



HOME OFFICE

BOMBS

Protecting People and Property

A HANDBOOK FOR MANAGERS - FOURTH EDITION

Preface

This is the fourth edition of the handbook *Bombs – Protecting People and Property* which was first published by the Home Office in 1994. The text has been fully revised: it incorporates the best and most up-to-date advice from experts in Government and the Police Service.

Bombs – Protecting People and Property has been written specifically with managers in mind. The advice which it contains is relevant to all businesses and organisations large or small and to local government.

The handbook is, of necessity, written with a wide audience in mind. It does not – cannot – address the particular circumstances of each reader. More detailed or specific advice and guidance on your business needs can be obtained from local police Crime Prevention Departments. You can make contact with the Crime Prevention Department in your area through your local police station.

Main Messages

- Assess the likelihood of terrorist attack on your organisation and plan your physical security measures accordingly
- Prepare your staff for the possibility of telephoned bomb threats
- Choose the mix of protective measures that best suits your premises and that will deter or detect the terrorist
- Encourage your staff to protect themselves and your customers and visitors through vigilance and good housekeeping
- Test your plans regularly, and evaluate the response
- Plan for – evacuation
 - search
 - recovery
- Participate in the counter-terrorist security planning in your community: communities defeat terrorism

More specific advice may be obtained from Police Crime Prevention Departments: the advice is free – please seek it.

Contents

Main Messages

Part 1	Introduction	6
Part 2	The Terrorist Threat	7
Part 3	Why Plan At All?	8
Part 4	Devices – And the Damage They Do	9
Part 5	Telephoned Bomb Threats	10
Part 6	Asset Protection	11
Part 7	Security Planning	13
Part 8	Five Plans for Five Possibilities	15
Part 9	Evacuation	19
Part 10	Search	21
Part 11	The Role of the Police	23
Part 12	Recovery Plans	24
Part 13	Useful Addresses	25
Appendix 1	Telephoned Bomb Threat Aide-Mémoire	26
Appendix 2	Protection against Flying Glass	28



Part I Introduction

1 In recent years the world has had to get to grips with terrorist crime. The threat presented in the United Kingdom has been at its greatest in connection with the affairs of Northern Ireland. But other groups have also resorted to terrorist crime to publicise their political objectives. Some of these groups are concerned with domestic issues, others operate on the international stage. Some seek to target particular organisations or individuals, others are more indiscriminate in their targeting.

2 It is important to keep the threat in perspective. Terrorist incidents in Great Britain are far from commonplace but when they occur they attract considerable publicity. For most of us, terrorism will remain something which we hear about on the news.

3 Others, however, will find themselves caught up in some way with a terrorist crime. This might be through receiving a telephone threat that a bomb has been planted; being evacuated from an area in which police suspect the presence of a bomb or, for the unfortunate few, being in the vicinity of a bomb explosion.

4 This handbook is designed to help reduce vulnerability to the threat from terrorism. It has been

written for managers in the private and public sectors. Because it addresses a wide audience the advice is general rather than specific. However, the guidance is sufficiently detailed to allow managers to adapt it to the circumstances of their own organisations.

5 More specific advice may be obtained from Police Crime Prevention Departments. The advice is free – please seek it.

6 The handbook aims to help managers to:

- assess the terrorist threat;
- take precautions against the threat of terrorist attack; and
- respond effectively to terrorist incidents.

7 Terrorists are seeking to get their way by violence; to cause damage to people and property; and to gain publicity for their cause. By adopting the measures suggested in this handbook, managers can prevent this.



The Terrorist Threat Part 2

8 Terrorist crimes, often involving shocking acts of violence, are used by various groups or individuals to promote various causes. Sometimes the criminal may resort to terrorist tactics for the purposes of extortion. They may choose specific targets; for example, persons or organisations associated with their political opponents. But increasingly there have been indiscriminate attacks, perhaps aimed at general disruption to the economic life of a country, which place members of the public at direct risk.

Assessing the Threat

9 It is not possible to produce a definitive statement on how to assess the threat of terrorist attack. But it is quite possible to work out the threats to a particular site or organisation, even though the causes that terrorists espouse may seem remote from everyday life. Here is a simple checklist of issues to take into account:

- What does the news tell us about the current national and international climate, or current terrorist campaigns?
- What can the local police tell you about the chance of a terrorist attack in your neighbourhood?
- Is there something about your building or your staff that would attract a terrorist attack: are you seen as having a special relationship with a high profile individual who is a terrorist target in his or her own right; has your company name been associated with animal experimentation?

- Does your location mean that you may suffer collateral damage from an attack on a high risk neighbour?

Terrorist capability – what they might do, and how – is one of the crucial factors in assessing threat. This booklet will describe terrorist capabilities in broad terms so that you can plan with that in mind.

Assessing the Vulnerability

10 You know already what it is that is important to you and your business survival. You probably have plans to safeguard some, or all, of these things from other threats already. For example, you will have defences against, and plans in anticipation of, fire, and defences against criminals who may want to steal your stock.

11 If you have reason to believe that you are likely to be a terrorist target because of the nature of your business, you should anticipate that terrorists will do research to work out where your greatest vulnerability is. What material about you is in the public domain? What published facts point to installations or services that are vital to the continuance of the business? What might attract attention as a prestige target even though its loss may not mean immediate business collapse?

Giving thought to what matters to you, and what is most vulnerable, will enable you to make realistic plans for deterring terrorist attack and minimising the damage should one occur at or near your premises.



Part 3 Why Plan At All?

12 Terrorist attacks, and attacks by extremist campaigners or malicious hoaxers, are designed to intimidate, disrupt, cause economic damage and – in some circumstances – cause injury or loss of life. There are good business reasons for planning to avoid all of these possibilities – or at least to minimise their consequences.

13 But there are also obligations on everyone (employer and employee alike) to play their part in protecting themselves and others. In a counter-terrorist context the police and other agencies may offer advice but the responsibility to seek advice and act upon it lies with the owner or occupier of the premises.

Health & Safety at Work Regulations 1992

14 These regulations provide that:

- All employers owe their staff and visitors a duty of care: the responsibility for safety on their premises rests with employers, not the police.
- Appropriate procedures must be in place in the event of serious, imminent danger.
- There should be persons competent to implement the procedures. (A competent person is one who has sufficient training and experience or knowledge to do what is required of him or her).
- Employees must be informed of the hazards, and the steps to be taken.

- In the case of serious, imminent danger, work must be stopped immediately and people must be moved to a place of safety.
- Access must be restricted, and resumption of normal work prevented, while the serious and imminent danger persists.

In the event of an incident, plans are disclosable and may be the subject of scrutiny in any subsequent enquiries or court proceedings.

What Should be Done?

15 Action should be on the following lines:

- Think about the threats you may face.
- Take the best available advice on the things you can do to reduce the chances that a bomb will cause injury to your staff or visitors.
- Make a contingency plan, ensure that all staff are familiar with it – and practise it.

The material in this booklet will help you to take all these steps, and give you some pointers towards simple measures that can be taken that will considerably reduce vulnerability to explosive devices of all types. Further advice is available through your local police Crime Prevention Department.



Devices – And the Damage They Do Part 4

16 Explosive or incendiary devices come in almost any shape and form. Past attacks have involved incendiary devices built into cigarette packets or tape cassettes, devices involving military grade high explosive in briefcases or sports bags or specially made for particular sites, and lorries packed with home-made explosive. There can be no exact descriptions of what to expect. But the details in this section will help managers to:

- focus on what damage each type of attack may do; and
- with the help of the remainder of this booklet, and the support of the Crime Prevention Department, plan for the consequences.

17 In Great Britain, businesses are most likely to face attack by:

- explosive or incendiary items which are delivered (the letter or package that comes by post or by hand);
- improvised incendiary devices;
- an improvised explosive device (“a home-made bomb”) in the building; or
- an improvised explosive device outside the building.

Delivered Items

18 The traditional postal bomb takes many forms – parcels, padded “jiffybags”, or envelopes of any shape or size. They may be delivered by hand or via a courier as well as “through the post”.

Postal bombs are generally designed to kill or maim the person who is opening them. Their effect is local. But a parcel bomb in particular may be large and designed to cause structural damage, in the same way as the bomb in the building.

The Bomb in the Building

19 Terrorists in particular have a long history of leaving hand-carried devices – hold-alls and so on – in public places or places to which access is simple. A device of this size can kill or maim anyone close to the seat of the blast, inflict injury on people and damage to stock in the immediate vicinity, and cause damage to glazing, cladding etc.

The Bomb outside the Building

20 The hand-carried bomb may also be a feature of terrorist attacks in the street or other public places like station concourses. More frequently in recent years, we have become accustomed to vehicle-borne devices, and particularly the lorry packed with home-made explosive. Such vehicles may contain 1 tonne or more of explosive:

- there will be major structural damage to buildings in a radius of up to about 50m;
- glass which is capable of killing or maiming will fall in a radius of 250m; and
- metal fragments from the device may still cause injury at 500m and beyond.



Part 5 Telephoned Bomb Threats

21 Terrorists sometimes telephone threats of bomb attacks; their calls appear to fall into two categories:

- 1 threats that actual devices have been planted; the aim is to save life (or to be able to blame inaction by others if there are casualties);
- 2 threats where no device has been planted, designed to disrupt.

22 The overwhelming number of telephoned bomb threat calls are made by malicious pranksters whose threats are empty. But making such calls is a crime, and they should always be reported to the police.

23 Occasionally the calls will actually be from terrorists. You will not be able to assess whether or not a call is “genuine”. The calls constitute a threat to the lives of your staff or your business or the lives of others in the community, and they must always be treated seriously and handled urgently.

24 Such calls may be the closest that you and your staff will come to terrorism. Because of the potential seriousness of each and every call, planning is needed, just as it is for other forms of attack.

25 The likelihood that you will be a recipient is increased if you are known or thought to operate a 24 hour switchboard service, and there is a belief that you will react quickly. Hotels and hospitals, organisations offering any sort of “emergency” service (including voluntary organisations), news agencies and any organisations involved with public transport may wish to give their switchboard operators special training in handling such calls.

26 But anyone may be a recipient of a bomb threat call. Handling them is not simple. It is difficult to remain calm and react effectively. Staff may be traumatized by the incident and will suffer more if they blame themselves for not reacting as well as they would have liked. The golden rules are:

- keep calm;
- try to obtain as much information as possible;
- dial 1471 (if that facility operates); and
- report it to the security co-ordinator and the police immediately.

All these things are difficult. To assist, a checklist is at Appendix 1. This should be on hand for use by all switchboard or reception staff.

27 The first line of defence against the common criminal may also prevent the terrorist from gaining access to premises. In terrorism, the priorities are to protect:

- the lives of staff and visitors;
- the contents of the building; and
- the fabric of the building.

Deter and Detect

28 Police Crime Prevention Departments will be able to provide all the necessary expert advice on physical security measures. Fire Departments and Planning Departments may also need to be consulted. What follows is therefore only a quick guide to the main considerations when seeking to deter or detect terrorism.

Doors

29 All external doors should meet the minimum requirements in respect of robustness and standard of locking systems. Those not in regular use should also have strong internal bolts. Glazed doors are only as secure as their glazing and this will need special attention.

Access Routes

30 The most effective access control is an efficient reception area. Access to side and rear entrances should be restricted to authorised persons only. Digital, swipecard or proximity locks all offer protection if security or reception staff cannot be present.

31 Visitors should be escorted, or wear temporary passes which might be colour-coded to show their validity and surrendered on leaving the building. Unauthorised visitors will be easier to detect if staff are asked to wear their passes at all times.

32 Searching of hand baggage and luggage has enormous deterrent value, and is well worth considering when the police have informed you that there is a particular risk. You have the right to refuse entry to any person who will not permit a search of their hand baggage.

You may also consider a body search but you have no power to carry out such a search unless the person agrees.

Windows

33 As a minimum, good quality key operated locks should be fitted to all ground floor windows and any windows to which access might be gained (eg from a flat roof).

Intruder Alarms

34 Many different forms exist and have to be selected for the circumstances of each site or installation.

CCTV

35 CCTV can make an important contribution to security in shops, outside buildings and in public places, as it is already doing across the country in the general context of community safety. The presence of cameras may also help to deter terrorists. If the system is of high quality and the product is recorded, CCTV provides a considerable aid to post-incident investigation which itself acts as a deterrent.

Lighting

36 Good lighting is a deterrent in its own right, and is essential for effective CCTV coverage.

37 In multi-occupancy buildings, shopping centres, high streets, business parks and the like, it is essential to make security – in the terrorist context just as in relation to any other crime – a joint communal effort. For example, common access control procedures can be agreed or CCTV cameras can be sited for maximum overall benefit. Effectiveness can be increased and costs greatly reduced.

38 It is possible to waste a lot of money on ineffective security systems. All good systems require the planning of an integrated security package that is focused on protecting your most valuable assets and your most vulnerable points. Remember, specific advice is available from the Crime Prevention Department – and it is free.



Good Housekeeping

39 Good housekeeping both inside and outside premises will reduce the opportunity for the planting of devices. Within buildings reduce the number of places where devices can be left:

- lock unoccupied offices and store cupboards;
- put simple plastic seals on maintenance hatches to which only occasional access is required;
- keep a place for everything and everything in its place;
- all communal areas – stairs, halls, toilets, rest rooms – should be kept clean and tidy;
- consider the removal of litter bins; but if you choose this option, take special care to increase cleaning effort so that rubbish is swiftly removed; and
- keep furniture in public areas to a minimum, and ensure that furniture and fittings are designed without spaces which give opportunities to hide a device.

40 Outside buildings, the same principles apply:

- keep everywhere as tidy as possible, including shrubbery and especially when it is close to entrances; and
- choose furniture and fittings that do not have spaces in which devices can be concealed.

Vigilance

41 Staff are certain to be one of your most valuable assets, and their protection is paramount. They are also one of the best sources of protection. They will usually know their own office, department, car park or whatever intimately. They should be encouraged to keep a sharp lookout for unusual behaviour or items out of place. Staff must be given confidence to report things and must know that their reports are taken seriously and recognised as a contribution to the business.

42 In a terrorist context they should particularly look out for anyone placing, rather than dropping, a packet or a bag in an unusual place, or in a fairly inaccessible spot like the back of a shelf in a shop.

Reducing the Consequences of Explosions

43 Planning for terrorist contingencies, and exercising search and evacuation plans are described in the following sections and are all part of reducing the damage that terrorists can do to your staff and business. As part of the physical security of your building, however, there are certain measures that you can take in respect of glazing that will considerably reduce death and injury to your staff and customers and bystanders.

Glazing Protection

44 Most casualties of terrorist attacks result from flying glass. There is extensive research data on blast effect on glass and tested solutions that will minimise the degree of shattering, the amount of injury and the costs of eventual building re-occupation. The solutions involve selecting combinations of types and thicknesses of glass to suit the circumstances, but a significant degree of protection can be obtained by using anti-shatter film, which holds fragments together, in combination with properly designed net curtains, which will contain flying glass in a “spinnaker” type effect. Detailed specifications are contained in Appendix 2.

Appointing a Security Co-ordinator

45 Successful response to an actual or potential terrorist attack depends on the creation of a company security policy and the appointment of a security co-ordinator to have full oversight of, and authority for, the totality of the terrorist security planning process.

46 The co-ordinator must have sufficient authority to direct the action to be taken in response to security threats. If he or she is not the Chief Security Officer, the person with the terrorist co-ordination responsibility must be involved in the planning and design of the building's exterior security, access control and so on, so that the terrorist dimension is taken into account. The co-ordinator must be consulted over any new building or renovation work, so that terrorist crime can be catered for in the design of the building, and the specification of glazing.

47 The co-ordinator should establish liaison with the Crime Prevention Department as a local and expert source of knowledge. During the development of plans, it is advisable to consult with all the emergency services. Under the Prevention of Terrorism Act 1989, police officers have special powers at or within cordons. Plans, particularly regarding evacuation, must therefore be shared with the police who are responsible for ensuring the safety of the general public in the vicinity of your building.

48 The co-ordinator has seven main responsibilities:

- production of the risk assessment, and the consequent defensive measures and planning;
- devising and maintaining a search plan;
- devising and maintaining evacuation plans;
- deciding on the extent and direction of evacuation;
- deciding when to re-occupy;
- liaising with the police and other emergency services; and
- arranging staff training, communication cascades and drills, including training for his or her own deputies.

The co-ordinator's end product should be a plan or set of plans that have been checked with the police and practised, and are regularly audited to ensure that they are still current and workable.

Creating Security Plans

49 There are three crucial steps in drawing up counter-terrorist plans:

Step One

- Identify what sort of threats you are facing.

Step Two

- Identify what it is that you want to protect (people, property and data are the three common categories) and in what ways they are vulnerable to terrorist attack in particular.

Step Three

- Identify the most appropriate measures to reduce the risk to an acceptable level (you will not be able to eliminate it altogether).

At the end of Step Three you will have a security plan. Before going on to that, remember these important factors about plans:

50 One person needs to have overall charge of planning, and he or she must have appropriate authority to get the co-operation of colleagues and if need be to recommend expenditure on protective measures.

51 Effective plans are simple, lucid and flexible – but flexibility does not mean that they can be open to interpretation when an incident is taking place, or can offer a range of options to follow, as this will simply confuse staff in the heat of an incident. Everyone must be clear what they are to do given a particular circumstance, as during an attack there is an inherent danger in trying to change plan.



52 Once they are made:

- plans must be followed; but
- they must be kept under review to reflect changes in buildings and personnel; and
- they should be checked regularly to make sure they remain accurate and workable – and there should be regular exercises.

Carrying Out Step One

53 This is the threat assessment checklist:

- What does the news tell us about the current national and international climate, or current terrorist campaigns?
- What can the local police tell you about the chance of a terrorist attack in your neighbourhood?
- Is there something about your building or your staff that would attract a terrorist attack: are you seen as having a special relationship with a high profile individual who is a terrorist target in his or her own right; has your company name been associated with animal experimentation?
- Does your location mean that you may suffer collateral damage from an attack on a high-risk neighbour?

Carrying Out Step Two

54 You know already what it is really important to you and your business. It may be something tangible and obvious: the data suite where all your transactions are recorded, or the one piece of equipment that keeps your whole plant running. It may also be less obvious – continued free access for the public, for example. You will have plans to safeguard some or all of these things from other threats already – for example, you will have defences against, and plans in anticipation of, fire, and defences against criminals who may want to steal your stock.

55 In the terrorist context you need to consider the research that may be carried out by the potential attacker to discover your main vulnerabilities or your prestige targets and to identify how each of these can best be protected.

Carrying Out Step Three

56 Step Three brings together the answers to Steps One and Two, and looks at what measures it is sensible to put in place to reduce the risk of damage.

Part 8 looks at five possible forms of attack and describes the sort of thing that the security plan should cover in each case.



Five Plans for Five Possibilities Part 8

Plan One: The Delivered Bomb

57 Most organisations receive huge amounts of mail, whether through the Post Office or other delivery and courier firms. This is an attractive route into your building or into your hands. It is a targeted attack. The aim is to kill or maim or disrupt, not to cause structural damage or mass casualties. The nature of your business and the current focus of terrorism or “activism” will give you, in consultation with the local police, a reasonable picture of how likely this form of attack is, and this will dictate just how far you want to go in your planning.

Preparing for the Possibility

58 Planning for the delivery of an explosive or incendiary device is based on two simple features:

- it will already have undergone some fairly rough handling, by the Post Office or by its courier.
- uncertainty over exact delivery times, and the weight and complexity of reliable timing devices, makes it very unlikely that the device will be triggered by a timer.

Handling delivered mail is therefore not generally dangerous in itself.

Recognising a Suspicious Item

59 The police Crime Prevention Department can give guidance on the features that may identify the typical letter or parcel bomb. And staff who handle mail can be helped to pick out potentially “suspicious” items by building good housekeeping measures into usual business routines:

- let staff know what is the usual pattern of deliveries and the types of item, and forewarn when unusual deliveries are expected; and
- encourage good practice in those you deal with regularly by having a clearly identifiable sender shown on each item.

Make sure that you have identified and briefed all staff who handle delivered items (think of Reception as well as the Mail Room).

60 If the risk and scale of the problem for you is sufficiently great you may want to invest in

commercially available X-ray or other equipment. The Crime Prevention Department can advise. This equipment is only as good as its operators and you will need a regular programme of training and checking to see that procedures are being followed.

Dealing with the Event

61 If you have detected a suspicious item:

- leave it alone (do not play with it to investigate it further, do not put it in a bucket of water or put something on top of it or throw it out of the window....);
- clear and secure the immediate area making sure the police will still have unhindered access to the suspicious item; and
- call the police.

Plan Two: Incendiary Devices

62 Incendiary devices are traditionally the weapon of choice against the retail sector, and occasionally against certain industries or public buildings. They may form part of a targeted attack (because of who the company is or what it sells) or the placing may be relatively random (if the aim is to damage a town centre or shopping mall itself). The purpose is to cause economic damage (directly and via publicity), not casualties.

Preparing for the Possibility

63 Planning against the possibility that an incendiary attack will be mounted against you is based on some basic assumptions:

- the device will be concealed for ignition when the premises are empty;
- as damage is the objective, having more than one potential seat of fire is attractive to the attackers;
- anything that triggers a sprinkler system will, because of the damage ensuing, be a good result even if total destruction is not achieved; and
- incendiary devices do not explode, they ignite.