PROTECTING AGAINST TERRORISM

THIRD EDITION

CPNI
Centre for the Protection of National Infrastructure

TOP TEN SECURITY GUIDELINES

The following protective security points summarise the guidance provided in this booklet. Whether creating, reviewing or updating security plans, keep these points in mind:

1. **Conduct a risk assessment** to decide on the threats the organisation might face and their likelihood. Identify existing and potential vulnerabilities and the impact of any breaches of security. **See pages 11-12**

2. If acquiring or extending premises, **consider security requirements** right from the planning stage. It will be cheaper and more effective than adding measures later. **See pages 13-26**

3. **Make security awareness a part of the organisation's culture**. Ensure staff are kept regularly informed and that security standards are fully supported at a senior level. **See pages 37-44**

4. **Ensure good basic housekeeping** throughout the premises. Keep public areas tidy and well-lit, remove unnecessary furniture and keep garden areas clear. **See page 17**

5. **Keep access points to a minimum** and issue staff and visitors with passes. Where possible, do not allow unauthorised vehicles close to the building. **See page 16**

6. **Install appropriate physical measures** such as locks, alarms, CCTV surveillance, complementary lighting and glazing protection. **See pages 17-18**

7. **Maintain appropriate mail-handling procedures**, consider establishing the mailroom away from the main premises. **See page 18**

8. When recruiting staff or contractors, **check identities and follow up references**. **See pages 23-26**

9. Consider how best to protect information and **take proper IT security precautions**. Ensure there are appropriate provisions for disposing of confidential waste. **See pages 19-22**

10. **Plan and rehearse business continuity and incident response plans**, make sure that key business functions can continue during disruptions. **See pages 27-36**

PROTECTING AGAINST TERRORISM

CONTENTS

PROTECTING AGAINST TERRORISM

This publication offers security advice and good practice for any organisation looking to protect against the risk of a terrorist act or limit the damage such an incident could cause.

It sets out how a security plan might be developed and updated, the key measures that can help protect staff, property and information and how businesses can prepare for the worst.

Protecting Against Terrorism is an overview of the security advice that derives from CPNI's work with the national infrastructure. Although aimed primarily at countering potential terrorist attacks, much of it represents good practice for businesses of any size, whether private or public sector.

It is intended as a starting point. Any major decisions or investment relating to protective security should always be taken in consultation with the wider sources of advice and information that are available and referenced throughout the following pages.

What is CPNI?

The Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides advice on protecting the country's essential services, facilities and networks from terrorism and other threats.

It is an interdepartmental organisation of experts and security specialists drawn from across government, police, the Security Service, academia and the private sector. It provides advice and research across physical, information and personnel security for the nine sectors that form what is known as the 'national infrastructure' and which provide the services that support everyday life:

- **Communications**
- **Energy**
- **Emergency services**
- **Financial services**
- **Food**
- **Government**
- **Health**
- **Transport**
- **Water**

More information about the work of CPNI, including some of the publications and guidance mentioned in *Protecting Against Terrorism,* is available from www.cpni.gov.uk.

CPNI
Centre for the Protection of National Infrastructure

Please note that previous editions of *Protecting Against Terrorism* were published by the Security Service (MI5). CPNI was formed in 2007 at which time it assumed responsibility as the government authority for protective security advice.

IMPORTANCE OF SECURITY PLANNING

There are sound commercial, legal and reputational reasons why organisations should keep security under constant review.

The threat from terrorism to the UK remains both real and serious. An attack could take place at any time without warning and any organisation could be affected – from the disruption caused by a suspect item found on its premises to, in the worst case, staff caught directly in the midst of a violent attack.

Acts of terrorism vary in terms of scale and purpose. Some seek merely to inflict superficial damage or cause public distress to draw attention to a particular cause. But others carry a more malicious intent.

Terrorism is not just about violent attacks on people and property. Disrupted communications systems, damaged assets and tarnished reputations can cause immediate and/or long-term harm to a business and so equally desirable from the terrorist point of view.

Threat to the UK

The most significant threat facing the UK comes from international terrorism and its stated ambitions to mount 'high impact' attacks that combine mass casualties with substantial disruption to key services such as energy, transport and communications. This is a threat that is different in scale and intent to any that the UK has faced before.

Northern Ireland-related terrorism also continues to pose a serious threat. Despite a peace process that has been active for several years, dissident republican terrorist groups have continued to attack economic and political targets.

Whilst anti-terrorism operations have achieved considerable success – in particular against international terrorism (see **CONTEST** information opposite) – the intelligence accumulated during police investigations and subsequent trials reveals that terrorist groups, both at home and abroad, continue to target UK citizens, businesses and interests.

Wider threats to business

Businesses also face a range of other threats that possess the potential to cause significant disruption: activist groups driven by political or social issues; organised crime; foreign intelligence agencies looking to advance domestic interests; competitors seeking a commercial edge; an amateur hacker showcasing their skills; or premeditated burglaries and opportunistic thefts. Even a member of staff, present or former, with a score to settle or opportunity they couldn't resist could present a risk to a business.

Prepared for the worst

Organisations need to be prepared. Even if the likelihood of being directly targeted by terrorists are remote, the repercussions of an attack elsewhere can spread right across the economy. Could a business still function if, for example, key suppliers or clients were directly affected, if telephone networks went down or if power supplies were cut? What if deliveries could not be made or payments completed?

No single security response or level of investment will provide 'total' protection. Nor is it practical for a business to invest in every solution available on the market. However, a considered and up-to-date security plan, one that is appropriate to the organisation and in proportion to the risks it faces, can help to protect against the worst possible consequences.

Good security is essential not only because it provides reassurance to staff, investors and clients, but because there are legal and commercial responsibilities to take into account:

Health and safety

Health and safety at work regulations place a legal responsibility on the owner or occupier of premises to have a 'duty of care' for staff and visitors. In the event of an incident, any subsequent inquiry or court proceeding will look for evidence that the relevant legislation was followed.

Business continuity

In the event of an incident, organisations must aim to return to 'business as usual' as soon as possible. This is particularly important for smaller businesses which may lack the resources to withstand more than a few days without trade.

Loss of reputation

The reputational damage of a security breach is something that will concern all senior management – the loss of trust following a failure to protect staff, clients or even data may prove difficult to recover.

Costs

Lost or destroyed assets may need to be replaced quickly and at great cost. This is in addition to any losses that might be incurred through the suspension of normal business.

Find out more...

CONTEST – The UK government's strategy for countering international terrorism

CONTEST is the government's comprehensive strategy to reduce the risk we face from international terrorism. Launched in 2003, and revised in 2009, it is based upon four key elements: Pursue, Prevent, Protect and Prepare.

The strategy involves thousands of people – intelligence officers, the emergency services, local authorities, businesses, voluntary and community organisations, governments and other partners – working in partnership at an international, national and local level.

For more information about the UK counter-terrorism strategy visit www.security.homeoffice.gov.uk

THE SECURITY PLAN

A security plan should be informed, integrated and multi-layered.

Businesses cannot remove all of the threats they may face, but they should possess a plan to protect their most valued assets and prepare their response to major disruptions.

Security planning must not evolve in an arbitrary or ad-hoc manner, nor develop solely from previous mistakes and errors. To be effective, plans must be built on information about almost every aspect of the business both now and into the future. It must be fully integrated with everyday operations, supply chains and routines. And it needs to be 'multi-layered' – where each measure is reinforced by the next.

The structures and terminologies will differ from one organisation to the next but each plan should broadly consist of the following components:

Information:
An assessment of the business and the environment in which it operates – the threats, the vulnerabilities, its most valued and critical assets.

Protective security:
The measures that protect against identified threats and vulnerabilities.

Response planning:
How the organisation will respond in the event of disruption.

Security culture:
Building security awareness across the organisation.

Developing a security plan

Large, multi-site organisations might operate separate plans for each location to reflect local structures and activities in addition to an overarching plan setting out common actions and inter-dependencies.

Ownership

A security plan needs to be a working document where every aspect is constantly reviewed and updated in response to organisational changes in circumstances. For any plan to keep pace with issues as they arise it must be formally owned by a member of staff who can take on the responsibility for overseeing arrangements and who possesses the authority to co-ordinate actions.

In larger organisations this might be the role of a dedicated member of staff with board-level status or a direct report to the board, possibly with the support of a specialist team. In smaller organisations it should be someone with similar influence and understanding of the business.

Whoever manages the plan will need to take full interest in almost every aspect of the business. From recruitment to IT policies, from outsourced services to new building and renovation work – there are security implications to almost every major decision.

Senior management support

Whatever the size of the organisation, it is crucial that the plan carries the full support of senior management and that this is communicated throughout the business, particularly where certain members of staff carry delegated responsibilities. In the event of an incident, the authority of those responsible for co-ordinating the response must be clearly understood by all staff.

Collaboration

The exchange of advice and information is an important part of all security plans. The opinions of senior management and staff across the organisation will be essential, but so too will be contributions from those outside the business such as the emergency services, neighbouring businesses and specialist experts (structural engineering, IT etc).

Confidentiality

The security plan will contain some of the most sensitive information available about the business and so it is important to be clear who has full access and how it is distributed. This applies to internal staff as much as when consulting the opinions of external partners.

The following pages in Protecting Against Terrorism *offer a guide to some of the points to consider when developing and maintaining a security plan. More detailed advice on every aspect is available from www.cpni.gov.uk. Other relevant resources are highlighted throughout the document.*

The starting point is to gather as much information as possible about the diverse threats a company might face in order to carry out a risk assessment exercise.

Find out more...

For further advice on producing security plans:

Secure in the knowledge – building a secure business
available from both: www.cpni.gov.uk and www.nactso.gov.uk

See also
www.ukresilience.info
www.direct.gov.uk
www.uktradeinvest.gov.uk/ukti/osib
(Overseas Security Information for Business (OSIB))

IDENTIFY THE THREATS

What puts an organisation at risk?

Some businesses will be more 'at risk' than others because of the services they provide, their relatively high profile or the number of people they accommodate. But the impacts of any attack are rarely confined to the target and other businesses and communities can find themselves adversely affected as the full implications spread.

Organisations need to understand the range of threats they face, both direct – where the business itself is the target – and indirect, from the comparatively low-key to the catastrophic.

Direct

Businesses should be constantly asking what it is about their operations or circumstances that could put their staff or key assets directly in harm's way. For example:

- What is the nature of the business or the services provided?
- Is there anything on site that could represent a valuable target e.g. materials, data, plans, technical expertise?
- Is the business associated with a high profile individual or a contentious area of work?
- Does the organisation maintain visibly high standards of security?

In short, how likely is it that the business, or its staff, could be the direct target of a pre-meditated attack?

Indirect

There may also be the indirect impacts that result from an attack elsewhere – where the business itself was not the target but finds itself dealing with the consequences.

For example, are the business premises located near an iconic, high-risk building? If so, how would it affect operations if the entire area could not be accessed for several days? Would staff be able to travel if the local transportation network was severely disrupted?

Are IT networks able to react to the sudden emergence of a new virus or vulnerability?

Could an incident in another city, or another country, cause significant problems for suppliers, clients or the delivery of essential materials?

Other social factors can also increase the threats to a business. Would concerns about job security amongst the workforce raise the risk of employees stealing or selling information?

The wider picture

A threat assessment should not limit itself to information obtained only from internal resources. It should also take advantage of external sources of information.

Consult neighbouring businesses and trade associations to find out what they judge to be the major risks to the local economy. Request details about the security standards applied by key suppliers to the organisation. And contact the local authority for any contingency plans and other relevant information provided for businesses in the area.

Keep abreast of current affairs through the media and maintain a regular check of current government advice about the general security climate.

The following websites serve as useful sources of information to check periodically:

www.mi5.gov.uk
www.homeoffice.gov.uk
www.businesslink.gov.uk
www.crimereduction.gov.uk

Crime Reduction Officers – contacted through the local police service – can provide advice about general crime prevention. Organisations with a particular concern about being a target for terrorism should also make contact with their local Counter Terrorism Security Advisers (CTSAs – see below).

Attend one of the local Project Argus briefings held around the country. These are free events open to any business during which attendees – managers and their staff – are guided through a simulated terrorist attack in order to help understand their reactions and to plan initial responses to an incident. See www.nactso.gov.uk/argus.php for more information.

The threats to an organisation will constantly evolve so the overarching aim should be to not only understand the scale of the threat, but also to stay alert to changing internal and external factors so that assessments can be regularly updated.

Find out more...

Counter Terrorism Security Advisers

Counter Terrorism Security Advisers (CTSAs) are a network of specialist police advisers who assist businesses and services that might be vulnerable to terrorist or extremist attack; this includes ‘crowded places’ such as shopping centres, sporting stadia, pubs, bars and hotels.

There are around 250 CTSA officers, at least two for every police force area, who are specifically trained in areas such as explosives, pathogens and toxins, radiological sources and security surveying.

For more information about the work of CTSAs, to download their published advice or attend one of their Project Argus events mentioned above visit www.nactso.gov.uk.

NaCTSO
National Counter Terrorism Security Office

THE VULNERABILITIES

Which areas of the business should be a priority for protection?

When deciding what should be protected it might help to use the following categories:

- **People** – staff, visitors, contractors, customers.
- **Physical assets** – buildings, contents, equipment and sensitive materials.
- **Information** – IT systems, online transaction systems, electronic and paper data.
- **Processes** – supply chains, critical procedures, production cycle.

Organisations need a clear consensus about those assets which they regard as *valuable* and those they regard as *essential*.

Most valuable

1 Those assets which the organisation has a duty to protect – staff, client services, production systems etc.

2 High-value assets that are worth additional or specific security investment.

3 Unique assets which, though not necessarily of a high monetary value, would be difficult to replace.

Some priorities will be obvious with plans and provisions already in place. But it would be wrong to assume everything has been identified and appropriately secured. As with the threats, values can change with some assets continuing to be worth the protection they are afforded whilst others, in terms of security resources, may have become undervalued.

Most essential

The most valuable assets may not necessarily be the most essential.

The latter are those assets – equipment, information systems, transportation etc – vital to the day-to-day running of the businesses which, if lost or compromised, could have major implications for other parts of the business.

The task of identifying which assets are the most essential should not be completed through discussions amongst management alone. Staff across the organisation should be consulted about how the temporary loss of their department and its services will impact the business. Though all staff will contribute to the normal running of business, not all will be essential for delivering the basic services.

Making decisions about what is essential is also a key part of the Business Continuity Plan (see page 27).

Existing vulnerabilities

In addition to protecting key assets there is also the need to identify where existing security measures need to be improved.

This involves an honest appraisal about how current security measures are performing and whether they remain sufficient or are leaving areas of the business exposed. The security measures in place may still perform to their specifications but have simply been outgrown by the organisation.

Questions businesses should ask include:

- Have new methods or technologies emerged that will improve existing security?
- Is existing security sufficient for any planned business expansion?
- Are mobile devices being responsibly used by staff?
- Do all areas of the business undertake consistent pre-employment checks?
- Is there an increased rate of staff turnover – is it expected to rise?
- Are staff able to take valuable data offsite without approval?

Security planning depends upon honest assessments. Past failures should not be brushed under the carpet. Have any records been kept about previous security breaches or 'near misses'? Does this reveal any patterns or highlight occasions where procedures did not work but nothing was done about it?

There may be other reasons why the business, or part of it, is vulnerable because groups or individuals may be able to exploit them. For example:

- Does the company website provide too much detail about the business and how it operates?
- Is there anything that identifies installations or services vital to the continuation of the business?
- Is there sufficient separation of public areas and operational areas?
- Are outsourced services in safe hands – what are their security standards?
- Are goods delivery areas exposed – is there sufficient control of who comes in?
- Do procedures require passes to be returned and user accounts closed when staff leave?
- Do external parties enjoy privileged access to property or information?

Find out more...

For further advice on assessing vulnerabilities in the business:

www.cpni.gov.uk

www.nactso.gov.uk

www.bis.gov.uk

www.thebci.org (The Business Continuity Institute)

www.crimereduction.gov.uk

www.homeoffice.gov.uk/secureyourbusiness

THE RISK ASSESSMENT

Decisions about security should take account of the threats, vulnerabilities and potential impacts.

It is not practical to commit to fully protecting every aspect of the business all the time.

Instead, major decisions about protective security measures or changes in procedure should only be taken following a full risk assessment. This involves a strategic analysis of the threats, vulnerabilities and the potential consequences to the business in order to identify the most important risks on which to focus resources.

Basic principles

The risk assessment process involves making logical assumptions about the likelihood of a threat and its potential impact should current security measures fail to protect it.

Though it is not possible to predict all possible threats to a business, by working through a range of potential scenarios and consequences that could happen it becomes possible to make informed judgements about priorities for the business.

There are various ways to carry out a risk assessment exercise and each organisation and/or location should use its own methodology as appropriate, but the process is likely to be based on the following principles:

1 Having identified its key assets (pages 7-8) the first step for the organisation is to use the information gathered in its threat assessment to identify the possible risks it faces, ranging from the catastrophic to the relatively minor:

- A bomb in, or near, the main building entrance.
- A suspect package received through the post.
- An employee using their access to sell confidential information.
- A virus introduced into the main IT system.
- An employee discreetly transferring small funds to an unauthorised account.

The pages on physical, personnel and information security measures (pages 13-23) provide further examples – use a balanced representation from all three or undertake a separate exercise for each.

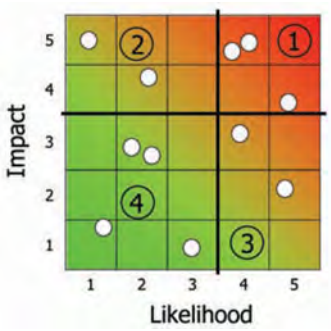
2 Allocate a simple score to denote the potential impact of each incident based upon an assumption about how it will affect the business (e.g. whether it could cause injuries and fatalities, financial losses, impact on productivity, reputation and client confidence).

Use a suitable scale for the business, e.g. score '5' for the worst possible outcome – it is almost certain that lives will be lost or buildings put out of use – but score '1' if it is likely the incident may be easily contained or recoverable at little cost and without publicity.

3 For each scenario put a second score representing the likelihood of the incident happening at each location. Consider why and how it could happen and how current security measures might perform (see pages 7-10).

Apply a similar consistent scoring system above, such as 1 ('extremely unlikely') to 5 ('certain'). For example, the likelihood of petty theft may score 5, but the chances of discovering an explosive device in the building may score 1.

4 When the two scores for each scenario are compared against other scenarios it starts to reveal the threats on which the business should focus.



It might help to plot the points on a 5x5 matrix using impact and likelihood as the axes. Best practice recommends looking at the scores in isolation – don't multiply them into a single figure as this can obscure results (i.e. a petty theft scores the same 5x1 as a bomb 1x5).

These scores are only indicative and the eventual actions agreed might still be swayed more by either the potential likelihood or impact, but this process should help to focus decisions. This exercise should be revisited regularly so that any changes in threat and vulnerability can be taken into account.

For more guidance about conducting risk assessments see *Risk assessment for personnel security* – and *Guide to producing operational requirements for security measures* available from www.cpni.gov.uk.

Appetite for risk

Whatever the method used to conduct the risk assessment it might help to categorise threats into a 'risk appetite', for example:

Protect	Areas where changes or improvements to current measures are necessary, either through new equipment or procedures.
Adapt	Risks that could be reduced through operational changes e.g. outsourcing, change of routines.
Accept	Risks judged as minimal where costs of mitigation/change outweigh benefit.
Contingency	Risks that will require plans to ensure there are alternatives or reserves – particularly assets deemed as essential to operations.

From this point an organisation should look at the strategies it needs to develop: the protective measures that can protect its interests and the response plans to ensure any incidents are efficiently managed.

Find out more...

For further advice on risk assessment:

www.cpni.gov.uk

www.businesslink.gov.uk

www.theirm.org (The Institute of Risk Management)

PROTECTIVE SECURITY

Physical, information and personnel security measures should complement and support each other.

What is protective security?

The most effective security response is likely to include a combination of physical, information and personnel security measures. Together, they work to secure a business through a mix of deterrence and detection, or by helping to minimise the consequences of any attack.

But all organisations are different – as are the sites and locations of which they comprise – so the appropriate mix of measures will depend on the nature of the risk-led assessment of the threats and vulnerabilities in each location.

Physical security

Physical security comprises the various installations, measures and controls that protect against an actual physical attack. For example:

- Intruder detection and alarms
- Access control systems
- Security guarding
- Hostile vehicle mitigation, including vehicle security barriers
- Blast protection

Information security

Information security measures aim to protect an organisation's data and its various forms of storage and distribution. This includes protecting IT systems against electronic attack as well as measures to secure information stored on mobile devices or paper:

- Network access control measures (typically enforced by 'firewalls')
- Electronic attack intrusion detection and prevention
- Identification and authentication measures (e.g. username/password)

Personnel security

Personnel security is about managing the risk of staff or contractors exploiting their legitimate access to an organisation for unauthorised purposes:

- Identity checking and pre-employment screening
- Risk assessment procedures
- Ongoing security measures

There is no value in directing all resources towards only one aspect of security – an extensive access control system will be of little use if the recruitment process does not track who is given legitimate access.

Instead, security should be developed around a 'multi-layered' principle where each layer supports the next and all working seamlessly together.

Appropriate and proportionate

Security measures can be resource intensive, costly and, if not carefully managed, can disrupt routines and alienate members of staff. This is why careful consideration and planning is required when choosing the right response and why specialist advice should be sought.

As a general guide, the following principles should be central to any decisions:

1 It is not possible to protect everything so **prioritise** the areas to protect.

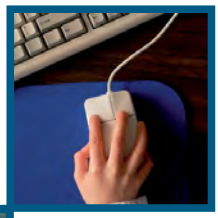
2 Measures should be **proportionate** to the threat.

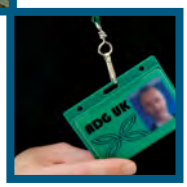
3 Do not let the cost exceed the **value** of the asset being protected.

4 Security is more **cost effective** when incorporated into forward planning.

The introduction of some measures can be made more cost-effective through careful planning. For example, a new access control system or the installation of reinforced glazing should be included at the start of any plans for building work or refurbishment. Similarly, the incorporation of sufficient security should be a key factor in the development of any new IT systems.

In certain situations – multi-occupancy buildings, shopping centres, high streets or business parks, for example – it might also be possible to agree communal security arrangements such as CCTV or external lighting and landscaping.





The following pages set out the various protective security measures that can help businesses reduce their vulnerability to attack.

Through factors such as the scale of the organisation, the available resources and the type of work it undertakes on site will dictate which are the most appropriate, an effective security response is likely to include a combination of physical, information and personnel measures.

PHYSICAL SECURITY

Physical security measures aim to prevent or deter direct attacks and reduce potential damage and injuries.

What to protect against

A physical attack is likely to involve a form of improvised explosive device (IED). These can be categorised according to means of delivery:

Vehicle bombs

The vehicle bomb is one of the most effective weapons in the terrorist's arsenal because of the potentially large quantities of explosive that can be directed towards the target with reasonable precision. The explosive device is typically prepared in advance and concealed within a vehicle.

Vehicle-borne threats may arise in various ways:

- Parked – where the vehicle is positioned close to, or underneath, the target.
- Encroachment – where the vehicle negotiates through any incomplete or wrongly spaced existing security barriers or tailgates a legitimate vehicle through an active barrier system into the premises.
- Penetrative – where the vehicle is impacted into its target.
- Deception – where the perpetrators deceive their way onto a site by using a prepared cover story, false documentation or 'trojan vehicle'.
- Duress – where a guard controlling a vehicle check point is forced to let a vehicle through or the driver of a legitimate vehicle is forced to carry an IED.

Several tonnes of explosive can be contained in larger vehicles which have been used to cause casualties and structural damage over a range of many hundreds of metres.

Person-borne/delivered

A person-borne device is usually concealed upon the person or carried in a rucksack, carrier bag or briefcase. To remain portable it will also usually weigh less than 15 kg (a quantity still sufficient to cause serious structural damage).

These devices have been used in suicide missions but have also been designed to be left unattended, possibly concealed behind furniture or screens, and timed to detonate without warning. In either case, the impact has often been increased by packing the device with nails, nuts, bolts and similar items that act as shrapnel which can have a devastating effect in a small space.

An incendiary device – which ignites rather than explodes – is usually a smaller item which, because it does not require an explosive, is simpler to make. They are usually intended to cause damage and disruption, by causing a fire or triggering the sprinkler system, for example, rather than casualties.

Postal devices

Letters, parcels or packages containing an explosive, incendiary or chemical device have been constructed in a variety of shapes and sizes. These are designed to look fairly innocuous but there are certain signs to suggest when extra caution should be shown during handling:

- The package is from an unexpected or unfamiliar sender.
- It is poorly spelt, inaccurately addressed or written in an unusual style and with more than the appropriate value of stamps for its size and weight.
- It is a padded envelope or bulky item that is unusually heavy for its size (most letters weigh up to about 30g, whereas letter bombs weigh 50g–100g).
- There is a pin-sized hole in the envelope or packaging.

Though any suspect item should be treated seriously, the majority of instances will be false alarms and so procedures for handling suspicious items should avoid exacerbating any disruption.

For more advice see BSI PAS 97 Mail Screening and Security, developed by CPNI in collaboration with BSI British Standards.

What businesses can do

How businesses defend against attack depends on individual circumstances. For most organisations the response will involve a mix of good housekeeping alongside appropriate investments in CCTV, intruder alarms and lighting that can deter as well as detect. In fact, many recommended counter-terrorism measures will help to protect against other criminal acts such as theft and vandalism and can also help companies address health and safety concerns for their employees.

Certain situations, however, may require more specialist equipment (mail scanning technology, for example) and organisations should seek professional advice for an assessment of their requirements and options before taking any major decisions (see Find out more... box on page 18 and References on pages 45-46).

External environment

If an attack by a vehicle bomb is a concern, the priority should be to ensure all unauthorised and/or unscreened vehicles are kept at a safe distance, ideally keeping cars at least 30 metres from the buildings and larger vans and lorries at least 90 metres away.

Access routes, car parks and surrounding open areas should be assessed for their traversability by a hostile vehicle. Suitable traffic calming measures such as bends and chicanes and successfully tested vehicle security barriers should be installed to create and enforce the appropriate blast stand-off distances. These vehicle security barriers can include active (moving) measures, such as retractable bollards, rising arm barriers and swing or sliding gates, and passive (static) measures such as structural walls, bollards and planters.

If vehicles are allowed within the security cordon then they should be screened at a checkpoint designed so that unauthorised vehicles can be rejected without letting them in to the cordon.

Reinforcing property

Doors and windows

External doors should be strong, properly lit and fitted with good quality locks. Any doors that are infrequently used should be internally secured (ensuring compliance with relevant fire safety regulations). Accessible windows should also be secured with good quality locks.

If there is not already one in place, a good quality alarm system should be fitted to external windows and doors. General anti-crime advice from the police will provide guidance about further improvements.

The quality of any glazing protection is important because up to 95% of all injuries from a bomb are caused by flying or falling glass. Anti-shatter film (ASF) is a relatively cheap and quick improvement whilst laminated glass should be used if windows are to be replaced or for new builds as it offers a higher level of protection. Specialist advice on glazing is available from www.cpni.gov.uk.

Protected spaces (Bomb Shelter Areas)

In certain situations it may be safer to move staff to a designated internal 'protected space' rather than evacuating a building. The protected space should be constructed from appropriately tested materials and, generally, not situated on the ground and first floors and also away from exterior walls. As it may be necessary to accommodate groups of people for uncertain periods of time these spaces should also be able to provide seating, drinking water, emergency power and external communications (procedures should not rely on mobile phones) as well as access to toilet facilities.

Note: Open-plan accommodation may lack the internal walls that could protect against blast or corridors that can provide evacuation routes and so measures such as blast-resistant glazing and clearly marked, regularly rehearsed exit routes are important.

Specialist advice about glazing and structural reinforcements should be sought in advance from www.cpni.gov.uk or from professionally qualified security engineers – a list of consultants is available from the Institution of Civil Engineers – www.ice.org.uk/rses.

Internal areas

Good housekeeping

Good housekeeping can help reduce opportunities for suspect items to be left on premises and make it easier for them to be noticed by staff (and help reduce the number of false alarms). Staff should be asked to:

- Keep external, public and communal areas – (exits, entrances, reception areas, stairs and corridors, washrooms etc) – clear and tidy.
- Lock unoccupied offices, rooms and store cupboards.
- Minimise furniture and plants in the entrances and public areas to reduce places in which to hide devices.
- Consider removing litter bins during periods of heightened threat – use clear plastic bags as a temporary alternative.

CCTV, alarms and lighting

Intrusion alarms can be a deterrent as well as a means of protection. If a police response to any alarm is required, the 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 the local police headquarters.

CCTV should be monitored regularly to help clarify whether a security alert is real. It is often vital in post-incident investigations, but only if the images are of sufficient quality to identify what happened and can be used in court. CCTV should also be planned in conjunction with the level of lighting that can be provided.

Reception areas

An efficient reception area is essential for monitoring access into and out of the premises. Where possible, entrances and exits should be fitted with a quality access control system that uses magnetic swipe or contact 'proximity' cards, supported by PIN verification. Visitors should be escorted by members of staff and also wear clearly marked temporary 'Visitor' passes that are returned when leaving.

Screening searches

Random screening of hand baggage can act as a deterrent and regular screening should be considered at times of increased threat. Organisations have the right to refuse entry to anyone who does not allow their possessions to be searched; however, body searches may only be carried out with the agreement of the individual.

Routine searching and patrolling of premises also represents a visible deterrent. Keep the patrols regular but not too predictable.

Mail facilities

Incoming mail and deliveries should be processed in one location, ideally in an off-site location or in an area that can easily be isolated. Deliveries should be handled without being brought through other parts of the building. Make sure that all staff who handle mail (including reception staff) are briefed and trained. Encourage regular correspondents to put their return address on each item.

If there is a concern about receiving mail or parcels – particularly if routine business means receiving large quantities each day – seek advice from local police CTSA.

See also BSI PAS 97 Mail Screening and Security available from the BSI British Standards.

Find out more...

For further advice on physical security:

www.cpni.gov.uk

www.nactso.gov.uk

www.scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology

www.ice.org.uk/rses (Institution of Civil Engineers)

www.bsigroup.com (*for BSI PAS 97 Mail Screening and Security)*

INFORMATION SECURITY

How information is used, stored and distributed is a major responsibility for all organisations.

What to protect against

As businesses rely more and more on their IT systems to improve efficiencies and provide greater functionality, so the information they retain becomes more vulnerable to both targeted and random attacks.

According to a 2008 survey by the UK government 35% of businesses suffered a malicious attempt to breach their IT security during the previous 12 months. And the larger the organisation the more likely it was to experience an attack with 85% of businesses of 500+ staff reporting that they had been attacked (2008 Information Security Breaches Survey, Department for Business, Innovation and Skills).

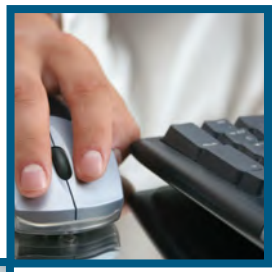
Whether stored as paper records or in electronic systems, the security of an organisation's information must be fundamental to any security and contingency planning. The key questions to be constantly asked are:

- Who would want access to our information and how could they acquire it?
- How could they benefit from its use?
- Can they sell it, amend it or even prevent staff or customers from accessing it?
- How damaging would the loss of data be? What would be the effect on its operations or reputation?

Complicating the task for many organisations is the fact that certain functions such as data processing, systems administration or server hosting are now routinely outsourced and sub-contracted, meaning that the security and integrity of their own information becomes dependent on the standards upheld by other organisations.

Human factor

Whilst investments in software and access controls will help reduce certain threats, there is a significant human factor involved. Many incidents of data loss or misuse stem from a mis-judgment or moment of carelessness by a member of staff.



Whether coerced into introducing malware (malicious software) into the network, or connecting unauthorised movable media such as USB sticks to systems, or ignoring procedures about taking confidential papers off-site, the biggest challenge can be ensuring staff are aware how vulnerabilities occur and how staff attitudes and habits make a difference.

Typical methods of electronic attack

Malicious software (Malware)

Malicious software (known as malware) refers to any file or program that is harmful to a computer such as viruses, worms, trojan horses and spyware (a program that gathers a user's information without permission). Typically spread by email or compromised websites, an infected computer has the potential to allow the attacker to collect passwords, scan drives, upload and download data or spread disruption across the entire network.

Malware sent as an email attachment directly to a recipient will appear to originate from a legitimate sender. The subject of the email and its attachment will aim to attract the recipient's interest and upon opening the malware is introduced.

Other routes into the network include portable storage devices and media such as CD-ROMs which the unsuspecting victim may insert straight into their machine – a particular issue for organisations with large numbers of staff working remotely and dialling into the network.

Hacking

Hacking refers to any attempt to gain unauthorised access into a computer system. There are a number of possible motivations ranging from disruptive or criminal intent to individuals showing off technical prowess. Hackers may have technical expertise, but the availability of hacking 'tools' has made it a less specialist activity.

Though usually the work of individuals, sophisticated co-ordinated attacks have been targeted at governments and high-profile businesses.

Phishing

Phishing attacks use a mix of technical deceit and social engineering to tempt victims into performing a series of actions that will allow access to confidential or sensitive information.

In most cases the attacker impersonates a trusted source, such as a bank or IT supplier, in the form of an official looking email, website or pop-up advert to draw attention to an urgent matter for which the recipient is pressed to provide details in response.

Phishing attacks have become more sophisticated and, as with email malware, protecting against them is as much about an individual's awareness as any central network security.

Denial of Service (DoS)

These are attempts 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.

What businesses can do

- Acquire all IT systems from reputable manufacturers and suppliers.
- All internet connected computers should be equipped with anti-virus and anti-spyware software and protected by a firewall. New computer viruses are released daily with suppliers continually fixing vulnerabilities in their software so check frequently for patches and updates. To ensure this software is regularly updated visit www.getsafeonline.org.
- Back-up information – preferably keep a secure copy in another location and make sure that all back-up and recovery procedures are regularly tested.
- Ensure that any contractors/third parties adhere to the same security policies and standards employed by the business.
- If outsourced service providers are used, contractual arrangements should be in place to safeguard data.
- Consider encryption packages for material taken off-site. Where possible, lock down or disable disk drives, USB ports and wireless connections.
- Ensure there are appropriate standards in place for disposing of digital media. Any digital media should be overwritten several times to make it unreadable and when it reaches the end of its life destroyed so that it cannot be readily reconstructed.
- Adhere to the principle that all staff and/or external contacts begin with the minimum level of access. Only extend access rights following specific management requests – make sure that those same rights are rescinded should the role or individual change.
- Impose data protection retention and deletion policies. There are legal requirements for the protection of the information a company retains and it is the responsibility of the business to ensure that it meets its obligations.
- Keep any information links with other companies under constant review. As relationships with businesses or clients change it may be necessary to cancel privileges such as extranet access or remove them from confidential mailing lists.

Educate staff

- Encourage security awareness amongst staff (see Security culture pages 37-43). Make sure they understand issues surrounding Malware and Phishing attacks or revealing information which can be used to gain access to a system.
- Provide guidance about safe use of email at work. Request that their work email account is used predominantly for work related correspondence and private email accounts are not used to contact clients or forward/receive confidential information.
- Restrict access to certain websites that are clearly non-work related; this includes any social networking and webmail sites where the security standards are not guaranteed.

Paper-based information

Many private or sensitive records will still be stored in hard copy and so it is important to ensure facilities and procedures are in place to securely store and dispose of them.

Responsible handling of documents

Sensitive, confidential or commercial documents should be appropriately marked with clear instructions issued to staff about handling when outside of the workplace. Staff should be fully aware of their responsibilities when in possession of such documents, for example never working on them in public, never leaving them in a parked vehicle and making use of any safe or safety box facility when staying in a hotel.

Clear desk and work areas

Staff should be encouraged to maintain 'Clear desk' policies by locking away all papers and portable media when away from their work areas or leaving at the end of the working day. This should include any papers left on printers, photocopiers or in meeting rooms. Valuable or sensitive documents, in particular, should not be left lying around or on display at any time.

An appropriate supply of secure cabinets or locked storage areas should therefore be provided.

Information disposal

Some of the material that businesses routinely throw away can be of use to a variety of groups including business competitors, identity thieves, criminals and terrorists. Staff names and addresses, telephone numbers, product information, technical specifications etc can all retain a value to the right people.

Paper documents may need to be destroyed by secure means. Staff should be provided with an easy method for shredding, incinerating or pulping so that valuable documents are not just disposed in general rubbish.

Find out more...

For further advice on information security:

www.cpni.gov.uk/Docs/Defending-against-electronic-attacks.pdf

www.getsafeonline.org

www.businesslink.gov.uk

www.ico.gov.uk (data protection advice)

PERSONNEL SECURITY

Personnel security measures help organisations to reduce opportunities for staff to misuse their legitimate access.

What to protect against

The placement or recruitment of an 'insider' – someone who exploits, or has the intention to exploit, their legitimate access to an organisation for unauthorised purposes – has been used by terrorist and criminal networks, as well as activists, journalists and competitors.

There are also examples of existing employees who have willingly volunteered to assist third parties or engage in insider activity for their personal gain.

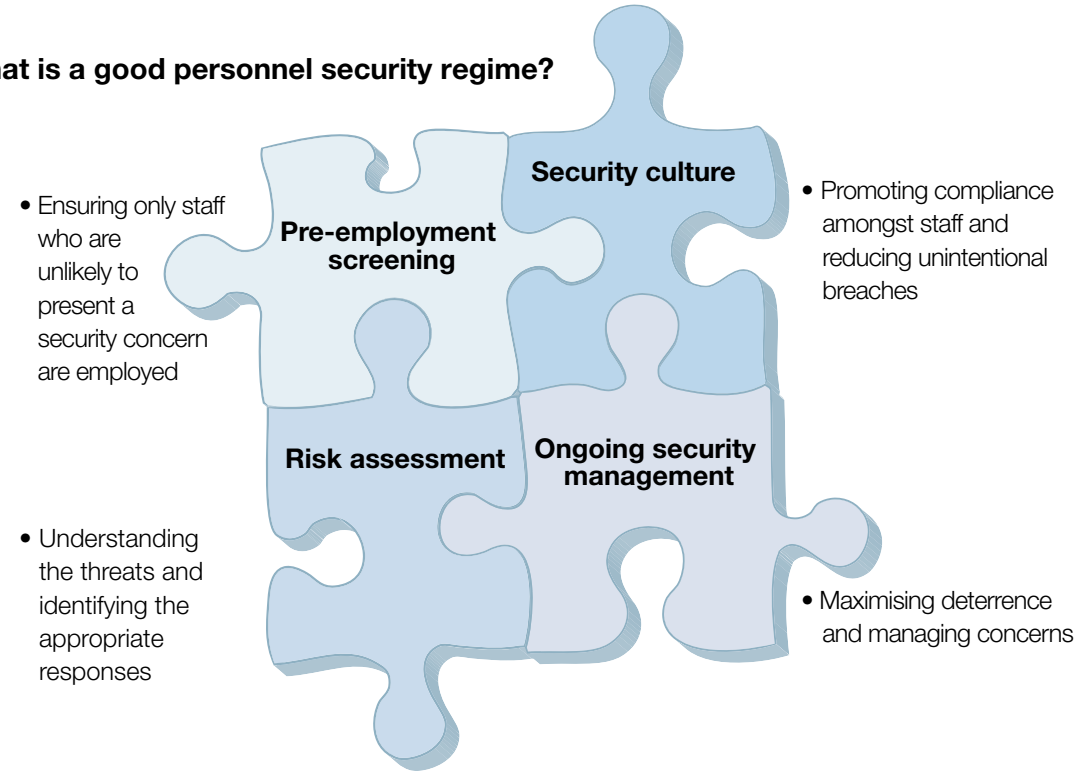
Closing down opportunities for those seeking to abuse their legitimate access is a complex challenge. Whilst there is no exact method for identifying staff who could represent a security concern, overcompensating with excessive measures can waste resources, disrupt routines and leave employees feeling distrusted and cynical.

What businesses can do

From the pre-employment process through to the final exit interview, organisations must demonstrate a consistent, transparent and indiscriminate approach to personnel security that extends to all members of staff whether permanent or contractor, whether senior management or part-time assistant.

An efficient personnel security regime should be viewed as a continuous cycle of identifying risks, evaluating procedures and raising awareness amongst all staff.

What is a good personnel security regime?



Risk assessment

Risk assessment is critical to the formation of a good personnel security regime, helping managers to focus resources on the areas of greatest concern, ensure that current measures are proportionate to the threats and provide a business case for adopting new measures where required.

When conducting a risk assessment there are a range of methods that organisations can apply (see pages 11-12) and, depending on the nature and size of the business, there may be value in conducting such assessments at various levels as appropriate, for example:

- An **organisation** assessment identifies the broad range of insider threats that an organisation faces and prioritises in terms of their likelihood and impact.
- The **group level** assessment identifies those groups of employees with the potential to carry out the highest impact threats and establishes whether the current countermeasures are sufficient and where additional measures are required.
- The **individual level** assessment examines the risk posed by individual employees of concern or small high-risk groups of employees, based upon a combination of their role, level of access and the existing environmental vulnerabilities.

Recruitment

Following the selection process, all prospective employees should be asked to provide proof of their identity, right to work and evidence of previous employment and education. A decision to request further checks should be based on the individual role and responsibilities.

All staff	Identity – name, address, date of birth Nationality and immigration status Right to Work *For example a combination of: Full current ten year UK passport or photocard driving licence; original, recent utility bills confirming service at current address; full birth certificate; proof of right to work in the UK.*
Good practice	Employment and education history *Official qualifications or licences plus full details of previous employers' name, address and dates of employment over the past three years.*
Dependent on role	Criminal record check Financial check Overseas check

Organisations should not accept duplicate or photocopied documents and obvious gaps and inconsistencies in the applicant's employment or residential history should be checked. Applicants should be reminded that supplying false information or failing to disclose relevant information could be grounds for dismissal and amount to a criminal offence.

On occasions when a candidate needs to be appointed quickly, it should be clear that the satisfactory completion of checks is a condition of employment.

When recruiting from agencies or contractors make sure that they can validate the identity of their staff and provide an authenticated photo in advance.

Develop good security practice in the workplace

Encourage staff to adopt 'security first' habits for both in and outside of the workplace:

- Where access passes are issued they should be routinely worn by staff when on the premises and removed when leaving. Staff should also feel encouraged to question anyone on site who is not wearing a pass and report any concerns.
- Maintain a 'clear desk' policy where all documents, files, keys and any other removable objects of value are locked away whenever rooms are left unattended. Provide secure disposal facilities (such as shredders) so that sensitive or commercial papers can be destroyed rather than left for collection and ensure printers and photocopiers are routinely cleared of papers.
- Reserve access to sensitive areas – e.g. server rooms – only to those who genuinely need it, with managers responsible for both issuing and removing access rights.
- Establish clear rules for occasions when staff may take commercially sensitive material out of the office. For the most valuable items it may be appropriate to require prior agreement from management with their removal and return formally recorded.
- Consider a confidential hotline/email account where employees can report concerns in confidence – offer both internal and external phone numbers for those working remotely.
- Request that all visitors register at reception and are escorted at all times. Passes issued to visitors should only offer the most basic access rights and must be returned on exit. Depending on the nature of the organisation it may be appropriate for visitors to leave mobile phones and similar devices at reception.

For further advice about promoting good practice measures during employment see *Ongoing Personnel Security* from www.cpni.gov.uk.

Staff departures

Employees leaving an organisation take considerable knowledge about internal operations, assets and security vulnerabilities with them – possibly to a competitor – and circumstances surrounding departures are not always amicable. A formal procedure for all departures will ensure all the necessary actions are taken without disrupting the employer-employee relationship.

An exit interview can provide an informal environment to remind an employee of their continuing obligations and recover to recover all keys, passes and passwords without individuals feeling singled out.

Find out more...

For further advice on personnel security:

www.cpni.gov.uk

Ongoing personnel security: a good practice guide
Risk assessment for personnel security
Pre-employment screening guidance
Document verification guidance

BUSINESS CONTINUITY PLAN

A plan for maintaining operations and returning to 'business as usual' following a terrorist attack or major disruption.

The Business Continuity Plan (BCP) is an essential part of any organisation's response planning. It sets out how the business will continue to operate following an incident and how it expects to return to 'business as usual' in the quickest possible time afterwards.
A BCP need not be specific to terrorist incidents and should apply to any major disruption such as a major fire, flooding or power fault.

Preparing a BCP requires important decisions about those assets within the organisation that, whatever the circumstances, it cannot afford to lose and the timescales within which operations must resume.

The plan itself sets out the agreed arrangements for bringing events under control, the necessary resources for maintaining critical business functions and the staff required for co-ordinating actions.

A wide range of advice for developing and maintaining BCPs is available (see the Find out more... box opposite), but the following is a summary of common principles:

Understanding the business

The first step is to identify the assets and processes that are critical to the business:

- Which roles and individuals are vital for fulfilling business commitments?
- What equipment, IT, transport etc will staff need to maintain operations?
- Which departments are vital for fulfilling orders and contractual obligations?
- Which suppliers and other third parties are integral to daily routines?

Some of the assets will have been identified during any recent risk assessment exercise (see pages 9-12).

For each asset identified there are three key questions to consider:

1 What would be the cumulative impact on the organisation if this asset was disrupted for certain periods of time such as the initial 24 hours, 48 hours, five days and so on?

2 How quickly must it be restored?

3 What alternative resources are available?

Continuity preparations

This process will highlight actions that could be taken now to improve resilience, for example:

- Cross-training of skills amongst the workforce.
- Documenting procedures so that delegated staff can perform unfamiliar tasks.
- Agreed relocation options both within and outside the premises (e.g. meeting rooms that could be quickly converted to work areas).
- Remote access to IT systems in nominated back-up locations or staff homes.
- Alternative sources of production equipment.
- Secure/off-site storage of data back-ups and valuable documentation.
- Agreed methods for out-of-hours contact for staff, suppliers, clients etc.

The plan

The BCP should then present all the steps that staff are expected to follow in the aftermath of an incident in order to maintain essential operations and return to 'business as usual' as soon as possible.

The structure and detail of the BCP will vary from business to business and from location to location but, in general, should include:

- The circumstances for instigating an incident room and who should report to it.
- Response and communications plans for handling the initial recovery.
- Clear roles and delegated responsibilities.
- Factors determining part or full evacuation of premises.
- How first-aid will be provided and the arrangements for marshalling crowds.
- Support for people with disabilities, restricted mobility or other needs.
- When and how alternative accommodation and facilities will be utilised.
- Contingency arrangements for critical transactions and operations – client orders, receipt of deliveries, production etc.
- Agreed procedures for re-commencing routine operations.

Advice regarding some of details listed above, such as internal and external communications, the setting up of an incident room and evacuation of the premises, is set out in the following pages.

Not all staff will be in a position to receive new instructions whilst in the midst of an incident. In certain situations, some staff may be tasked with responsibilities they have not previously performed by colleagues who would not usually carry the necessary authority. The BCP therefore needs to be an inclusive and accessible resource aimed at all parties, including those from outside the organisation. It must be clearly presented, avoiding vague internal references and abbreviations, and structured in such a way that people can quickly find and understand what is expected from them.

Rehearsals

The BCP should be constantly updated in response to changes within the organisation. Organising regular drills and exercises will help familiarise staff with procedures and refine details within the plan. For example, the agreed response to a bomb alert may differ from that of a fire alarm – the muster point may well be much further away to avoid any surrounding damaged buildings – and so staff need to understand the differences and why. See Security Culture on pages 37-44 for further advice on raising awareness amongst staff.

Find out more...

For further advice on business continuity plans:

The booklet *Expecting the Unexpected*, jointly published by NaCTSO, London First and the Business Continuity Institute outlines a process to follow when developing a BCP. A copy is available from www.cpni.gov.uk and from www.nactso.gov.uk.

Information about the Business Continuity Management Standard (BS25999), including a toolkit for implementing a continuity plan is available from www.direct.gov.uk.

The Government's Preparing for Emergencies pages on www.direct.gov.uk also provides extensive information and links to relevant organisations and resources.

Further advice about business continuity can be found at www.cabinetoffice.gov.uk/ukresilience.aspx and also via the Business Continuity Institute www.bci.org.uk.

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 so consult their websites for details.

INCIDENT RESPONSE

Advance preparations could make a big difference to an organisation's response to an incident.

In the midst of a major incident there may be little time to think about what actions need to be taken. These can be stressful and tense moments, possibly exacerbated by the lack of information about what has happened and if further disruption is anticipated. Media coverage may still be trying to establish the scale of the incident whilst the emergency services may be following their own rehearsed procedures until further details become available.

Where the business continuity plan sets out the actions, decisions and contingency arrangements for recovering operations, the response plan helps to shape the initial handling until the facts become available: how the incident will be managed, by whom and from where, and how resources and information will be made available to those who will manage the situation.

Contingency staff

Arrangements in the Business Continuity Plan may require certain staff to take charge of the initial response, assisted by nominated members of staff with relevant knowledge of production, stakeholder relations and IT support.

However, there must be some flexibility – attendance during an incident may be affected by access, particularly if the incident occurs out-of-hours, and some staff may be nominated simply because they live close enough to provide support.

Incident room

In larger organisations it may be possible to provide an area in which an incident room can be quickly set up (or, if space affords, permanently maintained). This is an accessible and secure room where nominated staff will meet to gather information, monitor developments and co-ordinate instructions in the immediate aftermath of an incident. A secondary back-up location, ideally off-site, might also be identified in case the preferred room is inaccessible.

The incident room may be required to operate on a 24hr basis and will need to be readily equipped with appropriate furniture, IT, communications, stationery, TV and radio and, if possible, accommodation. Any pre-prepared Response pack (see opposite) should also be available to staff within the incident room.

Incident log

Amongst the tasks to perform in the incident room will be the requirement to keep a running diary, recording important times and actions as they happen. Not only will this help shift handovers to track general progress, it can also help inform any post-event analysis.

The assumption should be to instigate the incident room for most major circumstances – the assembled team can stand down if necessary.

Working with the emergency services

All co-ordination with the emergency services should go though previously nominated individuals with appropriate authority within the organisation.

The emergency services may require details of the search plan (see pages 35-36) in addition to any other available building plans and details about any known casualties or areas of the site that may have become hazardous.

It should also be accepted practice that whilst on-site the instructions of the emergency services are followed over any organisational arrangements.

Response pack

A Response pack should include key documents and items that may be needed by those who will manage the incident room or work with the emergency services. Example contents are set out below, however these lists are not exhaustive and other items should be added as required.

Documents:

- Business Continuity Plan and Communications Plans
- Contact details for nominated response staff, plus list of all employees, their home and mobile numbers
- Emergency services contact details
- Details of any local utility companies, emergency glaziers, salvage organisations, building contractors, local authority contingency planners
- Building plans, including the location of gas, electricity and water shut off points and heating and ventilation controls. Also, any protected areas where staff will be sheltered.
- A recent stock and equipment inventory
- Financial and banking information
- Product lists and specifications

Equipment:

- Stand-alone laptop computer, compatible with the local network
- USB memory sticks or flash drives
- Spare keys/security codes
- Torch and spare batteries
- Hazard and cordon tape
- Small cash resource
- Card and marker pens for temporary signs and other stationery (pens, paper, etc)
- Mobile telephone with charger and appropriate credit

Find out more...

For further advice on response planning:

www.ukresilience.info

www.thebci.org

COMMUNICATIONS PLAN

Communications are essential in the midst of an incident.

It is important not to put all efforts into maintaining external relations at the expense of staff communications, and vice-versa. In order for messages to be accurate – and to avoid confusion or the spread of misinformation – specific tasks should be allocated to relevant, experienced staff.

Staff communications

In the event of a serious incident there will be the need to inform staff as soon as possible about what they are expected to do. This should be managed through tested internal communications channels such as the public address system, email alerts, intranet or any notice boards/signposts in communal areas.

Keep all messages clear and succinct. If there are any directions for staff to follow it is important not to require too many actions at once. People are more likely to respond to one or two instructions than a whole list.

A quick response might be vital (particularly if staff are monitoring media reports) so consider setting up pre-prepared templates for staff announcements. These can provide an agreed structure, tone of voice, directions and methods of distribution with just the necessary details to be added – this should help avoid delays from re-drafts or approvals from senior staff.

Maintaining contact

Make full use of internal communications to keep employees informed about any ongoing investigation as well as known disruption to local roads and public transport.

In the event of a full or part-evacuation there will, at some stage, be the need to give the 'all-clear' or update those congregated in protected areas (see page 17) or evacuation muster points, so it is essential to have adequate communications to these points. This may be managed by a public address system (which may need standby power), hand-held radio or other standalone systems, however organisations should not rely solely on mobile phones.

Out of hours cascade

If not already included in the contingency plans, consider arranging an agreed model for an out of-hour message cascade amongst staff. The cascade involves each team manager being responsible for contacting their direct reports before reporting back to confirm all staff (or as many as possible) have been reached. Staff should be familiarised with how the cascade will work and provided with regular updates of their colleagues' contact details.

External communications

Stakeholders

The Business Continuity Plan and Response Plans identify the lead contact for the emergency services but there may be reason to contact other external stakeholders to offer updates or simply provide reassurance, for example:

- Central office and/or other locations within the business
- Local Authority Emergency Planning Office
- Neighbouring businesses
- Utility companies
- Insurance company
- Customers and suppliers
- Major shareholders

In each case the communications plan should make it clear who is responsible for maintaining contact. In some instances it will be those co-ordinating the incident room but in others it may be more appropriate for staff members with relevant working relationships, knowledge or authority. Keep the contact details in the emergency pack.

Family and friends

If the organisation itself has been directly involved in, or situated close to, a major incident it is understandable that there will be concerned relatives and friends looking for information. In large incidents a hotline may be set up in conjunction with the emergency services and any public website should be updated with details of these numbers.

It might be appropriate to provide a script to those who manage general phone enquiries.

Media management

Depending on the seriousness of the incident it may be necessary to engage with the local or even national media who may be pressing for urgent information and reaction.

If certain staff within the organisation are familiar with media handling then all such enquires should continue to be directed to them to avoid the risk of inaccurate details being reported. It may be difficult to prevent staff or onlookers from making comments or using mobile devices to circulate images but, as far as the organisation's own formal response is concerned, information needs to be as accurate and appropriate as the situation allows.

A range of approved press statements for circulation will help co-ordinate messages with relevant external parties. If necessary a formal statement containing succinct, factual information should be issued to clarify as much as possible what has happened, what is being done about it and when any further information will be available.

BOMB THREATS

Procedures for handling bomb threats.

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

Calls may be of two kinds:

1 Hoax threats designed to disrupt, test reactions or divert attention

2 Threats warning of a genuine device – These may be attempts to avoid casualties or enable the terrorist to blame others if there are casualties. However genuine threats can provide inaccurate information about where and when a device might explode.

Base bomb threat procedures on the following principles:

Ensure that all staff who could conceivably receive a bomb threat are trained in handling procedures or have ready access to instructions. This applies particularly to courts, banks, hotels, hospitals, news agencies, public transport organisations and those offering any sort of emergency service. Switchboard operators should be familiarised with procedures.

Draw up a clear list of actions to follow upon receipt of a call. Even though staff may be unable to assess a threat's accuracy or origin, their impressions of the caller could be important. A suggested bomb threat checklist is available on www.cpni.gov.uk.

Consider that the member of staff who receives the threat may not be prepared – receiving such a threat may be the closest that many people ever come to acts of terrorism – so offer some basic advice for staff on handling a threat, for example:

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 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 report the incident to the relevant manager or security team to decide on the best course of action and 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 your impressions of the caller and 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.

EVACUATION PLAN

When to evacuate the premises and where staff should safely congregate.

An evacuation of the premises may be required because of:

- A threat aimed directly at the premises
- A threat or incident elsewhere that has been passed on by the police
- Discovery of a suspicious item in or in the vicinity of the building.

Depending on the size and location of the business, the plans for evacuating premises should confirm both the circumstances and arrangements for conducting either a full evacuation, a partial evacuation or evacuation to an internal safe area such as a protected space (page 17).

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 the building, or through an area thought to be contaminated, evacuation might not be the best course of action and internal protected spaces might have to be considered.

An important consideration when planning an evacuation route is to ensure people are kept away from other areas where a second device could detonate – arrangements should include a quick search of the muster point to ensure it is free from any further devices.

The general principle is if the device is within the building then consider evacuation, if the device is outside the building it may be safer to remain inside. Whatever the circumstances, tell the police what action you are taking as soon as possible.

In the case of a suspected **letter** or **parcel** bomb, evacuate the room, the floor concerned and the two floors immediately above and below.

The final decision to evacuate will be for the organisation, however the police should be able to advise. In exceptional cases the police may insist on evacuating the property.

Evacuation

Evacuation instructions should be clearly communicated with routes and exits well defined. Open-plan accommodation may lack internal walls that could protect against blast and fragments or corridors that offer evacuation routes, so measures such as blast resistant glazing and clearly defined, regularly rehearsed exit routes are important. Appoint individuals to act as marshals and as contacts once the muster point is reached.

Special arrangements may be needed for any disabled staff, pregnant women and visitors.

Muster points should be at least 500 metres away from the building. It is generally advised that two muster points are identified – in opposing directions – which are likely to be further away from the building than any designated fire alarm muster point. In the case of most vehicle bombs, for instance, this distance should put staff safely beyond the police cordons – although it would be advisable to have an alternative about 1 km away. Avoid using car parks as muster points.

Any evacuation plan should be agreed with the emergency services, the local authority and neighbours and ensure that any staff with specific responsibilities are sufficiently trained and plans are regularly rehearsed.

SEARCH PLANNING

Regular searches of premises should be part of a daily routine.

Regular searches are an important part of everyday good housekeeping. A full search, for example, might be included as part of the close-of-business routine each day. In particular, searches should be regularly performed when there is a heightened response level or security alert in the area.

Preparing a Search Plan

The search plan will depend upon the circumstances of each separate location, but the objective is always to ensure that the entire area is searched thoroughly on a regular basis. In addition to the main public and operational areas, the plan should ensure that surrounding grounds and car parks are included as well as stairwells, fire escapes, corridors, toilets and lifts etc.

To keep searches manageable, larger organisations might consider dividing their premises into separate sectors and provide searchers with written checklists – signed upon completion – to ensure no area is left unchecked.

Searches during and following evacuation

In the event of premises being evacuated, searches of the arranged muster points, the routes towards them and the surrounding areas should be made in advance to ensure there are no secondary devices.

A full search of the premises should also be conducted prior to re-occupation by staff. This is a responsibility that lies with the business and not the emergency services. The police will take responsibility for searches of any adjacent public areas.

Conducting the search

- Appoint a Search Co-ordinator to oversee the operation and liaise with nominated searchers.
- Initiate the search by issuing a message over a public address system (perhaps coded to avoid unnecessary disruption and alarm), by text message, via personal radio or by telephone cascade.
- Divide the priority locations into areas of a manageable size for one or two searchers. Ideally, staff should search in pairs to ensure nothing is missed.
- Ensure that those conducting searches are familiar with the areas and what they would normally expect to find there. They do not need to be experts in explosives or other devices but able to recognise anything that should not be there, is out of place or not yet accounted for.
- Develop appropriate techniques for staff to be able to routinely search public areas without alarming any visitors or customers present.
- During the searches place particular focus on: areas that are open to the public; any enclosed areas such as cloakrooms, stairs, corridors and lifts; any evacuation routes and muster points; car parks and other external areas such as goods or loading bays.
- Under no circumstances should a suspicious item found during a search be touched or moved in any way. The police should be informed immediately and they will ensure an appropriate response.

Check the Search Plan with local police and/or CTSA and practise it regularly.

SECURITY CULTURE

How an organisation engages and communicates with staff reflects its commitment to security.

In addition to the various protective measures that can be put in place, the level of security awareness amongst staff – their vigilance and everyday routines, for example – is an essential 'layer' of an organisation's response.

Staff training, response exercises and internal communications all play a part, but so does the way in which a business 'backs up' its words through its actions. For example, if staff are asked to keep paperwork securely locked away but are not provided with sufficient storage (or broken locks are never repaired) staff may question the management's commitment to security policies.

A 'security culture' is therefore about encouraging all members of staff to respect common values and approaches towards security both inside and outside of the workplace.

Staff communications

Clear, succinct, jargon-free guidance about security standards and procedures should be freely provided. Where detailed procedural documents are necessary they should be accompanied by at-a-glance summaries covering essential points such as the actions to be followed in the event of an incident or security breach.

Security messages should be kept visible to both staff and visitors by making use of available internal communications such as posters, leaflets, newsletters, staff magazines, message boards and desk furniture.

Management support

Senior management support is vital in order to demonstrate the value the organisation places on security. If the Chief Executive is seen not wearing their pass it sends a message to others that management do not take this policy seriously.

Ultimately, it is senior management who are likely to be held responsible for the impacts of any security breaches and so they should have a vested interest in the quality of their organisation's overall security culture.

Line management relations

Staff with direct management responsibilities are in a position to not only influence attitudes amongst colleagues but also to identify and address any behaviours of concern amongst their staff.

Through their regular contact – even to staff in different locations – it should be a part of their duties to ensure their teams are acting appropriately and ensuring that data handling standards are maintained etc. It might even be added as part of each line-manager's job description.

Employee welfare

There are circumstances (for example, a relationship breakdown or financial difficulty) which may impair an individual's judgement or performance. If staff feel compelled to conceal their concerns, it may encourage some to become disaffected with their employer or susceptible to manipulation.

Where possible, organisations should offer an environment in which employees can discuss issues in confidence and find out about where and when support can be provided (e.g. cases of illegal drug abuse or personal debt).

Security hotline

In larger organisations a hotline or email account can be offered where staff can report, anonymously or otherwise, any suspicions or actual incidents of illegal, unethical or improper conduct by their colleagues, such as bullying, failure to adhere to security procedures, fraud or theft.

It should be noted that providing a reporting hotline does raise a number of legal issues that need to be resolved. Organisations should seek legal advice first.

Find out more...

For further advice on security culture:

See Ongoing Personnel Security available from www.cpni.gov.uk

STAFF AWARENESS

Security reviews should be informed by regular rehearsals and consultations with staff.

Educating staff about security will not only help them to recognise vulnerabilities – and their possible consequences – but also help organisations identify new threats through the feedback they receive from staff.

Rehearse procedures

Oversights or weaknesses in any plans will often only be discovered when put to the test. Rehearsals, drills and exercises (see box below) will not only provide evidence of whether measures and response plans are working, but also ensure staff are familiar with any procedures and tasks that they are expected to perform.

It is generally recommended that most aspects of the security plan are tested at least annually in every location. Greater frequency may be required depending on the nature of the business (such as level of staff turnover etc.)

Put arrangements to the test

Equipment test: Ensure that equipment – particularly items key to the response plan (see page 28) – is frequently tested. This should include any alarms, public address systems, radio communications, emergency lifts etc as well as provisions for reserve power supplies, IT support and any incident response room.

Telephone cascade: Test any agreed model for out-of-hours contact (see page 31) to certify that it operates as planned. Staff moves and changes of address mean such details can quickly date.

Desk top contingency exercise: Invite staff to work through scenarios involving a breach of security within the organisation and the ensuing sequence of events. The 'incidents' should be based upon realistic situations with staff working in groups to understand how their actions and decisions will affect events. Such experiences, even over just a couple of hours, can lift staff out of their routines and into thinking 'what if'.

Full test: Conduct a full-scale evacuation to the designated external and internal muster points to ensure staff are familiar with their routes. This could also be extended into a full exercise in which events are played out in real time, such as the arrival of emergency services, media questioning etc.

Staff training

All employees must take responsibility for their adherence to the organisation's security policies, but it is down to the employer to ensure that they are appropriately trained.

Security training for all staff – whether permanent, temporary or a contractor – should begin during any induction process, followed by regular 'refresher' training and briefings. Ongoing task-specific training should then be provided according to the specifics of each role. In some circumstances it may also be appropriate to incorporate an element of assessment.

Training techniques might include formal presentations, workshops or scenario based role-plays etc but could also include less formal formats such as road shows, intranet content, films or desk-top packages.

Appraisals

Incorporating individual security standards into any performance appraisal process is another way of ensuring that regular personnel security checks are conducted on all staff.

Employees in more sensitive positions could be asked to complete an annual security appraisal form to determine any changes in their personal and financial circumstances which may pose a risk to the organisation's security. An example form is available in *Ongoing Personnel Security*, available from www.cpni.gov.uk.

Staff survey

Periodically gauging staff opinion about security habits can help determine whether measures and procedures are both appropriate and understood (See pages 41-42). Demonstrate that this is a transparent process by sharing the results – both positive and negative – with staff along with any resulting actions.

STAFF SURVEYS

Understanding current and changing attitudes to security.

Staff surveys about security standards within the organisation are a useful method of determining current attitudes and monitoring trends. This could be fulfilled during any existing annual survey conducted by the business or through a specially-organised exercise for specific groups.

To encourage honest feedback it may be beneficial to allow a measure of anonymity where possible.

Examples of possible questions* and format are set out below:

Informed	**Strongly agree**	**Agree**	**Undecided**	**Disagree**	**Strongly disagree**
All staff are conscientious about security					
Everyone is regularly informed about security issues through internal communications or team meetings etc.					
Enough training/induction time is allocated to security issues					
I am clear about what is expected if there is an incident					
I can find out about security changes easily					

Consistency	**Strongly agree**	**Agree**	**Undecided**	**Disagree**	**Strongly disagree**
The same standards are applied to suppliers, contractors, partners, temporary staff					
Access to buildings systems is effectively controlled					
Everything is monitored so it's hard to breach security rules					
If there is a security concern I know who to contact/get assistance					
Staff are encouraged to report concerns					
My manager/supervisor listens to my concerns					

Proportionate	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
Security procedures prevent me from doing my job					
It is often necessary to share security access (to sites, passwords, data)					
Enforcement of security measures is minimal					
Staff who raise issues are seen as trouble makers					
The organisation only learns from the lessons of previous incidents					
Our measures are not aimed at the right threats to our business					

Management support	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
Different rules seem to apply to management regarding security					
Lack of management interest means employees often ignore security procedures					
Managers have no way of finding out if security procedures are followed or not					
Management would support me if I stopped a task due to security concerns					
People who delay work for the sake of security are seen as awkward by colleagues					
Managers are slow to react to non-compliance					

** Questions taken from a wider range of questions featured in CPNI Security Culture Review and Evaluation Tool (SeCuRe) provided to national infrastructure organisations.*

SECURITY IN THE WORKPLACE

Good practice security habits for all employees.

1 Network and computer use

- Always lock the screen (Ctrl + Alt + Del) when leaving a computer terminal unattended and log-off completely when leaving for the day.
- Never insert a disk, USB or other portable device into the computer unless sure of its origin.
- When deciding on a password always use 'strong' passwords that contain a mix of letters, symbols and characters and choose a different password for each system. Never reveal the password to others, even to close colleagues or managers.

2 Email/downloads

- Do not open or respond to an email from an unrecognised source or download attachments and/or files without knowing what they are and where they are from – this is the most common way that computers pick up a virus. Equally, take care when attempting to download content directly from an unknown internet site.

3 Work areas

- Keep desks and work areas clear and tidy. Lock all documents and loose items away at the close of the working day. Ensure printers and photocopiers are always clear of any papers.
- All confidential/commercial documents should be appropriately marked and kept in a secure, lockable storage facility. Sensitive papers in particular should be securely disposed of – such as through a shredding machine – rather than left for collection.

4 Visitors

- All visitors should be provided with a temporary visitor badge with limited access rights. This badge should also be returned as they leave. All visitors should be escorted at all times when on the premises.

5 Personal details

- Never give out any personal or confidential details to anyone over the phone unless sure about the person requesting them and that they are entitled to them. Do not submit any details into an unfamiliar website or unsolicited email/internet pop-ups.
- Take care with the amount of information and photographs shared on any online social networking sites – for example, details of periods of time away from home – and avoid discussing work related issues.

6 Outside the workplace

- Avoid taking sensitive or valuable information away from work unless it is essential and secured via encrypted laptops or USB devices.
- When away from the premises and/or in public areas, keep all sensitive information secure to prevent loss or theft. For example, never leave such items locked in a car overnight.

7 Data handling

- Take care when dealing with private and personal data – ensure it is handled in accordance with the organisation's own rules and the requirements of the Data Protection Act. When issuing data to others be sure to understand what it will be used for and send only the data required.

8 Keep us informed

- Report any concerns or where others appear to be acting suspiciously and feel welcome to suggest any improvements that can be made to improve standards of security in the workplace.

USEFUL CONTACTS

Anti-terrorist Hotline
Tel: 0800 789 321

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

BSI British Standards
Tel: 020 8996 9001
www.bsigroup.com

The Business Continuity Institute
Tel: 0118 947 8215
www.thebci.org

Business Link – Practical advice for business
www.businesslink.gov.uk

Cabinet Office
Tel: 020 7276 1234
www.cabinetoffice.gov.uk

CESG – The National Technical Authority for Information Assurance
Tel: 01242 709141
www.cesg.gov.uk

Crime reduction
Tel: 020 7035 4848
www.crimereduction.homeoffice.gov.uk

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

Department for Business, Innovation and Skills
Tel: 020 7215 5000
www.bis.gov.uk

Directgov – Website of the UK Government
www.direct.gov.uk

European Network and Information Security Agency
Tel: +30 28 10 39 1280
www.enisa.europa.eu

Foreign travel
www.fco.gov.uk/en/travel-and-living-abroad/staying-safe/terrorism

Get Safe Online – Free, expert advice on how to be safe online
www.getsafeonline.org

Health and Safety Executive
Tel: 0845 345 0055
www.hse.gov.uk

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

Information Commissioner's Office
www.ico.gov.uk

Information Security and Assurance (ISA)
www.cabinetoffice.gov.uk/ogcio/isa.aspx

The Institute of Risk Management
Tel: 020 7709 9808
www.theirm.org

London Prepared
Tel: 020 7217 3036
www.londonprepared.gov.uk

Loss Prevention Certification Board
Tel: 01923 664100
www.brecertification.co.uk
www.redbooklive.com

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

NaCTSO – National Counter Terrorism Security Office
www.nactso.gov.uk

Neighbourhood Policing
www.neighbourhoodpolicing.co.uk

Overseas Security Information for Business (OSIB)
Tel: 0207 215 8000
www.uktradeinvest.gov.uk/ukti/osib

The Police Service of Northern Ireland
Tel: 0845 600 8000
www.psni.police.uk

Preparing for emergencies
www.direct.gov.uk/preparingforemergencies/

Securing Your Business – Self Assessment
www.homeoffice.gov.uk/secureyourbusiness

Security Industry Authority (SIA)
Tel: 0844 892 1025
www.the-sia.org.uk

Serious Organised Crime Agency (SOCA)
Tel: 0370 496 7622
www.soca.gov.uk

UK Police Service
www.police.homeoffice.gov.uk

UK Resilience
Tel: 020 7276 1234
www.cabinetoffice.gov.uk/ukresilience.aspx

OTHER USEFUL RESOURCES

Expecting the Unexpected

This guide is the result of a partnership between the 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.

Available from www.cpni.gov.uk and www.nactso.gov.uk

Secure in the Knowledge

This guide is aimed mainly at small and medium-sized businesses to help improve basic security. Ideally it should be read in conjunction with Expecting the Unexpected (see 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.

Available from www.cpni.gov.uk and www.nactso.gov.uk

The United Kingdom's Strategy for Countering International Terrorism (CONTEST)

The national strategy to reduce the risk to the United Kingdom and its interests overseas from international terrorism.

Available from www.security.homeoffice.gov.uk

REGISTER OF SECURITY ENGINEERS AND SPECIALISTS

CPNI sponsors the Register of Security Engineers & Specialists (RSES) which was developed to promote excellence in the field of security engineering and provide a ready means for individuals to demonstrate competence in this discipline through independent assessment.

The Register is managed and organised by the Institution of Civil Engineers (ICE) and provides a professional competence standard for potential clients and insurers through its code of ethics, demanding peer review and strict continuing professional development requirements. Further details about the RSES are available on the ICE website www.ice.org.uk/rses.

CPNI

Centre for the Protection of National Infrastructure

www.cpni.gov.uk