Counter Terrorism Protective Security Advice

for Higher and Further Education

ACPOS
ASSOCIATION OF CHIEF POLICE OFFICERS IN SCOTLAND

produced by

NaCTSO
National Counter Terrorism Security Office

NaCTSO

National Counter Terrorism Security Office

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

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

NaCTSO aims to:

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

foreword

This guidance has been developed to assist the higher and further education sectors in addressing the security issues relating to terrorist attacks. It is the product of discussions and sharing of best practice involving the National Counter Terrorism Security Office together with representatives from UK universities and colleges.

We want our Higher and Further institutions to be places where all students and staff are safe and secure and able to foster a culture of shared values and open debate to cohere the rightly celebrated diversity of the sector. But there is a real and serious threat of terrorist attacks in the UK and terrorism can come in many forms, not just a physical attack on life and limb. It can include interference with vital information or communication systems, causing disruption and economic damage.

The law requires institutions to carry out adequate risk assessments and ensure that suitable measures are in place to manage identified risks. Institutions should conduct prompt and regular reviews of those assessments and measures in light of new threats and developments at the institution and the surrounding area.

Equally important is that business continuity plans address security issues to ensure that institutions can cope with an incident or attack and return to 'business as usual' as soon as possible.

Having a robust security culture and being better prepared reassures your whole community that you are taking security issues seriously.

Heads of institutions should bring this guidance to the attention of all relevant staff. These are likely to include Security, Estates, Facilities, Health & Safety and HR Managers.

Although each institution will have its own particular circumstances, the guidance addresses all of the areas of concern for educational establishments and includes a number of useful Good Practice checklists.

John Denham
Secretary of State for Innovation, Universities & Skills

Admiral the Lord West of Spithead
GCB, BSc, DUniv

Department for
Innovation, Universities & Skills

contents

1. Introduction 5
2. Managing the Risks 9
3. Security Planning 13
4. Physical Security 15
5. Good Housekeeping 19
6. Access Control 21
7. CCTV Guidance 23
8. Small Deliveries by Courier and Mail Handling 25
9. Search Planning 29
10. Evacuation Planning 31
11. Personnel Security 35
12. Information Security 41
13. Vehicle Borne Improvised Explosive Devices (VBIEDs) 45
14. Chemical, Biological and Radiological (CBR) Attacks 47
15. Suicide Attacks 49
16. Firearm and Weapon Attacks 50
17. Hostile Reconnaissance 51
18. High Profile Events 55
19. Threat Levels 57
20. Communication and Training 59

APPENDIX 'A' Business Continuity Planning Checklist 61
APPENDIX 'B' Housekeeping Good Practice Checklist 62
APPENDIX 'C' Access Control Good Practice Checklist 63
APPENDIX 'D' CCTV Good Practice Checklist 64
APPENDIX 'E' Searching Good Practice Checklist 65
APPENDIX 'F' Evacuation/Invacuation Good Practice Checklist 66
APPENDIX 'G' Personnel Security Good Practice Checklist 67
APPENDIX 'H' Information Security Good Practice Checklist 68
APPENDIX 'I' Communication Good Practice Checklist 68
APPENDIX 'J' High Profile Event Good Practice Checklist 69
Grab Bag Checklist 70
Bomb Threat Checklist 72
Useful Publications 74
Useful Contacts 75

one introduction

This guide is intended to give protective security advice to those who are responsible for the security of higher and further education institutions, irrespective of size and location. It highlights the part institutions can play in the UK counter terrorism strategy, and how by mitigating the risk you can allow teaching, learning, research, knowledge transfer, community engagement and enterprise to continue as normal.

Terrorist attacks in the UK are a real and serious danger. The terrorist incidents in the Haymarket, London and at Glasgow Airport in June 2007 indicate that terrorists continue to target crowded places; largely because they are usually locations with limited protective security measures and therefore afford the potential for mass fatalities and casualties. Furthermore, these two particular incidents identify that terrorists are prepared to use vehicles as a method of delivery and will attack sites well away from London.

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

It is possible that institutions could be the target of a terrorist incident. This might include having to deal with a bomb threat or with suspect items left in or around the establishment.

In the worst case scenario staff and students could be killed or injured, and the premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Of course there is a need to make education institutions as accessible as possible and to ensure there is a welcoming environment. This guide is accordingly not intended to create a 'fortress mentality'. There is however a balance to be achieved where those accountable for security are assured that there are robust protective security measures available to mitigate against the threat of terrorism.

Law, Liability and Insurance

There are legal and commercial reasons why institutions' security plans should deter such acts, or at least to minimise their impact. They are:

Criminal prosecution and heavy penalties under health and safety laws for bodies and individuals who manage or are responsible for institutions are a real possibility in the wake of a terrorist incident, particularly if it emerges that core standards and statutory duties have not been met. Particularly relevant to protective security are the specific requirements of the Health and Safety at Work Act 1974 and Regulations made under it to do all of the following:

- Carry out adequate **risk assessments** and put suitable measures in place to manage identified risks, even where they are not of the institution's making and are outside their direct control: then be alert to the need to conduct prompt and regular reviews of those assessments and measures in light of new threats and developments

- **Co-operate and co-ordinate** safety arrangements between owners, managers, security staff, tenants and others involved on site, including the sharing of incident plans and working together in testing, auditing and improving planning and response
- **Ensure adequate training, information and equipment** are provided to all staff, and especially to those involved directly on the safety and security side
- Put proper procedures and competent staff in place to deal with **imminent and serious danger** and evacuation.

The need to focus on proper preparation and prevention to guard against criminal prosecution for safety and security lapses has sharpened with the coming into force in April 2008 of the Corporate Manslaughter and Corporate Homicide Act 2007, and will take on an even greater prominence when the current Health and Safety Offences Bill is passed into law. That Bill will give the courts power to send individual directors, managers and others to jail for up to 2 years for a breach of health and safety duties: at present the heaviest penalty that can be imposed is in almost all cases a monetary fine.

Insurance against the full cost of damage to your own commercial buildings from terrorist acts is becoming harder to find in some sectors at an affordable premium. Adequate cover for loss of revenue and business interruption during a rebuild or decontamination is expensive even where available from the limited pool of specialist underwriters. Full protection against compensation claims for death and injury to staff and customers caused by terrorism is achievable, albeit at a cost.

With individual awards for death and serious injury commonly exceeding the publicly-funded criminal injuries compensation scheme upper limit, there is every incentive for victims to seek to make up any shortfall through direct legal action against owners, operators, managers and tenants under occupiers liability laws. Having to pay large and numerous compensation claims out of your own uninsured pocket could have a high impact on your institution.

If your institution is not already involved, you should consider the Pool Re insurance scheme (www.poolre.co.uk). The Pool Re scheme has been set up by the insurance industry in co-operation with the UK government so that insurers can continue to cover losses resulting from damage caused by acts of terrorism to commercial property in Great Britain.

Emergency and business continuity planning

A business continuity strategy is essential in ensuring that institutions can simultaneously respond to an incident and return to **'business as usual'** as soon as possible. You should also develop an emergency response plan, which can be implemented to cover a wide range of possible situations.

The British Standards Institution (BSi) has produced a Business Continuity Management standard - BS25999 which provides further guidance on the subject of business continuity plans.

Emergencies - Planning for and Managing: A good practice guide for Higher Education Institutions - The Association of University Chief Security Officers (AUCSO) (available to download at www.ukresilience.go.uk)

See good practice checklist - Business Continuity in Appendix 'A'.

This guide recognises that institutions differ in many ways including size, location, layout and operation and that some of the advice included in this document may already have been introduced at some locations. This guide and the good practice checklists included as appendices constitute a 'health check' for institutions and are no replacement for specialised advice.

For specific advice relating to your particular institution, contact the nationwide network of specialist police advisers known as Counter Terrorism Security Advisers (CTSAs) through your local police force. They are coordinated by the National Counter Terrorism Security Office (NaCTSO).

It is essential that all the work you undertake on protective security is undertaken in partnership with the police, other authorities such as the land owners and trustee's as appropriate as well as your neighbours, if your premises are to be secure.

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

two managing the risks

Managing the risk of terrorism is only one part of an institution's responsibility when preparing plans in response to any incident which might prejudice personal safety or disrupt normal operations.

With regard to protective security, the best way to manage the risks to your institution is to start by understanding and identifying the threats to it, and its vulnerability to those threats.

This will help you to decide:

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

For some aspects of institutional security, simple good practice - coupled with vigilance and well exercised plans - may be all that is needed.

If, however, you identify areas of vulnerability, you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable.

The following diagram illustrates a typical risk management cycle:

Step One: Identify the threats.

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

- What can be learnt from the government and media about the current security climate, or about recent terrorist activities? (Visit www.cpni.gov.uk or refer to the Useful Contacts section at the back of this booklet)
- Is there anything about the location of your establishment, its visitors, sponsors, contractors, occupiers, students and staff, or your activities that would particularly attract a terrorist attack?

- Is there an association with high profile individuals or organisations which might be terrorist targets?
- Do you have procedures in place and available for deployment on occasions when VIPs attend your institution?
- Could collateral damage occur from an attack on, or other incident to a high risk neighbour?
- What can your local Police Service tell you about crime and other problems in the area of the institution?
- Is there any aspect of your courses, research, events or activities that terrorists might wish to exploit to aid their work, e.g. plans, technical expertise or unauthorised access?
- Do you communicate information about the threat and response levels to your staff?

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

Your priorities for protection should fall under the following categories:

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

You know what is important to your institution. You should already have plans in place for dealing with fire and crime, procedures for assessing the integrity of those you employ or contract, protection from IT viruses and hackers, and measures to secure the estate.

Consider what others could find out about your vulnerabilities, such as:

- Information about you that is publicly available, e.g. on the internet or in public documents.
- Anything that identifies installations or services vital to the continuation of your business.
- Any prestige targets that may be attractive to terrorists, regardless of whether their loss would result in business collapse.

You should have measures in place to limit access into service areas and vehicle access control measures into goods and service area.

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

It is important that your staff can identify and know how to report suspicious activity. (See hostile reconnaissance on page 51).

Step Three: Identify measures to reduce risk

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

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

If you need additional security measures, then make them most cost-effective by careful planning wherever possible. If you are using an area or premises normally used for another purpose, work with the occupiers to produce an integrated security package. Even if organisations / businesses surrounding your institution are not concerned about terrorist attacks, they will be concerned about general crime - and your security measures will help protect against crime as well as terrorism.

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

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

You should regularly exercise and revise your plans to ensure that they remain accurate, workable and current.

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

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

Further information on exercise planning can be found through the following link: http://www.ukresilience.gov.uk/preparedness/exercises/plannersguide.aspx

IT SHOULD BE REMEMBERED THAT ONE OF THE GREATEST THREATS TO ANY INSTITUTION IS COMPLACENCY.

three security planning

For many higher education (HE) and further education (FE) institutions the responsibility for the implementation of protective security measures following a threat and risk assessment will fall on a dedicated member of the security or estates management team. This person must have sufficient authority to direct the action taken in response to a security threat.

The security plan is part of a wider security strategy also comprising but not mutually exclusive to business continuity, intelligence/reconnaissance and emergency management.

He or she must be involved in the planning perimeter security, access control, contingency plans etc, so that the terrorist dimension is taken into account. The Security Manager must similarly be consulted over any temporary construction so that counter terrorism specifications, e.g. concerning glazing and physical barriers can be factored in, taking into account any planning and safety regulations.

The Security or Facilities Manager should already have responsibility for most if not all of the following key areas:

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

For independent and impartial counter terrorism advice and guidance that is site specific, the Security Manager should establish contact with the local police Counter Terrorism Security Adviser (CTSA). Most UK Police Forces have at least two CTSAs.

Your CTSA can:

- Help you assess the threat, both generally and specifically
- Give advice on physical security equipment and its particular application to the methods used by terrorists; The CTSA will be able to comment on its effectiveness as a deterrent, as protection and as an aid to post-incident investigation
- Facilitate contact with emergency services and local authority planners to develop appropriate response and contingency plans
- Identify appropriate trade bodies for the supply and installation of security equipment
- Offer advice on search plans

Creating your Security Plan

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

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

When creating your security plan, consider the following:

- Details of all the protective security measures to be implemented, covering physical, information and personnel securit
- Instructions on briefing content to security staff including type of behaviour to look for and methods of reporting
- Instructions on how to respond to a threat (e.g. telephone bomb threat)
- Instructions on how to respond to the discovery of a suspicious item or event
- A search plan
- Evacuation plans and details on securing the institution in the event of a full evacuation
- Your business continuity plan
- A communications and media strategy which includes handling enquiries from concerned family and friends. [See Chapter 19]

Security Managers should also be familiar with the following advice:

- The Fire Safety Risk Assessment - 'Small and Medium Places of Assembly' and 'Large Places of Assembly' guidance documents (available to download at www.communities.gov.uk).
- Emergencies - Planning for and Managing: A good practice guide for Higher Education Institutions - The Association of University Chief Security Officers (AUCSO) (available to download at www.ukresilience.go.uk)
- The Academic Technology Approval Scheme (information available at www.fco.gov.uk)

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

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

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

four physical security

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

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

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

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

Successful security measures require:

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

Action you should consider

Contact your Counter Terrorism Security Adviser (CTSA) through your local police force at the start of the process. As well as advising you on physical security, they can direct you to professional bodies that regulate and oversee reputable suppliers.

When considering a new building project, consult your local police force Architectural Liaison Officer (ALO), who will provide normal physical security advice. Your CTSA, however, will provide specific counter terrorism advice in conjunction with your ALO if such advice is required.

Remember, you will need to ensure that all necessary regulations are met, such as Local Authority permissions, health and safety and fire prevention requirements.

Plan carefully - as this can help keep costs down. Whilst it is important not to delay the introduction of necessary equipment or procedures, costs may be reduced if the premises or location you are using already has the necessary security which can be easily integrated within your own plan.

Security awareness

The vigilance of all staff and contractors is essential to your protective measures. They will know their own work areas very well and should be encouraged to be alert to unusual behaviour or items out of place.

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

Training is therefore particularly important. Staff should be briefed to look out for packages, bags or other items in odd places, carefully placed (rather than dropped) items in rubbish bins and unusual interest shown by strangers in less accessible places. See hostile reconnaissance on page 51. Training in emergency response plans should also be included in staff inductions.

Access control

Keep access points to a minimum and make sure the boundary between public and private areas is secure and clearly signed. Ensure there are appropriately trained and briefed security personnel to manage access control points or alternatively invest in good quality access control systems, especially in restricted access areas. See High Profile Events on page 55.

Security passes

If an access control system is in place, insist that staff and students wear their passes at all times and that the issuing is strictly controlled and regularly reviewed. Passes should include a photograph of the bearer. Visitors to private or restricted areas should be escorted and should wear clearly marked temporary passes, which must be returned on leaving. Anyone not displaying security passes in private or restricted areas should either be challenged or reported immediately to security or management.

Screening and Patrolling

The screening of hand baggage is a significant deterrent that may be a suitable protective security consideration for key events.

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

Traffic and parking controls

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

For site specific advice and guidance you should contact your CTSA or local Police Security Coordinator.

See also Vehicle Borne Improvised Explosive Devices on page 45.

Doors and windows

Good quality doors and windows on permanent structures are essential to ensure building security, advice on the appropriate standards can be obtained from your local police force.

If using a temporary building structure a survey of the existing doors, windows and build materials could be made to identify any gaps in mitigating your own security vulnerabilities. External doors should be strong, well lit and fitted with good quality locks where possible.

Doors that are not often used should be internally secured ensuring compliance with relevant fire safety regulations and their security monitored with an alarm system. **This is particularly important where an external search / screening operation is present in order to prevent unauthorised entry and bypassing any search regime.**

As a minimum accessible windows should be secured with good quality key operated locks. The police may provide further advice on improving the security of glazed doors and accessible windows.

- Many casualties in urban terrorist attacks are caused by flying glass, especially in modern buildings and glazing protection is an important casualty reduction measure.
- Extensive research has been carried out on the effects of blast on glass. There are technologies that minimise shattering and casualties, as well as the costs of re-occupation.
- Anti-shatter film, which holds fragmented pieces of glass together, offers a relatively cheap and rapid improvement to existing glazing. If you are installing new windows, consider laminated glass, but before undertaking any improvements seek specialist advice through your police CTSA or visit www.cpni.gov.uk for further details

Perimeter

The style and quality of perimeter security will depend on the risks and vulnerabilities identified in your security assessment. If any searching of persons or vehicles has taken place then a robust perimeter must be maintained in order to have full confidence in the security regime applied.

Temporary fencing will require supporting processes such as patrol, CCTV coverage and alarms to ensure reduction in risk. Equally, any temporary fencing must adhere to health & safety legislation and fire regulations, remembering safety must always have priority over security.

Integrated security systems

Intruder alarms, CCTV and lighting are commonly used to deter crime, detect offenders and delay their actions. All these systems must be integrated so that they work together in an effective and coordinated manner.

Intrusion detection technology can play an important role in an integrated security system; it is as much a deterrent as a means of protection. If police response to any alarm is required, your system must be compliant with the Association of Chief Police Officers' (ACPO) security systems policy (www.acpo.police.uk) in Scotland. For further information, contact the Alarms Administration Office at your local police headquarters.

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

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

Remember that CCTV is only effective if it is properly monitored, maintained and can provide an active response.

See CCTV guidance on page 23.

five good housekeeping

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

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

- Avoid the use of litter bins around critical/vulnerable areas i.e. do not place litter bins next to or near glazing, support structures, most sensitive or critical areas (but if you do, ensure that there is additional and prompt cleaning in these areas).
- Alternatively review the management of all your litter bins and consider the size of their openings, their blast mitigation capabilities and location.
- The use of clear bags for waste disposal is a further alternative as it provides an easier opportunity for staff to conduct an initial examination for suspicious items.
- Review the use and security of compactors, wheelie bins and metal bins to store rubbish within service areas, goods entrances and near areas where crowds congregate.
- Keep public and communal areas - exits, entrances, queues, lavatories - clean and tidy, as well as service corridors and areas.
- Keep the fixtures and fittings in such areas to a minimum - ensuring that there is little opportunity to hide devices.
- Temporary information stands, concessionaires and kiosks should be searched before and after use and secured or moved when unattended.
- Staff rooms and corridors should be kept tidy, and staff rooms should have access control.
- Lock unoccupied offices, rooms and store cupboards.
- Ensure that everything has a place and that things are returned to that place.
- Place tamper proof plastic seals on maintenance hatches.
- Keep external areas as clean and tidy as possible.
- All sites should have in place an agreed procedure for the management of contractors, their vehicles and waste collection services. The vehicle registration mark (VRM) of each vehicle and its occupants, should be known to the security or management in advance.
- If allowed, pruning vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any packages.

Additionally consider the following points:

Staff are trained in bomb threat handling procedures or at least have ready access to instructions - and know where these are kept. (See bomb threat checklist)

If you have CCTV, review your system to ensure it has sufficient coverage both internally and externally.

Fire extinguishers should be appropriately marked and authorised for the locations in which they will be kept. Regular checks should be made to ensure that they have not been interfered with or replaced.

Security management should identify a secondary secure location for a control room (if they have one) as part of their normal contingency plans.

All safety and security systems should have an uninterrupted power supply (UPS) available which is regularly tested if it is identified that power loss would impact on the safety of the public.

See good practice checklist - housekeeping in Appendix 'B'.

six access control

Any lack of vigilance around pedestrian and vehicle entrances to your institution and queues forming outside your buildings affords anonymity to a potential terrorist. Security staff should be a visible presence and should be briefed on what to look for and how to deal with it.

There should be clear demarcation between public and private areas, with appropriate access control measures into and out of the private areas. This relates to private areas within the institution, not public entrances.

Risk assessment

Refer to 'managing the risks' on page 9 and decide the level of security you require before planning your access control system. Take into account any special features you may require.

Appearance

The access control system to your private or restricted areas and service yards is often the first impression of security made upon persons visiting your premises.

Ease of access

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

Ideally, adopt a photo ID card access control system which varies in appearance for the different levels of access across the site. Security staff should be instructed what to examine when checking passes and this should be quality assured through testing.

Training

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

System maintenance

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

Interaction

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

Compliance

Your access control system should be compliant with:

- The Disability Discrimination Act 1995
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Fire Safety Order 2005
- Health and Safety Acts
- The Fire (Scotland) Act 2005

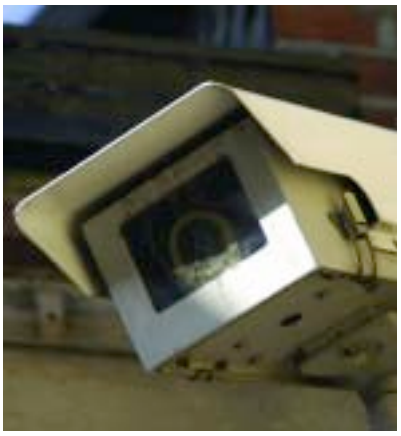
Access control is only one important element of your overall security system.

REMEMBER

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

See Good Practice Checklist - Access Control to Institutions Appendix 'C'

seven cctv guidance



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

If you have access to a CCTV system you should constantly monitor the images captured or regularly check recordings for suspicious activity ensuring at all times full compliance with the Data Protection Act 1998 which should be specified in your CCTV Data Protection Policy.

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

If you **contract** in CCTV operators they must be licensed by the Security Industry Authority if the CCTV equipment is deployed into fixed positions or has a pan, tilt and zoom capability and where operators:

- Cover all the entrances and exits to your premises and other areas that are critical to the safe management and security of your operation.
- Proactively monitor the activities of members of the public whether they are in public areas or on private property.
- Use cameras to focus on the activities of particular people either by controlling or directing cameras to an individual's activities.
- Use cameras to look out for particular individuals.
- Use recorded CCTV images to identify individuals or to investigate their activities.
- Wherever possible, ensure that all CCTV systems are integrated centrally through a single CCTV policy for your institution.

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

SIA licensing applies in Scotland from 1 November 2007. Further guidance can be found at www.the-sia.org.uk/home/scotland.

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

Ask yourself the following questions:

- Is your CCTV system currently achieving what you require it to do? Do you need it to confirm alarms, detect intruders through doors or corridors and produce images of evidential quality?
- Are the CCTV cameras in use for the protective security of your institution integrated with those used to monitor student or visitor movement?

- Would the introduction of an Automatic Number Plate Reader (ANPR) system complement your security operation?

The Home Office Scientific Development Branch (HOSDB) has published many useful documents relating to CCTV, including 'CCTV Operational Requirements Manual' (Ref: 55/06), 'UK Police Requirements for Digital CCTV Systems' (Ref: 09/05), and 'Performance Testing of CCTV Systems' (Ref: 14/95).

Consider also the following points:

- Ensure the date and time stamps of the system are accurate.
- Regularly check the quality of recordings.
- Digital CCTV images should be stored in accordance with the evidential needs of the Police. Refer to HOSBD publication 09/05.
- Ensure that appropriate lighting complements the system during daytime and darkness hours.
- For analogue systems change tapes daily - use no more than 12 times.
- Keep your recordings for at least 31 days.
- Use good quality video tape and check it regularly by playing it back on a different machine.
- Ensure the images recorded are clear - that people and vehicles are clearly identifiable.
- Check that the images captured are of the right area.
- Implement standard operating procedures, codes of practice, audit trails and signage.
- Give consideration to the number of camera images a single CCTV operator can effectively monitor at any one time.
- Do you have sufficient qualified staff to continue to monitor your CCTV system during an incident, evacuation or search?

See Good Practice Checklist - CCTV in Appendix 'D'

Please remember, a monitored CCTV system is only as effective as the response capability.

CCTV Maintenance

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

What occurs if a system is not maintained?

- The system gets **DIRTY** causing poor usability
- **CONSUMABLES** wear causing poor performance
- Major parts **FAIL**
- **WEATHER** damage can cause incorrect coverage
- **DELIBERATE** damage/environmental changes can go undetected

eight small deliveries by courier and mail handling

Institutions often receive a wide variety of deliveries. This offers an attractive route into premises for terrorists.

You should consider the need for a screening process at their mail handling site, whether at a temporary or permanent structure and consider the following:

Delivered Items

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

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

Delivered items come in a variety of shapes and sizes; a well made one will look innocuous but there may be telltale signs.

Indicators to Suspicious Deliveries/Mail

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

If a suspicious item is identified, follow these key steps:

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

Chemical, biological or radiological materials in the post

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

- Unexpected granular, crystalline or finely powdered material (of any colour and usually with the consistency of coffee, sugar or baking powder), loose or in a container.
- Unexpected sticky substances, sprays or vapours.
- Unexpected pieces of metal or plastic, such as discs, rods, small sheets or spheres.
- Strange smells, e.g. garlic, fish, fruit, mothballs, pepper. If you detect a smell, do not go on sniffing it. However, some CBR materials are odourless and tasteless.
- Stains or dampness on the packaging.
- Sudden onset of illness or irritation of skin, eyes or nose.

CBR devices containing finely ground powder or liquid may be hazardous without being opened.

What you can do:

- The precise nature of the incident (chemical, biological or radiological) may not be readily apparent. Keep your response plans general and wait for expert help from the emergency services.
- Review plans for protecting staff and visitors in the event of a terrorist threat or attack. Remember that evacuation may not be the best solution. You will need to be guided by the emergency services on the day.
- Plan for the shutdown of systems that may contribute to the movement of airborne hazards (e.g. computer equipment containing fans and air-conditioning units).
- Ensure that doors can be closed quickly if required.
- If your external windows are not permanently sealed shut, develop plans for closing them in response to a warning or incident.

- Examine the feasibility of emergency shutdown of air-handling systems and ensure that any such plans are well rehearsed.
- Where a hazard can be isolated by leaving the immediate area, do so as quickly as possible, closing doors and windows as you go.
- Move those directly affected by an incident to a safe location as close as possible to the scene of the incident, so as to minimise spread of contamination.
- Separate those directly affected by an incident from those not involved so as to minimisethe risk of inadvertent cross-contamination.
- Ask people to remain in situ - though you cannot contain them against their will.

You do not need to make any special arrangements beyond normal first aid provision. The emergency services will take responsibility for treatment of casualties.

Planning your mail handling procedures

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

- Seek advice from your local police Counter Terrorism Security Adviser (CTSA) on the threat and on defensive measures.
- Consider processing all incoming mail and deliveries at one point only. This should ideally be off-site or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the site.
- Consider identifying those who may be at a higher risk than others: academic and research staff for instance.
- Ensure that all staff who handle mail are briefed and trained. Include reception staff and encourage regular correspondents to put their return address on each item.
- Ensure that all sources of incoming mail (e.g. Royal Mail, couriers, and hand delivery) are included in your screening process.
- Ideally post rooms should have independent air conditioning and alarm systems, as well as scanners and x-ray machines. However, while mail scanners may detect devices for spreading chemical, biological, and radiological (CBR) materials (e.g. explosive devices), they will not detect the materials themselves.
- At present, there are no CBR detectors capable of identifying all hazards reliably.
- Post rooms should also have their own washing and shower facilities, including soap and detergent.
- Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual occurrences. Train them to open post with letter openers (and with minimum movement), to keep hands away from noses and mouths and always to wash their hands afterwards. Staff should not blow into envelopes or shake them. Packages suspected of containing biological, chemical or radiological material should ideally be placed in a double sealed bag.

- Consider whether staff handling post need protective equipment such as latex gloves and facemasks (seek advice from a qualified health and safety expert). Keep overalls and footwear available in case they need to remove contaminated clothing.
- Make certain post opening areas can be promptly evacuated. Rehearse evacuation procedures and routes, which should include washing facilities in which contaminated staff could be isolated and treated.
- Staff who are responsible for mail handling should be made aware of the importance of isolation in reducing contamination.
- Prepare signs for display to staff in the event of a suspected or actual attack.

nine search planning

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

As previously mentioned under Security Planning, it is recognised that for the majority of institutions responsibility for the implementation of any search planning, following a vulnerability and risk assessment, will fall upon the Security Manager.

The following advice is generic for most institutions, but recognises that they operate differently. If considered necessary, advice and guidance on searching should be available through your local Police Security Co-ordinator if appointed, CTSA or Police Search Adviser (POLSA).

Search Plans

- Search plans should be prepared in advance and staff should be trained in them.
- The conduct of searches will depend on local circumstances and local knowledge, but the overall objective is to make sure that the entire area, including grounds, are searched in a systematic and thorough manner so that no part is left unchecked.
- If you decide to evacuate in response to an incident or threat, you will also need to search it in order to ensure it is safe for re-occupancy.
- The police will not normally search premises. (See High Profile Events page 55). They are not familiar with the layout and will not be aware of what should be there and what is out of place. They cannot, therefore, search as quickly or as thoroughly as a member of staff or on site security personnel.
- The member(s) of staff nominated to carry out the search do not need to have expertise in explosives or other types of device. But they must be familiar with the place they are searching. They are looking for any items that should not be there, that cannot be accounted for and items that are out of place.
- Ideally, searchers should search in pairs; to ensure searching is systematic and thorough.

Action You Should Take

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

The sectorised search plan should have a written checklist - signed when completed - for theinformation of the Security Manager.

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

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

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

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

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

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

Searching visitors and their belongings is an element of protective security that should be considered. Some institutions routinely search visitors and their belongings, others carry out random searches.

Discuss your search plan with your CTSA.

See good practice checklist - Searching in Appendix 'E'

ten evacuation planning

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

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

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

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

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

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

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

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

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

Evacuation

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

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

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

For suggested 'Grab Bag' contents please refer to check list on page 70.

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

Disabled persons should be individually briefed on their evacuation procedures, and liaise with the institution to develop their own Personal Emergency Evacuation Plans (PEEPS).

In the case of suspected:

Letter or parcel bombs

If in a premises evacuate the room and the floor concerned and the adjacent rooms along with the two floors immediately above and below if applicable. If the structures are of temporary construction then evacuate at least 500 metres from the device.

Chemical, Biological and Radiological Incidents

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

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

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

Security managers should ensure that they have a working knowledge of the heating, ventilation and air conditioning (HVAC) systems and how these may contribute to the spread of CBR materials within the structure/building.

Protected Spaces

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

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

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

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

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

Communications

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

It is essential to have adequate communications within and between protected spaces. You will at some stage wish to give the 'all clear', or tell staff to remain where they are, to move to another protected space or evacuate the building. Communications may be by public address system (in which case you will need standby power), hand-held radio or other stand alone systems. Do not rely on mobile phones. You also need to communicate with the emergency services. Whatever systems you choose should be regularly tested and available within the protected space.

Converting to open plan

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

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

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

Open air events

If you host an event predominantly in the open with only temporary demountable structures such as marquees, event kiosks or simply an open space, the protected space principle is unlikely to offer any suitable refuge and evacuation may again be your only option.

eleven personnel security

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

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

What is personnel security?

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

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

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

Understanding and assessing personnel security risks

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

Data Protection Act

The Data Protection Act (DPA) (1998) applies to the processing of personal information about individuals. Personnel security measures must be carried out in accordance with the data protection principles set out in the act.

Pre-employment Screening

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

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

Pre-employment checks

Personnel security starts with the job application, where applicants should be made aware that supplying false information, or failing to disclose relevant information, could be grounds for dismissal and could amount to a criminal offence. Applicants should also be made aware that any offers of employment are subject to the satisfactory completion of pre-employment checks. If an organisation believes there is a fraudulent application involving illegal activity, the police should be informed.

Pre-employment checks may be performed directly by an institution, or this process may be sub-contracted to a third party. In either case the organisation needs to have a clear understanding of the thresholds for denying someone employment. For instance, under what circumstances would an application be rejected on the basis of their criminal record, and why?

Pre-employment screening policy

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

Identity

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

- A paper-based approach involving the verification of key identification documents and the matching of these documents to the individual.
- An electronic approach involving searches on databases (e.g. databases of credit agreements or the electoral role) to establish the electronic footprint of the individual. The individual is then asked to answer questions about the footprint which only the actual owner of the identity could answer correctly.

Pre-employment checks can be used to confirm an applicant's identity, nationality and immigration status, and to verify their declared skills and employment history.

From February 2008, the Immigration, Asylum and Nationality Act 2006 comes into force. This means there are changes to the law and employers face new requirements to prevent illegal working in the UK. These include an ongoing responsibility to carry out checks on employees with time-limited immigration status. Failure to comply with the new regulations could result in a possible civil penalty or criminal conviction. CPNI's guidance on pre-employment screening has been updated to reflect this new law. More detailed information can be found on the UK Border Agency website. (www.ukba.homeoffice.gov.uk)

Qualifications and employment history

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

Qualifications

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

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

Employment checks

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

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

Criminal convictions

A criminal conviction - spent or unspent - is not necessarily a bar to employment (see the Rehabilitation of Offenders Act). However, there are certain posts where some forms of criminal history will be unacceptable. To obtain criminal record information, a institution can request that an applicant either:

1. completes a criminal record self-declaration form, or
2. applies for a Basic Disclosure certificate from Disclosure Scotland.

It is also appreciated education institutions carry out formal Criminal Records Bureau (CRB) checks on persons seeking employment with them using their normal policies and procedures for additional information go to www.crb.gov.uk.

Financial checks

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

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

Contractor recruitment

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

Contracts should outline the type of checks required for each post and requirements should be cascaded to any sub-contractors. Where a contractor or screening agency is performing the checks they should be audited.

Secure contracting

Contractors present particular personnel security challenges. For instance, the timescales for employing contractors are often relatively short, and there is greater potential for security arrangements to be confused or overlooked (e.g. due to further sub-contracting).

In managing the insider risks associated with contractors it is important to:

- Ensure that pre-employment checks are carried out to the same standard as for permanent employees. Where this is not possible, due to tight deadlines or a lack of information available for background checking, then the resulting risks must be managed effectively. Preferably the implementation of any additional security measures will be guided by a personnel security risk assessment.
- Where pre-employment checks - or any other personnel security measures - are carried out by the contracting agency rather than the employing organisation, a detailed account of the checks to be undertaken and the standards achieved must be incorporated into the contract that is drawn up between the two. Furthermore, the pre-employment checking process conducted by the contractor should be audited regularly.

Confirm that the individual sent by the contracting agency is the person who arrives for work (e.g. using document verification or an electronic identity checking service).

Once the contractor has started work in the organisation, they will need to be managed securely. The following steps will help:

- Carry out a risk assessment to establish the threats and level of risk associated with the contractor acting maliciously in post.
- Ensure that the contract that exists, either between the organisation and the contractor, or between the organisation and the contracting agency, defines the codes of practice and standards that apply.
- Provide photo passes to contract and agency staff, and stipulate that they must be worn at all times. Ideally, the employing organisation should retain contractors' passes between visits, reissuing them each time only after the contractor's identity has been verified.

The employing organisation and the contracting agency (or the contractor, if no agency is involved) should agree a procedure for providing temporary replacements when the contractor is unavailable. These arrangements should be included in the contract between the two parties, and the employing organisation will need to decide what additional personnel security measures to implement - for example, restricted or supervised access - when the replacement is on site.

- Where a contractor is in post but the necessary pre-employment checks have not been carried out - or where the results of the checks are not entirely positive but the need for the contractor's expertise is such that they are employed anyway - then additional personnel security measures must be considered (e.g. continuous supervision).

Overseas checks

It is increasingly necessary to screen potential employees who have lived and worked overseas. As far as possible, organisations should seek to collect the same information on overseas candidates as they would for longstanding UK residents (e.g. proof of residence, employment references, criminal record). It is important to bear in mind that other countries will have different legal and regulatory requirements covering the collection of information needed to manage personnel security and therefore this step may be difficult.

A number of options are available to organisations wishing to perform overseas checks:

1. Request documentation from the candidate.
2. Hire professional/ an external screening service.
3. Conduct your own overseas checks.

In some circumstances you may be unable to complete these overseas checks satisfactorily (e.g. due to a lack of information from another country). In this case, you may decide to deny employment, or to implement other risk management controls (e.g. additional supervision) to compensate for the lack of assurance.

See Good Practice checklist - Personnel Security in Appendix 'G'

Students

Some postgraduate overseas students will have had to apply for an Academic Technology Approval Scheme (ATAS) certificate, designed to stop the spread of knowledge and skills that could be used in the proliferation of weapons of mass destruction (WMD) and their means of delivery. This is in common with other governments around the world.

More information is available from the Foreign and Commonwealth Office
www.fco.gov.uk/en/fco-in-action/counter-terrorism/weapons/atas

The points based system for overseas staff and students came into operation in March 2009. More information is available from the Home Office www.ukba.homeoffice.gov.uk/studyingintheuk

For additional advice please refer to 'A Good Practice Guide on Pre-Employment Screening' via the CPNI website.

QUIET STUDY
AREA
LOANS
COLLECTIO

twelve information security

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

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

When considering this type of attack you should look at the facilities and processes at your institution and any other place you operate from. Many institutions may contract in security access control systems. Make sure it is clear who is responsible for management and security of data.

Before taking specific protective measures you should:

- **Assess the threat and your vulnerabilities** (See Managing the Risks on page 9).
- Consider to what extent is your information at risk, who might want it, how might they get it, how would its loss or theft damage you?
- Consider current good practice information security for countering electronic attack and for protecting documents.

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

Electronic attack

Attacks on electronic systems could:

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

Electronic attacks are much easier when computer systems are connected directly or indirectly to public networks such as the internet.

The typical methods of electronic attack are:

Malicious software

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

1. Running or executing an attachment received in an email.
2. Clicking on a website link received in a website.
3. Inappropriate web browsing which often leads to a website distributing malicious software.
4. Allowing staff to connect removable memory devices (USB memory sticks, disks, CD's, DVD's) to corporate machines.
5. Allowing your staff to connect media players and mobile phones to corporate machines.

Denial of service (DoS)

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

Hacking

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

Malicious modification of hardware

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

What to do

- Acquire your IT systems from reputable manufacturers and suppliers.
- Ensure that your software is regularly updated. Suppliers are continually fixing security vulnerabilities in their software. These fixes or patches are available from their websites - consider checking for patches and updates daily.
- Ensure that all internet-connected computers are equipped with anti-virus software and are protected by a firewall.
- Back up your information, preferably keeping a secure copy in another location.
- Assess the reliability of those who maintain, operate and guard your systems (refer to the section on Personnel Security on page 35)
- Consider encryption packages for material you want to protect, particularly if taken offsite - but seek expert advice first.
- Take basic security precautions to prevent software or other sensitive information falling into the wrong hands. Encourage security awareness among your staff, training them

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

- Make sure your staff are aware that users can be tricked into revealing information which can be used to gain access to a system, such as user names and passwords.
- Consider investing in secure cabinets, fit locking doors and ensure the proper destruction of sensitive material
- Where possible, lock down or disable disk drives, USB ports and wireless connections.
- Ensure computer access is protected by securely controlled, individual passwords or by biometrics and passwords.
- Implement an acceptable use policy for staff concerning web browsing, email, use of chat rooms, social sites, trading, games and music download websites.

Organisations can seek advice from the Government website - www.itsafe.gov.uk.

Examples of electronic attacks

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

Disposal of sensitive information

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

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

The principal means of destroying sensitive waste are:

Shredding

Industry standards for document shredding do not currently exist in the UK: but have been established in Germany for some time (DIN). Much of the EU has adopted the German standard.

Shredding machines specified to DIN 32757 - 1 level 4 will provide a shred size 15mm x 1.9mm

Suitable for medium to high security requirements.

Incineration

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

Pulping

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

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

Before investing in waste destruction equipment you should:

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

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

thirteen vehicle borne improvised explosive devices (VBIEDs)

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

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

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

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

Effects of VBIEDs

VBIEDs can be highly destructive. It is not just the effects of a direct bomb blast that can be lethal: flying debris such as glass can present a hazard many metres away from the seat of the explosion. Some institutions might have hazardous materials or harmful substances, which could increase the danger associated with such an attack.

What you can do

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

- Ensure you have effective vehicle access controls, particularly at goods entrances and service yards. Do not allow unchecked vehicles to park next to public areas where there will be large numbers of people or where there is a risk of structural collapse.
- Insist that details of contract vehicles and the identity of the driver and any passengers approaching your goods/service areas are authorised in advance.
- Consider a vehicle search regime at goods/service entrances that is flexible and can be tailored to a change in threat or response level. It may be necessary to carry out a risk assessment for the benefit of security staff who may be involved in vehicle access control.
- Establish and rehearse bomb threat and evacuation drills. Bear in mind that, depending on where the suspected VBIED is parked and the layout of your establishment, it may be safer in windowless corridors or basements than outside if this facility is available.
- **Consider using robust physical barriers to keep all but authorised vehicles at a safe distance. Seek the advice of your local Police Counter Terrorism Security Adviser (CTSA) on what these should be and on further measures such as electronic surveillance including Automatic Number Plate Recognition (ANPR) and protection from flying glass.**
- **Train and rehearse your staff in identifying suspect vehicles, and in receiving and acting upon bomb threats. Key information and telephone numbers should be prominently displayed and readily available.**

- It should be emphasised that the installation of physical barriers needs to be balanced against the requirements of safety and should not be embarked upon without full consideration of planning regulation and fire safety risk assessment.

See Good Practice Checklist - Access Control in Appendix 'C'

fourteen chemical, biological and radiological (CBR) attacks

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

Chemical

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

Biological

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

Radiological

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

A radiological dispersal device (RDD), often referred to as a 'dirty bomb', is typically a device where radioactive materials are combined with conventional explosives. Upon detonation, no nuclear explosion is produced but, depending on the type of the radioactive source, the surrounding areas become contaminated.

As well as causing a number of casualties from the initial blast, there may well be a longer term threat to health. A number of terrorist groups have expressed interest in, or attempted to use, a 'dirty bomb' as a method of attack.

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

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

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

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

What you can do

- Review the physical security of any air-handling systems, such as access to intakes and outlets.
- Improve air filters or upgrade your air-handling systems, as necessary.
- Restrict access to water tanks and other key utilities.
- Review the security of your food and drink supply chains.
- **The Home Office advises organisations against the use of CBR detection technologies as part of their contingency planning measures at present. This is because the technology is not yet proven in civil settings and, in the event of a CBR incident, the emergency services would come on scene with appropriate detectors and advise accordingly.** A basic awareness of CBR threat and hazards, combined with general protective security measures (e.g. screening visitors, CCTV monitoring and active response of perimeters and entrance areas, being alert to suspicious deliveries) should offer a good level of resilience. In the first instance, seek advice from your local police force CTSA.
- If there is a designated protected space available this may also be suitable as a CBR shelter, but seek specialist advice from your local police force CTSA before you make plans to use it in this way.
- Consider how to communicate necessary safety advice to staff and how to offer reassurance. This needs to include instructions to those who want to leave or return to the site.

Institutions should be aware that all hazardous materials and harmful substances, including seemingly innocuous low-level isotopes, could provide the opportunity for a terrorist attack. Suitable security must be maintained around all such substances.

fifteen suicide attacks

The use of suicide bombers is a very effective method of delivering an explosive device to a specific location. Suicide bombers may use a lorry, plane or other kind of vehicle as a bomb or may carry or conceal explosives on their persons. Both kinds of attack are generally perpetrated without warning. The most likely targets are mass casualty crowded places, symbolic locations and key installations.

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

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

There is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the police.

See Hostile Reconnaissance - page 51.

sixteen firearm and weapon attacks

Education institutions around the world have suffered a number of lone and group attacks. However, terrorist use of firearms and weapons is still infrequent, but it is important to consider this method of attack and be prepared to cope with such an incident. Below is some general guidance to aid your planning in this area.

Cover

- Find the best available ballistic protection.
- Remember, out of sight does not necessarily mean out of danger, especially if you are not ballistically protected.

GOOD COVER	BAD COVER
Substantial Brickwork or Concrete	Internal Partition Walls
Engine Blocks	Car Doors
Base of Large Live Trees	Wooden Fences
Natural Ground Undulations	Glazing

Confirm

- It is a firearms / weapons incident.
- Exact location of the incident.
- Number of gunmen.
- Type of firearm - are they using a long-barrelled weapon or handgun
- Direction of travel - are they moving in any particular direction

Consider the use of CCTV and other remote methods of confirmation reducing vulnerabilities to staff.

Contact

- **Who** - Immediately contact the police by calling 999 or via your control room, giving them the information shown under **Confirm**
- **How** - use all the channels of communication available to you to inform students, staff and visitors of the danger.
- **Plan** - for a firearms / weapons incident.
    1. How you would communicate with students, staff and visitors
    2. What key messages would you give to them in order to keep them safe.
    3. Think about incorporating this into your emergency planning and briefings
- **Test** - your plan before you run your event

Control

- As far as you can, limit access and secure your immediate environment.
- Encourage people to avoid public areas or access points. If your have rooms at your location, lock the doors if possible and remain quiet.

See Physical Security on page 15.

If you require further information please liaise with your Counter Terrorism Security Adviser (CTSA) .

seventeen hostile reconnaissance

Hostile reconnaissance is used to provide information to operational planners on potential targets during the preparatory and operational phases of terrorist operations. Many of the activities described below are linked to normal behaviour at Educational institutions. It is behaviour or activities outside of what would be described as normal, that requires reporting to police and monitoring if possible.

Primary Role of Reconnaissance

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

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

Operation Lightning is a national intelligence gathering operation to record, research, investigate and analyse:

- Suspicious sightings.
- Suspicious activity.

at or near:

- Crowded places.

or prominent or vulnerable:

- Buildings.
- Structures.
- Transport infrastructure.

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

The following sightings or activity may be particularly relevant to your institution.

- Significant interest being taken in the outside of your establishment including parking areas, delivery gates, doors and entrances.
- Groups or individuals taking significant interest in the location of CCTV cameras and controlled areas.
- People taking pictures, filming, making notes or sketching of the security measures. Tourists should not necessarily be taken as such and should be treated sensitively, but with caution.
- Overt/covert photography, video cameras, possession of photographs, maps, blueprints etc, of critical infrastructures, electricity transformers, gas pipelines, telephone cables, etc.

- Possession of maps, global positioning systems (GPS), photographic equipment (cameras, zoom lenses, camcorders). GPS will assist in the positioning and correct guidance of weapons such as mortars and Rocket Propelled Grenades (RPGs). This should be considered a possibility up to one kilometre from any target.
- Vehicles parked outside buildings or other facilities, with one or more people remaining in the vehicle, for longer than would be considered usual.
- Parking, standing or loitering in the same area on numerous occasions with no apparent reasonable explanation.
- Prolonged static surveillance using operatives disguised as demonstrators, street sweepers, etc or stopping and pretending to have car trouble to test response time for emergency services, car recovery companies, (AA, RAC etc) or local staff.
- Simple observation such as staring or quickly looking away.
- Activity inconsistent with the nature of the building.
- Unusual questions - number and routine of staff/VIP's visiting the institution.
- Individuals that look out of place for any reason.
- Individuals that appear to be loitering in public areas.
- Individuals asking questions regarding the identity or characteristics of individual visitors, groups of visitors, or the jobs or nationalities of visitors, that may visit the institution.
- Persons asking questions regarding security and evacuation measures.
- Persons asking questions regarding institution staff or student hangouts.
- Persons asking questions regarding VIP visits.
- Delivery vehicle in front of the establishment.
- Vehicles, packages, luggage left unattended.
- Vehicles appearing over weight.
- Persons appearing to count pedestrians/vehicles.
- Strangers walking around perimeter of the institution.
- People 'nursing' drinks and being over attentive to surroundings. Persons loitering around area for a prolonged amount of time.
- Persons attempting to access plant equipment or chemical areas.
- Delivery vehicles or other trucks attempting to access the main driveway to the institution.
- Delivery vehicles arriving at the institution at the wrong time or outside of normal hours.
- Vehicles emitting suspicious odours e.g. fuel or gas.
- Vehicle looking out of place.
- Erratic driving.
- Questions regarding the institution structure.
- Noted pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures, (bomb threats, leaving hoax devices or packages).

- The same vehicle and different individuals or the same individuals in a different vehicle returning to a location(s).
- The same or similar individuals returning to carry out the same activity to establish the optimum time to conduct the operation.
- Unusual activity by contractor's vehicles.
- Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or assault equipment, i.e. ropes, ladders, food etc. Regular perimeter patrols should be instigated months in advance of a high profile event to ensure this is not happening.
- Attempts to disguise identity - motorcycle helmets, hoodies, etc. or multiple sets of clothing to change appearance.
- Constant use of different paths, and/or access routes across a site. 'Learning the route' or foot surveillance involving a number of people who seem individual but are working together.
- Multiple identification documents - suspicious, counterfeit, altered documents etc.
- Non co-operation with police or security personnel.
- Those engaged in reconnaissance will often attempt to enter premises to assess the internal layout and in doing so will alter their appearance and provide cover stories.
- In the past reconnaissance operatives have drawn attention to themselves by asking peculiar and in depth questions of employees or others more familiar with the environment.
- Sightings of suspicious activity should be passed immediately to security management for CCTV monitoring, active response were possible and the event recorded for evidential purposes.

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

Reconnaissance trips may be undertaken as a rehearsal to involve personnel and equipment that will be used in the actual attack e.g. before the London attacks on 7th July 2005, the bombers staged a trial run nine days before the actual attack.

Reporting suspicious activity to police that does not require an immediate response, contact the CONFIDENTIAL ANTI-TERRORIST HOTLINE - 0800 789 321

ANY INCIDENT THAT REQUIRES AN IMMEDIATE RESPONSE - DIAL 999.

eighteen high profile events

There may be events held at your institution, which for various reasons, are deemed to be more high profile and therefore more vulnerable to attack. This may involve pre-event publicity of the attendance of a VIP or celebrity, resulting in additional crowd density on the event day and the need for an appropriate security response and increased vigilance.

In certain cases the local police may appoint a police Gold Commander (Strategic Commander in Scotland) with responsibility for the event; who may in turn, appoint a Police Security Co-ordinator (SECCO) and/or a Police Search Adviser (POLSA).

Police Security Co-ordinator

The Police Security Co-ordinator (SECCO) has a unique role in the planning and orchestration of security measures at high profile events.

The SECCO works towards the strategy set by the Police (Gold) Strategic Commander and acts as an adviser and co-ordinator of security issues.

A number of options and resources are available to the SECCO, which will include liaison with event management, identifying all the key individuals, agencies and departments involved in the event as well as seeking advice from the relevant Counter Terrorism Security Advisor.

The SECCO will provide the Gold/Strategic Commander with a series of observations and recommendations to ensure that the security response is realistic and proportionate.

Police Search Adviser

The SECCO can deem it necessary to appoint a Police Search Adviser (POLSA) to a high profile event.

The POLSA will carry out an assessment of the venue and nature of the event, taking into consideration an up to date threat assessment and other security issues.

A report, including the POLSA's assessment, recommendations and subsequent search plan will be submitted through the SECCO to the Gold/Strategic Commander.

Enhanced Security Provision at High Profile Events

During High Profile Events there may be extra threats not only from terrorism but criminal activity, politically disruptive groups, fixated persons, self-publicists and lone adventurers.

Enhanced measures may be required in order to provide static protection or in order to eliminate or reduce the opportunity for attack by placing defensive perimeters between any protected person and a potential attacker.

Dependent on the nature of the threat and outcome of the risk management process, consideration should be given to a range of physical, technical and procedural protective security options that may, on their own, be sufficient to exclude, deter, detect or disrupt the threat.

What measures need to be considered

For major events an "Island site" is commonly created to provide a sterile zone around it, with secure perimeter access which is rigorously controlled by static protection measures.

Physical and technical security measures may include:

- Physical protection measures such as extra doors, locks, lighting and target hardening.
- Technical measures including enhanced or extended CCTV and alarms if required.
- Vehicle security at the event site.
- Personal safety advice to VIP's on reducing their own vulnerability when travelling to and from a venue, avoiding predictable routines, etc.
- Care and retention of sensitive information and communications, this is particularly pertinent when advertising the event, is the event public or private, official or unofficial and the extent of pre-publicity or public knowledge of an event may cause the level of threat or resultant planning to change considerably.
- Early identification of all organisations involved in the event, their roles and responsibilities. Including details of the structures of each organisation and links between respective functional levels.
- The circumstances under which an event will be discontinued and the method and ownership for such decisions, and means by which by which this will be communicated.
- The circumstances under which a venue will be evacuated and VIP's removed.
- Clarification of the role, powers and capability of any private security staff or stewards either permanent or temporarily contracted for the specific event. This includes any specialist skills required for searching, e.g. operating search equipment, search arches or luggage scanning.
- Prepare lists for restricted circulation only to partners (see care and retention of sensitive material above), incorporating invited and confirmed guests, chronology of events, copies of invitations, car passes and any other relevant materials, such as plans, maps and contact lists, etc.
- Specimen copies of any accreditation passes and badges allowing access to the various security zones, etc.
- Create security zones within the secure perimeter to segregate VIP's from invited guests, the general public and the media, etc. Consider providing a 'Green Room' or place of safety where a VIP could shelter in the event of an incident.
- Identity safe routes to and from the venue, as well as safe evacuation / escape routes.
- Arrangement of parking for VIP vehicles and consideration of parking restrictions adjacent to the venue if a VBIED threat is identified.
- Ensure the personnel security and secure contracting principles referred to in chapter eleven are strictly adhered to for secure areas and island sites.
- Where a particular venue is likely to be used as a more permanent venue or on a long term basis, Crime Prevention Through Environmental Design (CPTED) principles should be considered along side any appropriate Counter Terrorism security advice, with the aim of designing out identified structural vulnerabilities.
- Liaison with security providers and other partners should be ongoing rather than a 'one-off' process.

See Good Practice Checklist - High Profile Events in Appendix 'J'

nineteen threat levels

As of 1 August 2006, information about the national threat level is available on the Security Service, Home Office and UK Intelligence Community Websites.

Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. This information may well be incomplete and decisions about the appropriate security response should be made with this in mind.

In particular, those who own, operate, manage or work at major events are reminded that SUBSTANTIAL and SEVERE both indicate a high level of threat and that an attack might well come without warning.

Threat Level Definitions

CRITICAL	**AN ATTACK IS EXPECTED IMMINENTLY**
SEVERE	**AN ATTACK IS HIGHLY LIKELY**
SUBSTANTIAL	**AN ATTACK IS A STRONG POSSIBILITY**
MODERATE	**AN ATTACK IS POSSIBLE BUT NOT LIKELY**
LOW	**AN ATTACK IS UNLIKELY**

Response Levels

Response levels provide a broad indication of the protective security measures that should be applied at any particular time. They are informed by the threat level but also take into account specific assessments of vulnerability and risk.

Response levels tend to relate to sites, whereas threat levels usually relate to broad areas of activity.

There are a variety of site specific security measures that can be applied within response levels, although the same measures will not be found at every location.

The security measures deployed at different response levels should not be made public, to avoid informing terrorists about what we know and what we are doing about it.

There are three levels of response which broadly equate to threat levels as shown below:

CRITICAL	**EXCEPTIONAL**
SEVERE	**HEIGHTENED**
SUBSTANTIAL	
MODERATE	**NORMAL**
LOW	

Response Level Definitions

RESPONSE LEVEL	DESCRIPTION
EXCEPTIONAL	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk.
HEIGHTENED	Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk.
NORMAL	Routine baseline protective security measures, appropriate to your business and location.

What can I do now?

- **Carry out a risk and vulnerability assessment that is specific to your event.**
- **Identify a range of practical protective security measures appropriate for each of the response levels. Your Counter Terrorism Security Advisor can assist you with this.**
- **Make use of the good practice checklists on the following pages to assist you in your decision making process.**

The counter measures to be implemented at each response level are a matter for individual premises or organisations and will differ according to a range of circumstances.

All protective security measures should be identified in advance of any change in threat and response levels and should be clearly notified to those staff who are responsible for ensuring compliance.

twenty communication and training

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

A communication strategy incorporating both the physical and electronic activities and supporting the delivery of safe passage, messaging and signage. The placing, interpretation and integration of signage is essential for enabling invacuation and evacuation within or outside a building or buildings. Associated with this is the electronic activation of messaging services through telephone, radio, electronic signage and other media assistance with the delivery of a clear and deliverable output which will in turn support other communication elements being utilised. Safe passage away from areas under threat is the key rationale behind any such strategy and should have contingency delivery built into the planning stages to enable alternative activities to take place if the planning capability is compromised.

The consideration of a signage strategy incorporating placement, size and directional activity is a key aspect of an overall communication strategy. The delivery of effective and efficient movement possibilities from one area to another reduces tensions during an evacuation, invacuation or other threat situation.

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

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

Security Managers should regularly meet with staff to discuss security issues and encourage staff to raise their concerns about security.

Consideration should be given to the use of any website and/or publications that could communicate crime prevention and counter terrorism initiatives.

All Security Managers should involve their local Counter Terrorism Security Adviser and/or Police Security Co-ordinator when considering improvements to an established site or premises for the purposes of holding a significant event.

You could consider establishing networks of good practice among AUCSO, AOC and HEBCoN colleagues.

Further training or presentations such as Project Griffin or Operation Fairway (DVD) may be available for suitable staff via your local Counter Terrorism Security Advisor.

See Good Practice Checklist - Communication in Appendix 'I'

good practice checklists

The following checklists are intended as a guide for those who manage security at education institutions to assist them in identifying the hazards and risks associated with counter terrorism planning.

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

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

- Have you consulted your, Counter Terrorism Security Advisor, Police Security Co-ordinator, local authority and local fire and rescue service?
- Who else should be included during consultation - e.g. Highway Manager, Open Space Manager and Land Owner?
- Which measures can be implemented with ease?
- Which measures will take greater planning and investment?

appendix a

Emergency and Business Continuity Planning

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

appendix b

Housekeeping Good Practice

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

appendix C

Access Control for Institutions

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

appendix d

CCTV

	Yes	No	Unsure
Do you constantly monitor your CCTV images or playback overnight recordings for evidence of suspicious activity?			
Do you have an active response to your CCTV monitoring programme?			
Do you have your CCTV cameras regularly maintained?			
Do the CCTV cameras cover the entrances and exits to your institution?			
Have you considered the introduction of ANPR to complementyour security operation?			
Do you have CCTV cameras covering critical areas in your institution, such as IT equipment, back up generators, cash offices and restricted areas?			
Do you store the CCTV images in accordance with the evidential needs of the police?			
Could you positively identify an individual from the recorded images on your CCTV system?			
Are the date and time stamps of the system accurate?			
Does the lighting system complement the CCTV system during daytime and darkness hours?			
Do you regularly check the quality of your recordings?			
Are your 'contracted in' CCTV operators licensed by the Security Industry Authority (SIA)?			
Have you implemented operating procedures, codes of practice and audit trails?			
Is each CCTV camera doing what it was installed to do?			

appendix e

Searching

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

appendix f

Evacuation / 'Invacuation'

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

appendix g

Personnel Security - identity assurance

	Yes	No	Unsure
During recruitment you should require:			
Full name			
Current address and any previous addresses in last five years			
Date of birth			
National Insurance number			
Full details of references (names, addresses and contact details)			
Full details of previous employers, including dates of employment			
Proof of relevant educational and professional qualifications			
Proof of permission to work in the UK for non-British or non-European Economic Area (EEA) nationals			
Do you ask British citizens for:			
Full (current) 10-year passport			
British driving licence (ideally the photo licence)			
P45			
Birth Certificate – issued within six weeks of birth			
Credit card – with three statements and proof of signature			
Cheque book and bank card – with three statements and proof of signature			
Proof of residence – council tax, gas, electric, water or telephone bill			
EEA Nationals:			
Full EEA passport			
National Identity Card			
Other Nationals:			
Full Passport and			
A Home Office document confirming the individual's UK Immigration status and permission to work in UK			
Identity Card for foreign nationals. Further information is available at www.ukba.homeoffice.gov.uk			

appendix h

Information Security

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

appendix i

Communication

	Yes	No	
Are security issues discussed/decided at senior management level and form a part of your organisation's culture?			
Do you have a security policy or other documentation showing how security procedures should operate within your institution?			
Is this documentation regularly reviewed and if necessary updated?			
Do you regularly meet with staff and discuss security issues?			
Do you encourage staff to raise their concerns about security?			
Do you know your local Counter Terrorism Security Adviser (CTSA) and do you involve them in security developments?			
Do you speak with your neighbours about issues of security and crime that might affect you all?			
Do you remind your staff to be vigilant when travelling to and from work, and to report anything suspicious to the relevant authorities or police?			
Do you make use of your website, to communicate crime and counter terrorism initiatives, including an advance warning regarding searching?			

appendix j

High Profile Event

	Yes	No	Unsure
Do you consider "island Site" for VIP's in your planning phrase?			
Do you consider extra physical and technical measures for High Profile Events?			
Do you offer or plan for security VIP advice when travelling to and from your institution / event?			
Do you have separate security arrangements for the care and retention of sensitive information and communications?			
Do you have special arrangements for cancellation and/or evacuation during these events?			
Are security access controls and security passes enhanced and details recorded?			
Do you arrange special parking and evacuation routes for VIP's?			
Are CTSA's and other important partners liaised with on regular basis?			

What do the results show?

Having completed the various 'Good Practice' checklists you need to give further attention to the questions that you have answered 'no' or 'Unsure' to.

If you answered 'Unsure' to a question, find out more about that particular issue to reassure yourself that this vulnerability is being addressed or needs to be addressed.

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

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

grab bag checklist

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

Equipment:

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

Some extra items you could consider:

- Spare keys / security codes
- Mobile telephone with credit available, plus charger (wind up if possible).
- Disposable / Small camera.
- Hard hats / protective goggles / heavy duty gloves

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

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

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

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

bomb threat checklist

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

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

Actions to be taken on receipt of a bomb threat:

Switch on tape recorder/voicemail (if connected)

Tell the caller which town/district you are answering from

Record the exact wording of the threat:

_____

_____

Ask the following questions:

Where is the bomb right now? _____

When is it going to explode? _____

What does it look like? _____

What kind of bomb is it? _____

What will cause it to explode? _____

Did you place the bomb? _____

Why? _____

What is your name? _____

What is your address? _____

What is your telephone number? _____

(Record time call completed:)

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

_____

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

_____

Contact the police on 999. Time informed: _____

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

Time and date of call: _____

Length of call: _____

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

ABOUT THE CALLER

Sex of caller: _____

Nationality: _____

Age: _____

THREAT LANGUAGE (tick)

❒ Well spoken?

❒ Irrational?

❒ Taped message?

❒ Offensive?

❒ Incoherent?

❒ Message read by threat-maker?

CALLER'S VOICE (tick)

❒ Calm?

❒ Crying?

❒ Clearing throat?

❒ Angry?

❒ Nasal?

❒ Slurred?

❒ Excited?

❒ Stutter?

❒ Disguised?

❒ Slow?

❒ Lisp?

❒ Accent? If so, what type?_____

❒ Rapid?

❒ Deep?

❒ Hoarse?

❒ Laughter?

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

BACKGROUND SOUNDS (tick)

❒ Street noises?

❒ House noises?

❒ Animal noises?

❒ Crockery?

❒ Motor?

❒ Clear?

❒ Voice?

❒ Static?

❒ PA system?

❒ Booth?

❒ Music?

❒ Factory machinery?

❒ Office machinery?

❒ Other? (specify) _____

OTHER REMARKS

_____

_____

_____

_____

Signature

_____

Date _____

Print name

_____

useful publications

Publications

Protecting Against Terrorism (2nd Edition)
This 38 page booklet gives general protective security advice from Mi5's Centre for the Protection of National Infrastructure (CPNI). It is aimed at businesses and other organisations seeking to reduce the risk of a terrorist attack, or to limit the damage terrorism might cause. The booklet is available in PDF format and can be downloaded from www.cpni.gov.uk or email enquiries@cpni.gsi.gov.uk to request a copy.

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

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

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

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

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

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

Both booklets and a viewable version of the 'Secure in the Knowledge' DVD are now available to download and view from the NaCTSO website www.nactso.gov.uk

Emergencies - Planning for and Managing: A good practice guide for Higher Education Institutions - The Association of University Chief Security Officers (AUCSO)

This Guide provides information on good practice in emergency management with specific reference to Higher Education Institutions (HEIs) in the UK.The aim of the Guide is to assist HEIs in developing their ability to respond to emergencies. In particular the document seeks to assist those involved in emergency management activities in developing and reviewing their emergency plans, provide further information and access to resources (including research, local networks and additional guidance in this field) and consolidate understanding among Higher Education (HE) managers. (available to download at www.ukresilience.go.uk)

useful contacts

NaCTSO (National Counter Terrorism Security Office)
t. 020 7931 7142
www.nactso.gov.uk

Security Service
www.mi5.gov.uk

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

Home Office
t. 020 7035 4848
www.homeoffice.gove.uk

ACPO (Association of Chief Police Officers)
t. 020 7227 3434
www.acpo.police.uk

ACPOS (Association of Chief Police Officers Scotland)
t. 0141 435 1230
www.acpos.police.uk

HOSDB (Home Office Scientific Development Branch)
t. 01727 816400
www.hosdb.homeoffice.gov.uk

The Business Continuity Institute
t. 0870 603 8783
www.thebci.org

London Prepared
www.londonprepared.gov.uk

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

Confidential Anti-terrorism Hotline
t. 0800 789321

Chief Fire Officers Association
t. 01827 302300
www.cfoa.org.uk

National Risk Register
t. 020 7276 1234
www.cabinetoffice.gov.uk

International Centre for Crowd Management and Security Studies
www.crowdsafetymanagement.co.uk

Emergency Planning Society
www.the-eps.org

HEBCoN (Higher Education Business Continuity Network)
www.hebcon.org.uk

AUCSO (Association University Chief Security Officers)
www.aucso.org.uk

DIUS (Department Innovation Universities and Skills)
www.dius.gov.uk

Universities UK
www.univrsitiesuk.ac.uk

AoC (Association of Colleges)
www.aoc.co.uk

GuildHE
www.guildhe.ac.uk

notes

Acknowledgments

With thanks to the following for their knowledge, expertise and time

Centre for the Protection of National Infrastructure (CPNI)
Department Innovation Universities and Skills (DIUS)
The Association of University Chief Security Officers (AUCSO)
Universities UK
Association of Colleges (AoC)
Higher Education Business Continuity Network (HEBCoN)
Medical Research Council (MRC)
GuildHE

Thanks to all universities and further education colleges/institutions that assisted in this publication

Produced by the National Counter Terrorism Security Office

Home Office

CPNI
Centre for the Protection of National Infrastructure

© ACPO 2009. The Association is a private company limited by guarantee. Registered No. 3344583
Registered office. 25 Victoria Street, London SW1H 0EX.