employers (again, insist on originals) and check with the originators that they are genuine
- Give full details of previous employers (name, address and date) covering at least the past three years
- Give details of any unspent convictions, where allowed under the Rehabilitation of Offenders Act 1974. In certain circumstances – for example, where the post involves working with children or vulnerable adults – employers who are registered with the Criminal Records Bureau may seek details on the applicant's spent convictions. Remember, however, that a conviction – spent or unspent – need not be a bar to employment
- Provide proof of the right to work in the UK if relevant. For European Economic Area (EEA) nationals, ask to see their national identity card or passport and Home Office documentation confirming immigration status and permission to work.

Having obtained this information, check it: the increasing availability of reasonably good quality false documentation on the internet has made establishing identity more of a problem than it used to be. Look out for any obvious gaps and inconsistencies in the applicant's employment or residential history. All this will take time, so if you need the candidate to start work quickly, or if an offer of employment is made, then make the satisfactory completion of the checks a condition of employment. In all cases, remind applicants that supplying false information or failing to disclose relevant information could be grounds for dismissal and could amount to a criminal offence.

Personnel procedures intended to prevent criminal activity or terrorism may be regarded as unwelcome and intrusive. Whatever the circumstances, measures should be demonstrably proportionate to the perceived risks

and, as far as possible, staff should understand the risks and accept the measures taken to mitigate them. Think along the following lines:

- Make it easy for staff to discuss their concerns confidentially and informally
- Encourage managers and staff to be alert to anything unusual in employees' behaviour or attitudes, reassuring them that any information will be handled sensitively and confidentially. Note that any action taken as a result of such concerns must be in accordance with employment law
- Operate a security awareness programme to remind managers and staff of potential threats, both internal and external, and of their roles in countering them
- Permit access to sensitive locations, assets or information only to those who genuinely need it
- Consider imposing physical controls to restrict access to particularly sensitive areas, or random searching on entry and exit of staff in such areas. Explain the reasons behind such intrusive action.

After recruitment, it is important to try to identify any suspicious behaviour that might suggest unreliability or conflict of interest in a member of staff. Any possible early signs should be acted on, usually by discussion with the individual. Good personnel security is best achieved by creating a culture in which security is accepted. It should be easy for staff and managers to discuss their concerns and problems about others privately and informally. You may want to consider some form of confidential reporting line, sometimes known as whistle blowing.

Staff might be affected by altered circumstances that compromise their trustworthiness regardless of their professional standing and previous reliability. This can be the result of a wide range of life events, from stressful personal or working circumstances to deliberate recruitment by malicious third parties. Circumstances leading to vulnerability might be subtle and difficult to recognise but could include financial difficulty, peer, family or external group pressure and perceptions of unfairness at work.

**Other potential warning signs to watch out for are:**

- Drug or alcohol misuse
- Expression of support for violence-prone views, actions or incidents
- Major unexplained changes in lifestyle or expenditure
- Sudden loss of interest in work, or overreaction to career changes or disappointments
- Manifestations of stress such as over-emotional behaviour
- Unusual interest in security measures or areas of work outside the normal remit
- Changes in working patterns, for instance working alone or at unusual hours, failing to take holidays
- Frequent unexplained absences
- Repeated failure to follow recognised procedures
- Unusual travel abroad

- Relationships with or support for individuals or institutions that are generally regarded as professionally suspect
- Sudden or marked change in religious, political or social affiliation or practice which has an adverse impact on the individual's performance or attitude to security.

Individual cases will have unique features and it may take a combination of behaviours and attitudes to warrant further concern. It is important to note that some of these signs may be the result of ill-health. You should allow for this in your consideration of them.

You may also wish to consider whether to undertake checks for existing staff where this has not already been done to a satisfactory level.

If you have serious reason to suspect that you are being bugged or subject to other forms of electronic eavesdropping, do not report your suspicions over a telephone or from the place that is suspect. Use a public telephone box or mobile phone away from the building in question. There are some commercial security firms that can sweep your premises and equipment, but report any serious suspicions of espionage on behalf of terrorists or foreign powers to the police.


*SIA licence for security guards (example)*

Since 20 March 2006, all contracted-in security guards, key holders, CCTV operators (see also page 13), cash and valuables-in-transit personnel and close protection operatives must hold a licence from the Security Industry Authority (SIA). The licence gives you the assurance that they have passed an identity check, criminal record check and achieved the level of competency required to do the job. If your organisation buys in security then many of the checks recommended for personnel vetting will have already been done.

## Contractors and agency staff

The use of contractors and agency staff for many services (e.g. IT support, cleaning, catering, security guarding and consultancy) can create additional vulnerabilities and expose businesses to greater personnel security risks. While some agencies may be careful in their selection procedures, the less rigorous are open to exploitation by terrorists and sympathisers. Therefore, you should:

- Make it a contractual obligation that contractors validate the identities and bona fides of their staff
- Conduct regular monitoring of contractors' compliance with the contract

- Establish that each contractor is part of a recognised professional organisation responsible for accrediting standards in that industry
- Confirm that the individual sent by the contractor or agency is the person who actually turns up. For instance, ask the contractor to provide an authenticated photo of the individual, together with their full name, in advance of arrival. Ask the individual to provide photo identification that can be checked on entry
- Provide photo passes to contract staff, once you are satisfied that the person who turns up on the day is genuine. The pass must be worn at all times. Ideally, the employer should retain the pass between visits and hand it over only once the photo has been checked
- Agree a procedure for substituting contract staff with temporary replacements when the usual contract staff are away or ill; consider whether the replacement's duties or access need to be restricted
- Supervise where possible contract staff whenever they are on the premises and particularly if they have access to sensitive areas
- Nominate a permanent member of staff to be responsible in personnel terms for contract staff (i.e. not merely for overseeing delivery of the contract), so that potential security problems may be identified and addressed early.

# Information security

The theft, copying or destruction of information is a problem for many organisations. Your confidential information may be of interest to business competitors, criminals, foreign 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 protective measures you should:**

- **Assess the threat and your vulnerabilities** (see section on *Risk assessment* on page 4). 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 basic security measures** to protect paper-based information such as operating a clear desk policy, not leaving sensitive information lying around or displayed on notice boards, using secure cabinets, locking appropriate doors and giving guidance to staff, especially those who have to take information off the premises.

## Electronic attack

Electronic attack could:

- Allow the attacker to remove 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 hardware or software devices 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:

**Hacking**

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

**Malicious software**

The techniques and effects of malicious software (e.g. viruses, worms, trojans) are as variable as they are widely known. The use of e-mail, systems that interconnect, external contractors and remote access (e.g. for home working) allows virus infections to spread ever more widely and rapidly.

**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. The purpose of such modifications would be to allow a subsequent attack to be made, possibly by remote activation.

**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.

## What to do

- 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 *Managing staff securely*, page 13)
- Consider encryption packages for material you want to protect, particularly if taken off-site – 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.

Government and local government organisations, as well as those dealing with government or other sensitive work, can seek advice on computer security from the National Infrastructure Security Co-ordination Centre (NISCC) – visit **www.niscc.gov.uk**.

## 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. As a result, an important corporate merger was severely undermined
- 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
- Former employees remotely connected to a transatlantic shipper's system from a competitor's office premises. They caused havoc by creating false multimillion pound transatlantic shipping orders.

# 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, information falling under the Data Protection Act, 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

A cross-cutting shredder should be used so that no two adjacent characters are legible. This produces a shred size of 15mm x 4mm assuming a text font size of 12.

## 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 authority). 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 papier 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.mi5.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.

# Section 3 | Bombs and how to deal with them

## Bomb attacks

This section provides additional information on specific types of bomb attacks and how you can protect against them. Even during periods of heightened terrorism, the chances of anyone being directly affected by a bomb attack are low, but if you think you are at greater risk from terrorism, contact your local Counter Terrorism Security Adviser (CTSA) who can help with your risk assessment plan.

**Most terrorist bombs are improvised** and so are known as improvised explosive devices or IEDs. They can be categorised by their means of delivery:

- Vehicle (car, lorry, bike)
- Letter (parcel or packet)
- Person-borne (rucksack, briefcase, handbag or concealed on the body).

They can also be categorised by content, e.g. chemical, biological, radiological, nuclear, incendiary or conventional IED.

If you have reason to believe you might become the target of a bomb attack, you should assess the threat and potential damage and plan how to prevent

or mitigate it, as outlined in Section 1 of this booklet. Always bear in mind the importance of communications with staff, whether to inform, update or to reassure (for further information see the section on communications on page 34).

*South Quay, London Docklands, 1996*

## Vehicle bombs

Vehicle bombs 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 they can cause a great deal of damage. In general, vehicle bombs break down into three categories:

- **Under vehicle improvised explosive device (UVIED)**

A UVIED is a type of small, 'booby-trap' IED placed in, on or under a vehicle, and designed to explode when the vehicle moves, killing or injuring the occupants

- **Vehicle-borne improvised explosive device (VBIED)**

A VBIED is a car or van filled with explosive, driven to a target and then detonated

- **Large vehicle-borne improvised explosive device (LVBIED)**

An LVBIED is a lorry or truck filled with explosives. These vehicles enable terrorists to carry very large amounts of explosives, possibly several tonnes, to a target and are capable of causing casualties and destruction over a range of many hundreds of metres.

Vehicle bombs typically use an improvised explosive or incendiary mixture to provide the explosive charge. The bomb can be made at leisure and at a safe distance from the target. The explosives may be concealed in a container such as a beer keg, dustbin, wheelie bin or large suitcase.

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 it can be detonated on the spot by a suicide bomber.

Building a vehicle bomb requires a significant investment of time, resources and expertise. Because of this, terrorists will seek to obtain the maximum impact for their investment. They generally choose high-profile targets where they can cause the most damage, inflict mass casualties and attract widespread publicity.

### What you can do

If you think your organisation may be at risk from any form of vehicle bombing you should:

- Ensure that an identified individual is responsible for security and that the police know your plans and the layout of your building
- Employ basic good housekeeping such as vehicle access controls and parking restrictions

- Consider using physical barriers to keep all unauthorised vehicles at a safe distance. Seek police advice on what these barriers should be and on further measures such as electronic surveillance
- Where possible, vehicles that are permitted to approach your building should be authorised in advance and searched. The identity of the driver should also be cleared in advance
- Do what you can to make your building more blast resistant, paying particular attention to windows. Have the building reviewed by a qualified security engineer when seeking advice on protected spaces (see page 33). You may wish to obtain further technical advice regarding communications and announcement systems
- Establish and rehearse bomb threat and evacuation drills (see page 32). Bear in mind that, depending on where the suspected vehicle bomb is parked and the design of your building, staff may be safer in windowless corridors or basements than outside. Assembly areas for staff 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 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
- Train and rehearse your staff in identifying suspect vehicles, and in receiving and acting upon bomb warnings. Key information and telephone numbers should be prominently displayed and readily available.

## Letter bombs

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

Letter bombs may be explosive or incendiary (the two most likely kinds), or conceivably 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 letter bomb will probably have received fairly rough handling in the post and so is unlikely to detonate through being moved, but any attempt at opening it may set it off. Unless delivered by courier, it is unlikely to contain a timing device. Letter bombs come in a variety of shapes and sizes; a well-made one will look innocuous but there may be tell-tale signs (for further information on chemical, biological or radiological letter bombs see page 28).

**Indicators of a letter bomb:**

- 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 foreign 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 30g, whereas most effective letter bombs weigh 50–100g and are 5mm or more thick
- It has more than the appropriate value of stamps for its size and weight
- It is marked 'personal' or 'confidential'
- It is oddly shaped or lopsided
- The envelope flap is stuck down completely (a normal letter usually has an ungummed gap of 35mm at the corners)
- There is a pin-sized hole in the envelope or package wrapping
- There is any unusual smell, including but not restricted to almonds, ammonia or marzipan
- It has greasy or oily stains on the envelope
- There is an additional inner envelope and it is tightly taped or tied (however, in some organisations sensitive material is sent in double envelopes as standard procedure).

## What you can do

Although any suspect item should be treated seriously, remember that the great majority 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 police CTSA on the threat and on 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 the building
- Make sure that all staff who handle mail are briefed and trained. Include reception staff. Encourage regular correspondents to put their return address on each item
- Ensure that all sources of incoming mail (e.g. Royal Mail, couriers, 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 CBR materials themselves. At present, no CBR detectors are consistently 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 CBR material should ideally be placed in a double-sealed bag

- Consider whether staff handling post need protective equipment such as latex gloves and face masks (seek advice from a qualified health and safety expert). Keep overalls and footwear available in case staff need to remove contaminated clothing
- Make certain that post opening areas can be promptly evacuated. Rehearse evacuation procedures and routes (see page 32), which should include washing facilities in which contaminated staff could be isolated and treated
- Prepare signs for display to staff in the event of a suspected or actual attack.

## Person-borne devices

**Hand-delivered IEDs**

These are usually carried in containers such as rucksacks or briefcases, which are chosen to blend in easily with the target surroundings. Given the requirement to be easily portable, such bombs are unlikely to weigh more than 25kg, although even an ordinary-sized briefcase can contain about 12kg of explosive. A 25kg suitcase bomb could destroy a house or cause serious structural damage to larger buildings.

Terrorists often increase the effectiveness of their bombs by packing them with nails, nuts and bolts or similar items to act as shrapnel. Such weapons can have a devastating effect in a small space.

**What you can do:**

- Operate general good housekeeping practices. Strictly control the access of staff and visitors to your premises. This greatly reduces the chance of a bomb being carried in
- At times of high alert, baggage searches may be the only available means of protection and deterrence
- Should a suspicious item be found during a search, under no circumstances should it be touched or moved in any way. The police should be informed immediately and they will ensure an appropriate response
- Consider physically restricting access from the reception area into the rest of the building, for instance by the use of full height access control barriers or doors.

**Suicide bombers**

Suicide bombers may use a lorry, plane or other kind of vehicle as a bomb or may conceal explosives on their persons. Both kinds of attack are generally perpetrated without warning. The most likely targets are symbolic locations, key installations, VIPs or mass-casualty 'soft' targets.

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

- Denying access to anyone or anything that has not been thoroughly

searched. Ensure that no one visits your protected area without your being sure of his or her identity or without proper authority. Seek further advice through your local police force's CTSA

- Establishing your search area 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 the police
- Effective CCTV systems can help prevent or even deter hostile reconnaissance, and can provide crucial evidence in court
- There is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the police.

## Other methods of attack

Terrorists can use weapons such as mortars and rocket-propelled grenades to deliver an explosive fixed projectile into a site or premises from outside the perimeter in a 'stand off' attack. The range and size of explosive warhead varies considerably, depending on the type of weapons, which may be of military origin or homemade. Such attacks are rare and often require a level of expertise which exceeds that required for a simpler IED attack.

## Incendiary devices

These are generally hand-carried devices, often deployed against economic targets such as retail outlets and transportation. The usual intention is to cause economic damage and weaken public confidence rather than cause mass casualties.

When planning protective measures, remember that incendiaries are generally small, that they ignite rather than explode (often when the target premises are empty) and that there is usually more than one device. The attacker will regard the attack as a success even if they do no more than trigger the sprinkler system, which itself can damage stock or furnishings. Incendiary devices are fairly simple to make and do not require access to explosives.

### What you can do:

- Make security measures part of your normal anti-crime precautions, along with regular checks on fire extinguishers, sprinklers, smoke alarms and fire blankets
- Conduct discreet searches during business hours at times of high risk. Staff should be trained in what to look for but do not need a high degree of knowledge since most devices are not elaborately concealed; the terrorist needs to find easily accessible hiding places
- Since anyone finding a suspect device will probably be unable to tell whether it is incendiary or explosive, brief them to clear the surrounding area and call the police. If a device ignites, it may be sensible to make an immediate and brief attempt to extinguish it – provided normal fire arrangements and staff training are adequate. Remember, however, that there may be a number of devices and be prepared to evacuate the building according to pre-arranged plans.

## Chemical, biological and radiological attacks

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.

A radiological dispersal device (RDD), often referred to as a 'dirty bomb', is typically a device where radioactive materials are combined with conventional explosives. Upon detonation, no nuclear explosion is produced but, depending on the type of the radioactive source, the surrounding areas become contaminated. As well as causing a number of casualties from the initial blast, there may well be a longer-term threat to health. A number of terrorist groups have expressed interest in, or attempted to use, a 'dirty bomb' as a method of attack.

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 of 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. 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.

The likelihood of a CBR attack remains low. 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 within the building, 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 (see page 16).

### What you can do:

- Review the physical security of your air-handling systems, such as access to intakes and outlets
- 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. Refer to page 24 for further information
- 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 and, in the event of a CBR incident, the emergency services would come on scene with appropriate detectors and advise accordingly. 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 letters and packages) should offer a good level of resilience. In the first instance, seek advice from your local police force CTSA
- If you have a designated protected space (see page 33) this may also be suitable as a CBR shelter, but seek specialist advice from your local police force CTSA 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, return to or enter the building.

## Chemical, biological or radiological materials in the post

Terrorists may seek to use chemical, biological or radiological materials in letter bombs. 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. garlicky, fishy, fruity, mothballs, peppery, meaty, rotten. 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 emergency services
- Review plans for protecting staff 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 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)
- 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 minimise the risk of inadvertent cross-contamination
- Ask people not to wander off – though you cannot contain them against their will
- You do not need to make any special arrangements beyond normal first aid provision. The emergency services will take responsibility for treatment of casualties.

# Procedures for handling bomb threats

Most bomb threats are made over the phone. The overwhelming majority are hoaxes, often the work of malicious jokers, although terrorists also make hoax calls with the intent of causing alarm and disruption. Any such hoax is a crime and, no matter how ridiculous or unconvincing, should be reported to the police.

### Calls from terrorists may be of two kinds:

1 **Bomb threats when no bomb has actually been planted.** These hoaxes may not be merely malicious but designed to disrupt, to test reactions or to divert attention

2 **Bomb threats warning of a genuine device.** These may be attempts to avoid casualties, but they also enable the terrorist to blame others if there are casualties.

Even genuine threats are frequently inaccurate with regard to where and when a bomb might explode, and staff receiving a bomb threat may not always be those trained and prepared for it. But although they may be unable to assess a threat's accuracy or origin, their impressions of the caller could be important.

Receiving such a threat may be the closest that many people ever come to acts of terrorism, so be prepared for affected staff to be temporarily in a state of shock. Affected individuals may need counselling or other support.

## Base your bomb threat procedure on the following:

- **Ensure that all staff who could conceivably receive a bomb threat are trained in handling procedures** – or at least have ready access to instructions. This applies particularly to courts, banks, hotels, hospitals, news agencies, public transport organisations, voluntary organisations and those offering any sort of emergency service. Switchboard operators should be familiar with procedures and rehearse them regularly
- Draw up, ideally with advice from your local police CTSA, **a clear and accessible list of actions** to take on receipt of a call (see below), or use the *Bomb threat checklist* at the back of this booklet. Your list should include the following instructions:

1 **Stay calm and listen**

2 **Obtain as much information as possible** – try to get the caller to be precise about the location and timing of the alleged bomb and try to establish whom they represent. If possible, keep the caller talking

3 **Ensure that any recording facility is switched on**

4 When the caller rings off, **dial 1471** (if that facility operates and you have no automatic number display) to see if you can get their number

5 **Immediately tell the designated Security Co-ordinator**. It is their responsibility to decide on the best course of action and who should notify the police. If you cannot get hold of anyone, and even if you think the call is a hoax, inform the police directly. Give them your impressions of the caller as well as an exact account of what was said

6 If you have not been able to record the call, **make notes for the security staff or police**. Do not leave your post – unless ordered to evacuate – until the police or security arrive.

# Search planning

Search planning should be incorporated into your overall security plan (see Section 1). Searches may be conducted as part of routine good housekeeping – in shops, for example, at the close of business or when there is a security alert in your area.

Staff involved in searching your premises must be familiar with the areas they are searching and with what they would normally expect to find there, but they do not need to be experts in explosives or other devices. **In particular, they should look for anything that should not be there or is out of place, and anything that cannot be accounted for**. Ideally, staff should search in pairs to ensure nothing is missed.

Searches are also made following evacuation. In this instance, it is the responsibility of the police to confirm that the building is safe for re-occupation. If a search is required, the police may need the assistance or involvement of your staff, who will have a far better knowledge of the premises.

## When preparing a search plan you should:

- **Appoint a Search Co-ordinator** to produce and maintain your search plan. He or she should initiate any searches and liaise with other searchers
- **Divide your building into search sectors**, each of a manageable size for one or two searchers
- **Prioritise the important areas that need to be searched**, particularly those areas open to the public, other vulnerable areas such as cloakrooms, stairs, corridors and lifts, as well as evacuation points and routes, car parks and other outside areas such as goods or loading bays
- **Consider how to initiate the search:**
  - By sending a message over a public address system (perhaps coded to avoid unnecessary disruption and alarm)
  - By personal radios or pagers
  - By telephone cascade
- **Ensure the searchers know what to do** on discovering a suspicious item – under no circumstances should it be touched or moved in any way – and the police should be informed immediately
- **Check your search plan with your local police CTSA and practise it regularly.**

# Evacuation planning

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

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

**Remember that in any bomb threat warning, the time given for an explosion is unlikely to be accurate.**

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 right past a suspect device outside your building, or through an area believed to be contaminated, evacuation may not be the best course of action. You might have to consider the use of protected spaces (see page 33).

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.

The decision to evacuate will normally be yours, but the police will advise. In exceptional cases they may insist on evacuation, although they should always do so in consultation with your Security Co-ordinator.

Planning and initiating evacuation should be the responsibility of the Security Co-ordinator (see Section 1). Depending on the size of your business 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 letter bomb found in the post room)
- Full or partial evacuation to an internal safe area, such as a protected space, if available (see page 33)
- 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. Appoint people 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 police cordons – although

it would be advisable to have an alternative about 1km away. Car parks should not be used as assembly areas.

Disabled staff should be individually briefed on their evacuation procedures. Many organisations advise the use of firefighter lifts for evacuating disabled staff in the event of an incident.

**In the case of suspected:**

- **Letter or parcel bombs**

Evacuate the room and the floor concerned and the adjacent rooms along with the two floors immediately above and below (see also page 23)

- **CBR incidents**

Responses to CBR incidents will vary more than those involving conventional or incendiary devices (see also pages 26 to 29), but the following general points should be noted:

- The exact nature of an incident may not be immediately apparent. For example, an IED might also involve the release of CBR material
- In the event of a suspected CBR incident within the 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 the building, close all doors and windows and switch off any systems that draw air into the building.

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

Building 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.

# 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 or concrete walls, e.g. internal corridors, toilet areas or conference rooms with doors opening inwards
- Away from windows, external doors and 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 the blast can travel up them. If, however, the stair and lift cores are entirely enclosed, they could make good protected spaces
- Avoiding ground 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 and communications.

Consider duplicating critical systems or assets in other buildings at 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 parts of your building that offer similar protection to that provided by a protected space.

## Communications

Ensure that designated 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 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, 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 will 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 (see page 12). If your premises are already open plan and there are no suitable protected spaces, then evacuation may be your only option.

**Evacuation or moves to protected spaces should be practised and tested on a regular basis.**

# Bomb threat checklist

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

Photocopy this form or visit **www.mi5.gov.uk** to download the pdf and print it out.

## Actions to be taken on receipt of a bomb threat:

- **Switch on 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 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 Security Co-ordinator of name and telephone number of the person informed:** _____
- **Contact the police on 999. Time informed:** _____

## The following part should be completed once the caller has hung up and the Security Co-ordinator and the police have been informed.

- **Time and date of call:** _____
- **Length of call:** _____
- **Number at which the call was received (i.e. your extension number):** _____

## About the caller

- **Sex of caller:** _____ **Age:** _____
- **Nationality:** _____

✓ **Tick** where appropriate

## Language

- ☐ Well spoken
- ☐ Irrational
- ☐ Taped message
- ☐ Offensive
- ☐ Incoherent
- ☐ Message read by threat maker

## Caller's voice

- ☐ Calm
- ☐ Crying
- ☐ Clearing throat
- ☐ Angry
- ☐ Nasal
- ☐ Slurred
- ☐ Excited
- ☐ Stutter
- ☐ Disguised
- ☐ Slow
- ☐ Lisp
- ☐ Accent

Type of accent

_____

- ☐ Rapid
- ☐ Deep
- ☐ Hoarse
- ☐ Laughter
- ☐ Familiar

If so, whose voice did it sound like?

_____

_____

## Background sounds

- ☐ 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: _____

# Useful contacts

**Association of Chief Police Officers**
Tel: 020 7227 3434
www.acpo.police.uk

**The Business Continuity Institute**
Tel: 0870 603 8783
www.thebci.org

**British Standards Institute**
www.bsi.org.uk

**Criminal Records Bureau**
Tel: 0870 90 90 811
www.crb.gov.uk

**Home Office**
Tel: 020 7035 4848
www.homeoffice.gov.uk

**ITsafe** (information security)
www.itsafe.gov.uk

**London Prepared**
www.londonprepared.gov.uk

**Loss Prevention Certification Board**
www.brecertification.co.uk
www.redbooklive.com

**Metropolitan Police Anti-terrorist Branch**
Hotline: 0800 789321
www.met.police.uk

**MI5 – The Security Service**
www.mi5.gov.uk

**National Infrastructure Security Co-ordination Centre (NISCC)**
www.niscc.gov.uk

**Preparing for Emergencies**
www.pfe.gov.uk

**Security Industry Authority (SIA)**
Tel: 020 7227 3600
www.the-sia.org.uk

**UK Government's Computer Emergency Response Team (UNIRAS)**
www.uniras.gov.uk

**UK Police Service**
www.police.uk

# Useful publications

***Expecting the Unexpected***

This guide is the result of a partnership between the business community, police and business continuity experts. It advises on business continuity in the event and aftermath of an emergency and contains useful ideas on key business continuity management processes and a checklist.

***Secure in the Knowledge***

This guide is aimed mainly at small and medium-sized businesses. It provides guidance and information to help improve basic security. Ideally it should be read in conjunction with *Expecting the Unexpected* which is mentioned above. By following the guidance in both booklets, companies are in the best position to prevent, manage and recover from a range of threats to their business.
Both booklets are available to download at **www.mi5.gov.uk**

For copies of *Protecting Against Terrorism* email nsacenquiries@nsac.gsi.gov.uk

This publication was produced in partnership with the Cabinet Office, the Home Office and ACPO.

HM Government


National Counter Terrorism Security Office

And supported by London First and the CBI.

Ref: 272839/0306/D88