Beyond Lawful Protest:

Protecting Against Domestic Extremism

ACPOS
ASSOCIATION OF CHIEF POLICE OFFICERS IN SCOTLAND

produced by

NaCTSO
National Counter Terrorism Security Office

Contents

Preface

This is an updated edition of the publication originally called ***Extremism - Protecting People and Property,*** published by the Home Office in 2001. The text incorporates the best and most up-to-date advice from experts in Government and the Police Service.

Beyond Lawful Protest: Protecting Against Domestic Extremism has been written specifically with managers in mind. The advice that it contains is relevant to all businesses and organisations whether large or small, and to local government.

Domestic extremism has been a particular anxiety to many companies and organisations because of a tendency by a small number of activists to target people or groups, their homes and their business premises. This has involved harassment and intimidation of various types, including 'hate' campaigns which can be disturbing and distressing. On occasion specific threats have been made.

The majority of protest activity in the UK is both lawful and peaceful and is carried out by law abiding citizens who wish to exercise their freedoms to assemble and to express themselves; these freedoms are an important part of our democracy and are protected within the Human Rights Act 1998. Unfortunately there are a small number of people who are prepared to break the law in the belief that it will further their 'cause'. It is this unlawful activity which is beyond lawful protest that we refer to as domestic extremism.

Nothing in this handbook is intended to prevent or stifle lawful and peaceful protest; the police have a key role in helping to facilitate such a protest. At the same time however, the police have a duty to prevent crime and disorder and this booklet is intended to help companies and organisations to also enjoy their rights and freedoms to conduct lawful business free from crime or excessive disruption.

It is important to stress that good progress has been made over recent years in tackling domestic extremism. Even though such incidents are rare, it is wise for businesses to take sensible measures. The purpose of this handbook is to help people feel that there are things which can be done to reduce the impact of any such activities on their professional and private lives. Any action taken must be balanced and proportional.

As part of its aim to be a comprehensive guide to managers, many potential threats are covered. These are provided as examples where lessons have been learned in the past. Such incidents can help to prepare for the future, but remember, these incidents are rare. **Your preparedness for such incidents will help you deal with such unlikely events.**

Managers are asked to think about the advice given in the section 'How to use this handbook' rather than make this document widely available as a sole source of guidance to staff. The handbook is not for wider distribution and should be kept securely.

NaCTSO

Who we are, what we do and how we do it.

The National Counter Terrorism Security Office (NaCTSO) is a police unit co-located with the Centre for the Protection of the National Infrastructure (CPNI). We are funded by and report to the Association of Chief Police Officers.

NaCTSO contributes to the UK government's counter terrorism strategy (CONTEST) by supporting the Protect and Prepare strands of that strategy.

Our staff can offer specialist advice regarding the security of explosives and pre-cursor chemicals (including fertilisers), pathogens and toxins, radiological sources and other toxic chemicals.

We also provide guidance in relation to business continuity, designing out vehicle borne terrorism, the protection of crowded places and reducing opportunities for terrorism through environmental design.

To achieve national delivery on behalf of the Association of Chief Police Officers (ACPO) NaCTSO trains, tasks and coordinates a nationwide network of centrally funded, specialist police advisers known as Counter Terrorism Security Advisers (CTSAs). The primary role of these advisers is to provide help, advice and guidance on all aspects of counter terrorism protective security across a variety of sectors.

How to use the handbook

This handbook reviews the potential threats from extremist activities, how to tackle security planning and what measures to consider in particular circumstances. Its aim is to give people confidence so that they can pursue their professional and private lives with the minimum amount of disruption. Working in an atmosphere of continuing concern is damaging to the confidence and morale of staff. Leadership from the top of an organisation can help to prevent such problems.

We recommend that security managers and senior management select material from this handbook for incorporation in company and/or trade body literature. **Please note that this handbook** quotes many internet sources that will be updated hereafter, whereas this handbook will become outdated.

Main Messages

- Assess the likelihood of extremist activity directed at your organisation and/or employees. Plan your security measures accordingly.
- Choose the mix of protective security measures that best suits your premises and that will deter, detect or delay extremist activity.
- Prepare your staff for the possibility of extremist activity, without alarming them.
- Encourage your staff to protect themselves, your customers and visitors; through vigilance and good housekeeping.
- Test your plans regularly and evaluate the response. If possible, do this with local emergency services.

Plan for:

- Demonstrations
- Intrusions
- Intimidation
- Suspicious Mail

More specific advice can be obtained from your local police Counter Terrorism Security Adviser or Crime Prevention Department. The advice is free and impartial. Also, use the contact list at the back of this document for suitable contact points and websites. Your local Crime Prevention Department will be able to deliver good basic advice on what to do or how to prepare for such incidents. The Counter Terrorism Security Adviser has specific training on such issues and will deliver security advice based on the risks posed.

Part One: Introduction

The United Kingdom has seen a number of incidents that have been committed by a broad range of individuals or groups. This includes anti globalisation, environmental, anti animal experimentation and groups opposed to road transportation. Protests have been conducted in many different ways but include picketing, occupying business premises, the harassment of secondary or tertiary contractors and, on very rare occasions, the use of violence.

Remember, it is important to keep the threat in perspective. Most protests are peaceful and undertaken in accordance with the law. They are conducted by reasonable people who are content to make their point and then leave. Extremist activity is more rare.

The extremist side of such protests tends to go beyond lawful protest. Some examples in recent years have shown us that what has started as a peaceful protest or campaign, can develop in more serious ways. For example, while most letters sent to a company objecting about something remain just that, some may start off polite, but become more threatening and abusive as time goes on. Similarly, most peaceful demonstrations remain peaceful, but can be infiltrated by more extremist elements who will endeavour to stir things up with the intention of provoking confrontation.

Sometimes it is just not possible to anticipate how a protest campaign will develop. Managers are therefore advised to treat all such incidents as potentially suspicious from the start. Evidence, such as letters or records of times and places where groups have been seen should be preserved. The police should be made aware.

This handbook is designed to help you plan for such incidents so that, rare as they are, you are prepared and know what to do, which will result in minimising the impact on your business and way of life. If the nature of your business means that there is a greater likelihood of the business or staff members being targeted, you should make your plans in conjunction with the local police.

The National Extremism Tactical Coordination Unit (NETCU) is a national police unit tasked with providing tactical advice and guidance on policing single-issue domestic extremism. The unit also supports companies and other organisations that are the targets of domestic extremism campaigns. NETCU is a valuable source of information and advice. Their website is constantly updated at www.netcu.org.uk.

Advice in this handbook is for a large and diverse audience. It is generic rather than site specific. The guidance is, however, sufficiently detailed to allow managers to adapt it to the circumstances of their organisation. You need to:

- Assess the threat from extremist activity.
- Take precautions against the threat of extremist activity.
- Respond effectively to incidents of extremist activity.

REMEMBER: Extremists are seeking to get their way through intimidation. They do this by generating smear campaigns, threatening violence and damage, and in extreme circumstances may actually carrying out such threats against individuals and organisations. By adopting the measures suggested in this handbook, managers can help reduce the chances of a successful attack.

REDACTED

REDACTED

Part Three: Why Plan at All?

The activities of extremist campaigners or malicious hoaxers are designed to damage the reputation of an organisation, intimidate, disrupt, cause economic damage and – in very rare circumstances – cause injury. There are good business reasons for planning to avoid all of these possibilities – or at least minimise their consequences.

There are also obligations placed upon everyone (employer and employee alike) to play their part in protecting themselves and others. In a counter-extremism 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.

Management of Health and Safety at Work Regulations 1999

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.
- 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 any steps to be taken.
- In the case of serious imminent danger, work must be stopped and people 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 may be the subject of scrutiny in any subsequent enquiry or court proceedings.

What should be done?

Action should be on the following lines:

- Think about the threats you may face.
- Take the best available advice on the steps you can take to reduce the chances of any harm being caused to staff or visitors.
- Make a contingency plan and ensure that all staff are familiar with it – **and practice it**.

The material in this handbook will help you take all these steps, and provide some simple measures that will considerably reduce your vulnerability to extremist activity. Further advice is available through your local police crime prevention department.

REDACTED

REDACTED

Part Five: Security Planning

Appointing a Domestic Extremism Co-ordinator (DECO)

The successful response to an actual or potential extremist attack depends on the creation of a company security policy and the appointment of a DECO. This person must have full oversight of and authority for the totality of the counter extremism security planning process.

A DECO 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 DECO must be involved in the planning and design of the buildings exterior security, access control and so on, so that the extremist dimension is taken into account.

The DECO should establish liaison with the local police as a source of expert knowledge. This may be the local Crime Prevention Officer, police Crime Prevention Design Adviser (sometimes called the Architectural Liaison Officer) or the police Counter Terrorism Security Adviser. For the purpose of this document, they will be referred to as your local police expert.

On a national level, your attention is drawn to the police National Extremism Tactical Co-ordination Unit (NETCU). This unit was established in response to extremism activity in the UK. NETCU collate information and distribute salient points to those businesses that could be affected by such activity. They have a plethora of advice and information regarding extremism in the UK. Their contact details are:

PO Box 525
Huntingdon
PE29 9AL
Tel: 01480 425091
Fax: 01480 425007
e-mail: mailbox@netcu.pnn.police.uk
Web: www.netcu.org.uk

During the development of plans, it is advisable to consult with all the emergency services. For example, under the prevention of terrorism legislation, police 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.

The DECO has six main responsibilities:

- Production of a risk assessment, and the consequent control measures.
- Devising and maintaining the appropriate contingency plans.
- Deciding on the action to be taken appropriate to the nature of the incident.
- Deciding on when to re-occupy a building if evacuation has occurred.
- Liaising with the police and other emergency services.
- Arranging staff training, communication cascades and drills, including training for his or her deputy.

The DECO's end product should be a plan or set of plans that have been checked with the police and practised. Such plans must be 'living' documents that are regularly reviewed and

updated to ensure they are current and valid. A number of industries have security forums, who should be consulted where relevant. There maybe plans already in existence that could be adapted.

Creating Security Plans

There are three crucial steps in drawing up counter-extremism plans. You should identify what sort of threats you are facing and the realistic possibility of an incident occurring. These are:

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 most common categories), and how they may be vulnerable to extremists.

Step Three

- Identify the most appropriate measures to reduce the risk to an acceptable level.

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

- One person must be in overall charge of planning and they must have the appropriate authority to get the co-operation of colleagues. They should also have the authority to permit expenditure of protective security measures.
- 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 during an incident. Everyone must be clear what he or she is to do given a particular set of circumstances. Avoid changing plans during an incident.

Once they are made, plans must be:

- Followed.
- Kept under review to reflect any changes.
- Checked regularly to make sure they remain accurate and workable – and there should be regular exercises.

Carrying out Step One

There are four important considerations when drawing up Step One:

- What does the news tell us about the current national and international climate of extremist activity?
- What can the local police tell you about the chance of extremist activity occurring in your neighbourhood?
- What is there about you organisation or company that would attract extremist attention?
- Are you seen as having a special relationship with another organisation, company or individual that could be the target of extremists?
- Are any of the outside elements critical to the running of your organisation or company likely to be targeted?
- Are you the neighbour of a company or organisation that maybe targeted? Could your business be affected by collateral damage or disruption from protests?

Carrying out Step Two

Assess what is really important to you and your business. It may be something tangible and obvious such as a data suite or power plant. It could be less obvious, such as ready access to the public. You should already have plans to safeguard some, or all, of these features from other risks such as accidental fire or theft. Use these as a basis when considering the extremist threat.

In the extremist context you need to consider the research that may be carried out by the potential attacker to discover your main vulnerabilities. Remember, your vulnerabilities may be away from your home site, as well as on it.

Carrying out Step Three

Having considered Step One and Two, you will now be able to establish the level of risk you are at. You must now take steps to reduce that level of risk as much as possible. Part 10 of this document looks at six possible forms of extremist activity. Your security plan should cover all of these eventualities.

Part Six: Asset Protection

The first line of defence against common criminal behaviour may also be that which will deter extremists from gaining access to your premises. Your priorities must be to Protect:

- The safety of all personnel on your site.
- The contents of your building(s).
- The business operation.

Deter, Detect and Delay

Regularly review existing security measures, for example CCTV, access control and perimeter protection. Remember that security systems will only be effective if they are used and maintained correctly. All staff share responsibility for the security of the site and the safety of their colleagues.

Your local police can provide you with expert advice on physical security measures. This advice is free and impartial. You must also consult with the local fire officer to ensure that fire regulations are being complied with. Consideration should also be given to liaising with your Local Authority, to ensure any new measures do not breach planning laws.

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. A very effective way of achieving this is by the use of an 'Operational Requirement'. This process will ensure you get what you want with a performance criteria identified with which to measure your system against. Consult with your local police expert regarding this.

The following is a guide on methods that you can use to achieve the three D's. The objective is to deter extremists from your site by good security measures and alertness. Failing that, you want to be able to detect anyone who has unlawfully gained access (this could be by force or by stealth such as getting employment). Finally, you must delay anyone from causing your business or organisation any harm (see Part 9 on Personnel Security).

Information Security

Depending on the size and nature of your organisation, information security could be a major consideration. Extremists have successfully attacked and disrupted IT systems in the past. If your organisation does not have the appropriate IT management resources to deal with this issue, consider seeking specialist advice via your trade association or Chamber of Commerce.

Infiltration/Social Engineering

These are two potentially highly successful ways of obtaining access to your company or organisation. You must carry out pre-employment screening. You may wish to employ a company to do this on your behalf. Once new staff have commenced work, consider carefully where they should work during the first 6 months. Do you have to allow them access to vulnerable or controversial parts of your site? Please follow the guidance in Part 9 as closely as possible if you have assessed yourself as being at a high risk.

Physical Security Standards

The following information will assist you with regards to the types of physical security measures that you can use, or improve, to increase the protection of your site. Many such measures have been tested by the Loss Prevention Certification Board or the British Standards Institute. Some elements have been tested and approved by the Association of Chief Police Officers (ACPO) and the Association of Chief Police Officers in Scotland (ACPOS) Crime Prevention Initiative and badged as 'Secured by Design'. Your local police contact can advise you on the most suitable measures to use. You must be aware that some security products are untested and may not be as effective as the manufacturer's claims.

Perimeter Fences

If you have a perimeter fence, how regularly do you check it? Is it well maintained and would it keep even an opportunist out? Has the local wildlife burrowed under it? Have local residents damaged it to use a short cut? Chain Link fences are not considered to be a security measure. A more robust option would be palisade fencing or a welded mesh fence.

Doors

All external doors should be strong and robust with door fixings that are commensurate to the strength of the door itself. The glazing on such doors should be kept to a minimum or be appropriatly robust glazing installed. Doors must also be fitted into robust walls. There is little point in having a very strong door with excellent locks which is attached to a plaster board wall.

Walls

As with external doors, external walls must be strong and robust. If they are not, there are cost effective measures that can be taken to improve this.

Windows

As with the above, ground floor windows and any that could be accessed easily from, say, a flat roof must be strong and be able to at least delay a possible attack. Laminated glass fitted correctly into a robust frame with good locks is recommended, but you could also consider shutters, grilles or bars.

Intruder Alarms

Advice from the police should be sought regarding this. There are many different types of alarms for many different scenarios. The police will advise you on what is most appropriate for your site.

CCTV

Closed Circuit Television (CCTV) can make an important contribution towards your security regime. Again you should seek the advice of the police as to what is appropriate for your site and what role your CCTV system should play in your security regime. There are also laws regarding the use of CCTV that you must comply with.

Lighting

Good lighting can be a deterrent in its own right. It is also essential to get the lighting right, otherwise it could have an adverse effect on a CCTV system. Seek further advice regarding lighting. It is important for it to be effective whilst at the same time avoiding other issues such as light pollution.

Access Control

The control of access should be considered through the entirety of your site. This starts with the access on to your actual site, whether by car or foot and continues through access issues into buildings, a part of building, a particular room or even something contained within a room. There are many aspects to consider and the local police expert will be able to advise you. Here are a few basic points which you must consider:

- Access to everything on your site should be restricted to those who need it. For example, everyone will need access to a canteen, but few will need to go into the kitchen. Should an administrator be granted access to an area where machinery operates? Establish who needs access to what – then control it.
- If you have grounds around your building, you should endeavour to maintain a secure boundary with the least number of entry and exit points as possible. (See perimeter fences above) In most circumstances it is best to have a person report to a security gatehouse as soon as they arrive at the site.
- If a person can walk straight off the street into your building, or your building is shared by other companies, you should clearly mark where the reception point is and ensure all persons have to pass through that point.
- The best form of access control into and within buildings can be delivered by way of a swipe card or proximity card reader. This is even better if supported by a key pad and PIN (Personal Identification Number). Cards should contain a photo of the person to who it belongs, a reference number (no name) and a PO Box postal address for the cards return should it be lost.
- All staff must wear their security cards at all times and be encouraged to challenge any person without an appropriate card/badge.
- Issues relating to access control can be complicated with many variables involved. Seek advice from your local police adviser over this matter.
- Visitors should be logged in as soon as they arrive on site and on leaving the site. See Part 9 for further advice on this and other personnel access issues.

Good Housekeeping

Good housekeeping both inside and outside your premises will reduce the opportunity for unlawful extremist activity. The following are some useful points regarding this:

- Consider what information is given over the phone by staff – it could be used against the company or individuals. Staff should identify who the caller is and request their contact details should they be cut off. If your staff are still unsure, they should ask for a contact number and tell the person that they will be called back. This will allow time for some basic checks to establish if the call is genuine or not.
- Consider having a 'clear desk' policy, whereby all material and documentation that could be useful to someone outside the company is locked away by staff at the end of the working day.
- Ensure that any unwanted documentation relating to your business or organisation is discarded in a sensible way. Shredding documentation is a good method for final disposal.

1. This advice supersedes the advice given in 'Protecting Against Terrorism' 2nd Edition

- Staff should be charged with ensuring that their workspace is locked and secured at the end of the day and at weekends, if appropriate.
- Computers and monitors should be turned off when not in use. PC's should be password protected where possible. Even if staff are away from their PC for a short period of time, the computer should be programmed to lock automatically to prevent unauthorised access.
- If an office or a room contains sensitive material or practices, they should be kept locked and secure at all times when unattended. A person should be delegated responsible for ensuring such areas are secured at the end of each day, if appropriate.
- Vigilance must be maintained in car parking areas. Staff should be reminded not to leave belongings in their car, especially anything which may identify the staff member or where they live. All staff must report any suspicious activity to the DECO or security manager: for example, a person writing down car number plates.
- Any suspicious activity should be reported to security staff and recorded in an incident log book. Such log entries should be reported to the police if they become regular. An increase in log activity may pre-empt a protest or other extremist activity. This incident log book should be kept in one place and all staff made aware of where it is and who is responsible for it.
- Seek mutual support from neighbouring companies to develop an early warning system to help identify potential activists or suspicious persons in the area of your premises.
- Consider putting simple plastic seals on maintenance hatches that are rarely used.
- All communal areas such as stairs, hallways and corridors must be kept clear of items so that anything suspicious will stand out.
- Regularly check the outside of buildings for any sign of attempted entry. Also maintain good house keeping around the outside. Any large stones or bricks that could be used as missiles should be removed. Wooden pallets or such like items that can assist someone to climb should be removed. These problems are more likely to occur if you have building work ongoing at your site.
- Consider any external furniture you may have. How necessary is it? Could something be hidden under a bench? Are you giving an unknown person and excuse to loiter? Are litter bins really necessary? Most of these features provide good hiding places. If you can remove them and consider other options such as a robust cleaning regime.
- Ensure all your exterior planting is well maintained. Trees must not obscure lighting or CCTV cameras. Shrubs should be kept low so that lines of sight are maintained and you are not providing a hiding place.
- Many companies now have designated smoking areas outside the building. These areas are best placed away from entrances and fire exits.

Multiple Occupancy

In multi-occupancy buildings, shopping centres, high streets, business parks and the like, it is essential to make all forms of security a joint communal effort. For example, common access control procedures can be agreed or CCTV cameras can be situated for maximum overall benefit. Effectiveness will be increased and costs reduced for all parties.

Part Seven: Delivered Items

Delivered items[1], which include letters, parcels, packages and anything delivered by post or courier, have been used by extremists on occasions. These events have usually attracted a significant amount of publicity, which may make them appear as if they are a common event. A properly conducted risk assessment should give you a good idea of the likely threat to your organisation and indicate the level of precautions you should consider.

Delivered items may be explosive or incendiary (the two most likely kinds), or conceivably chemical, biological or radiological (CBR). Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality. A delivered item will probably have received fairly rough handling in the post and so is unlikely to detonate because it is moved.

However, any attempt to open such an item may well set it off. Unless delivered by a courier, it is unlikely to contain a timing device. Delivered items come in a wide variety of shapes and sizes; a well made device will look innocuous but may still have tell tale signs.

Indicators of a suspicious delivered item:

- Unexpected item, especially if hand delivered.
- A padded envelope ('Jiffy Bag') or other bulky package.
- An additional inner envelope or other contents that may be difficult to remove.
- Labelling or excessive sealing that encourages opening at a particular end or in a particular way.
- Oddly shaped or lopsided.
- Envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges).
- Marked 'To be only opened by', 'personal' or 'confidential'.
- Item addressed to the organisation or a title/post (rather than an individual).
- Item addressed to a high profile individual.
- Unexpected or unusual origin (postmark and/or return address).
- No return address or a return address that cannot be verified.
- Poorly or inaccurately addressed.
- Address printed unevenly or unusually.
- Unfamiliar writing or style.
- Unusual postmarks.
- More stamps than needed for size/weight of package.
- Unusual smell.
- Greasy or oily stains emanating from within.

Additional explosive or incendiary indicators:

- Unusually heavy or uneven weight distribution
- Small hole(s) in envelope or wrapping

Additional CBR indicators:

- Powders liquids or odours emanating from package
- Wrapping stained by liquid leakage
- Unexpected items or materials found in package during x-ray or at first opening (loose or in a container): powdered, crystalline or granular solids; liquids; sticky substances or residues
- Unexpected odours observed on opening
- Sudden onset of illness or irritation of skin, eyes or nose

Action upon discovery of any suspicious delivered item:

This may occur in a designated post room or anywhere else in a building. Ensure that you have appropriate emergency response plans in place

- Avoid unnecessary handling
- Put it down on a cleared flat surface
- Keep it separate so that it is easily identifiable
- If it is in an x-ray facility, leave it there
- Move away immediately
- Clear immediate area and each adjacent room, including rooms above and below
- ***If there is any suggestion of CBR materials, move those directly affected to a safe location close to the incident – keep these individuals separate from those not involved***
- Prevent others approaching or accessing cleared areas
- Do not use mobile phones or two way radios in the cleared area or within 15 metres of the suspect package
- Communicate regularly with staff, visitors and the public
- Notify police – ensure that informant/witness remains available to brief police

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED