



THAMES VALLEY
PROJECT
GRIFFIN

GUIDE

Confidential Anti-Terrorist Hotline **0800 789 321**

Introduction



In the interests of the safety of staff and customers, companies have to guard against a variety of potential threats. These can include attacks by terrorists, radical political organisations, or even disgruntled customers.

While incidents are far from commonplace, constant vigilance is necessary. It is vital that everyone is aware of the procedures that are in place to deal with threats to staff, buildings or customers.

The threat presented in the United Kingdom has seen groups resort to terrorist activity to publicise and progress their political objectives.

Some are concerned with domestic issues; others operate on the international stage. Some seek to target particular organisations or individuals; others are more indiscriminate.

Keeping the threat of terrorist incidents in perspective, it is important to establish that terrorist incidents in the United Kingdom are rare, but when they occur they attract both national and international interest. For most of the population within the United Kingdom, terrorist related crime will remain something that is heard about on the news.

Others however may find themselves involved in the scene of a terrorist crime or the events leading up to a suspected terrorist incident. This involvement might include observing suspicious activity, dealing with a suspect package on business premises, receiving a telephone call stating that a bomb has been left at a location or being involved in the safe evacuation of large amounts of people to an area that is designated as safe.

Alternatively some of the population may be involved in the aftermath of a terrorist attack and require assistance and support.

This Project Griffin Guide, has been designed by Thames Valley Police in partnership with specialist staff whose responsibility includes the content contained within.

This manual gives guidance to all staff, but in particular, to those who have a regular involvement in the effective operation of businesses within Thames Valley.

The intention of the 'Project Griffin Awareness Day' supported by The Project Griffin Guide is to help reduce vulnerability to the threat from terrorism. As Project Griffin is designed to address the wider audience, the advice contained within is general, rather than specific. It has been written with a wide audience in mind; it therefore does not and cannot, deal with the specific needs and particular circumstances of individuals within an organisation.

The material enclosed within this manual will provide the reader with the additional information needed to achieve the Project Griffin objectives.



1. Thames Valley Police & Griffin

Section 1.2: THAMES VALLEY POLICE AND THE HOME OFFICE COUNTER TERRORIST STRATEGY



- The main focal point of this project and the introduction within Thames Valley Police is clear. It is to increase the awareness of staff who are already a visible deterrent and whose role is likely to be significant in the initial stages of either identifying a suspicious package or after a terrorist incident has occurred.
- Developing and delivering the Government's counter-terrorism strategy involves stakeholders from across government departments, the emergency services, voluntary organisations, the business sector and partners from across the world.

What is the strategy based on?

Since early 2003, the United Kingdom has had a long-term strategy for

countering international terrorism (known as CONTEST). Its aim is to reduce the risk from international terrorism, so that people can go about their daily lives freely and with confidence.

The strategy is divided into four principal strands: Prevent, Pursue, Protect and Prepare.

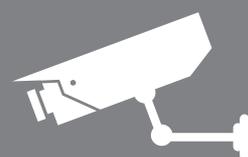
Prevent

The Prevent strand is concerned with tackling the radicalisation of individuals, both in the UK and elsewhere, which sustains the international terrorist threat. The Government seeks to do this by:

- Tackling disadvantage and supporting reform by addressing structural problems in the UK and overseas that may contribute to radicalisation, such as inequalities and discrimination

(continued overleaf)





2. Hostile Reconnaissance

Section 2.1: GUIDANCE

2.1 BACKGROUND

Previous experience has shown that prior to a terrorist attack, some form of covert reconnaissance will be undertaken. This may be in the form of cars or other vehicles in the vicinity or persons photographing, recording and documenting locations.

It is the responsibility of all of us to help ensure that Thames Valley remains an environment where any such actions will be recognised and dealt with quickly and effectively.

All members of staff should be encouraged to report any suspicious incidents at any time of the day or night.

This section provides examples of activity that might be regarded as 'suspicious'.

One or two isolated incidents on their own, might not be considered to be 'suspicious', but when repeated or put together with similar incidents, such activity should be reported for appropriate assessment to:

THAMES VALLEY POLICE IN THE FIRST INSTANCE

0845 8 505 505

Use this number to report a non emergency crime or to give information to Thames Valley Police.

(continued overleaf)





2. Hostile Reconnaissance

Section 2.2: WHAT TO LOOK OUT FOR

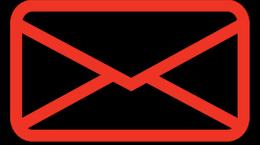
- Slow vehicle movement driving past buildings
- Observation of security reaction drills or procedures
- Foot surveillance involving two or three individuals working together
- Prolonged static surveillance using operatives disguised as food or flower vendors, news agents or street sweepers not previously seen in the area
- Activity inconsistent with the nature of the location
- People asking probing and inappropriate questions about security measures
- Unusual movement and activity by contractor's vehicles
- The same or similar individuals returning to carry out the same activity, whether in a vehicle or on foot.

THIS LIST IS BY NO MEANS EXHAUSTIVE, ANY ACTIVITY WHICH YOU CONSIDER MAY BE PUTTING YOUR COMPANY OR STAFF AT RISK OF ATTACK, SHOULD BE CONSIDERED AND ACTED UPON.



3. Mail Room Security

Section 3.6: FUNCTIONING OF BOMBS



An explosive device contained in a letter or parcel received through official post office channels normally functions in one of the following ways:

- On opening of the letter or parcel
 - On withdrawal of string or tape at any stage
 - On removal of the contents
 - On piercing of the wrapping
 - On opening of the contents – often a book is used for this purpose
 - On operating the enclosed item (often an electrical gift)
 - On opening a greetings card (e.g. those that might play an audible message).
- If delivered by courier – check their credentials, then ring his / her company to check the origin of the package
 - If a commercial package, the company concerned should be contacted to check if the package is genuine
 - Contact the addressee to see if the package is expected.

A further method of functioning, which particularly applies to items that have been placed at premises or delivered by hand, is the operation of a time delay mechanism, (i.e. without the letter or parcel being opened or distributed).

Actions

To provide further confirmation:

IF THE ITEM IS STILL SUSPICIOUS – DO NOT PANIC

- The package has made it this far through the mail. There is no reason that it should function if it is not opened further
- Evacuate the room and direct personnel to proceed to a pre-determined point, which is away from windows and out of line of sight. Nominate an individual to check all personnel are present



(continued overleaf)



4. Chemical/ Biological

Section 4.2: ROLES AND RESPONSIBILITIES

Section 4.3: CONTINGENCY PLANS

● The role of security and response

Specific actions:

- Receive the first telephone call from staff
- To be the first reassuring point of contact
- To offer initial advice in accordance with the following guidelines:

Take details of call including:

- Name of caller and position in company
- Building location of incident and address
- Department(s) affected
- Number of staff in direct contact with substance / and in direct proximity
- Telephone number (including mobile) of contact point
- Advise that the line be kept clear for further communication

- Obtain sufficient brief details of incident for passing to the police

- Inform the caller that a security manager will be in contact shortly

- Senior management may consider more immediate action e.g., evacuation, ensuring safe working practice is implemented.

4.3 CONTINGENCY PLANS

Business site managers should prepare contingency plans to minimise the effects of a chemical or biological attack. These business plans should be checked on a regular basis.

Each location/site is different, therefore local procedures may vary depending on the internal design of each location.

There needs to be an area designated for those members of staff who have been contaminated and a separate area designated for those staff who have not been contaminated. Has your business identified these areas?



4. Chemical/ Biological



Section 4.7: INTERNAL – Instructions to the person who opened the package and other members of the mail room staff

Section 4.8: EXTERNAL – If a device is discovered or initiated externally

Section 4.9: EXTERNAL – If a device is deployed adjacent to the air intakes of the air conditioning system

4.7 INTERNAL – INSTRUCTIONS TO THE PERSON WHO OPENED THE PACKAGE AND OTHER MEMBERS OF THE MAIL ROOM STAFF

- After informing the designated emergency co-ordinator for the relevant business or his / her deputy, all persons in the mail room should wash their hands and face in hot soapy water, with a diluted bleach solution if possible
- The individual who opened the package and mail room staff should then be isolated in separate rooms to await instructions and be debriefed by the emergency services.

4.8 EXTERNAL – IF A DEVICE IS DISCOVERED OR INITIATED EXTERNALLY

- Advise the designated emergency co-ordinator

- Switch the air conditioning system off
- Close all fire doors
- Close all windows in the rest of the building
- Move all occupants located on the ground and below ground floors up the building to the first floor and above, on the opposite side of the building to the device to await instructions from the emergency services.

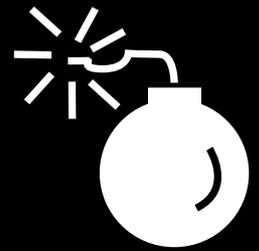
4.9 EXTERNAL – IF A DEVICE IS DEPLOYED ADJACENT TO THE AIR INTAKES OF THE AIR CONDITIONING SYSTEM

- Switch off the air conditioning system
- Preferably prevent unauthorised access to the air conditioning air intakes
- Physically secure the access routes, alarm and cover with CCTV for alarm verification.



5. Bombs

Section 5.1: DEVICES



5.1 DEVICES Improvised Explosive Devices (IED)

Terrorists usually use improvised explosive devices (IED) disguised to look like everyday objects. So, it is important to recognise any suspicious object that could be a bomb.

Remember:

- Be suspicious of objects that are out of place or unaccounted for
- Treat any suspect package with caution
- Be aware of any unusual stains on the package, e.g. grease, etc.

High Explosive Devices (HED)

- **A High Explosive Device typically consists of the following components:**

Explosive

Commercial explosive is a dense putty-like material that may be in blocks, lumps or sticks and often has a distinct almond or marzipan smell.

Home made explosives (HME) will usually be in the form of powder or granules and can be made from commercially available substances like fuel, oil, sugar or garden fertilisers.

Detonator

Usually a small copper or silver tube with coloured wires attached, capable of sending an electric shock to detonate the explosive.

In HME, the detonator can be any number of improvised devices.

Timer

Either a mechanical clockwork timer or electronic timer mounted on a printed circuit board. The timer acts as a switch to close the firing circuit at a predetermined time.

Power Source

Usually a battery powering both the timer and detonator.

Wiring

Wires of various colours linking the various components.

Container

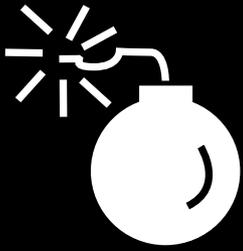
Used to transport and disguise the components, the container can take any form.

Incendiary Device

- An incendiary device is designed to burn fiercely, emitting intense heat and flame. It is often small enough to fit into an audio cassette case or video tape case. They are very lightweight and often difficult to detect by metal or x-ray detector.

(continued overleaf)





5. Bombs

Section 5.2: PRECAUTIONS

- Making the decision to evacuate the premises or move to internal safer areas if applicable
- Making the decision to re-occupy
- Liaison with the police in deciding this action
- The selection of staff for 'floor marshalls' and search teams
- The training of all staff in bomb threat procedures
- The arranging of training and rehearsals
- The regular amending and updating of all documentation.
- Be aware that certain terrorist organisations may provide a codeword, which must be recorded and immediately passed to the Police.

Telephone warnings

Terrorists often give telephone warnings. However, hoax callers often attempt to disrupt businesses and frighten staff with spurious bomb warnings.

In the event of a warning, the emergency co-ordinator or deputy will determine the response. The exception is when a warning comes from the police; then they will assume responsibility, while relying heavily upon staff for advice.

Whether the threat is considered credible or not, you must:

Responding To Incidents

Notification of a threat

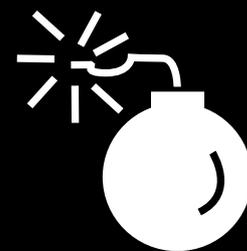
Notification of a bomb / attack can come from a number of sources:

- Police – who receive information of an explosive device planted in the vicinity
- Member of the public – who informs staff of a suspicious vehicle or item
- Staff member – who has received a suspicious item or found a suspicious vehicle or item
- Telephone message – from an individual, or switchboard (warnings are often sent to a third party, e.g. call centres, newspapers, etc)
- Telephone the Police: 999
- Telephone Security
- Give as much information as possible
- Consider carrying out a search
- Consider whether to evacuate the premises
- Provide any codeword given during the initial call.



5. Bombs

Section 5.6: SEARCH PROCEDURES AND METHODS Section 5.7: EVACUATION



It is vital that they know that they are searching for an unidentified object that:

- Should not be there
- Cannot be accounted for
- Is out of place.

As soon as the search has been completed or a suspicious object has been found, the emergency co-ordinator should be informed.

DO NOT TOUCH THE SUSPECT PACKAGE / DEVICE

A full description of the package will be required, but do not place staff at risk by remaining in the vicinity for an unnecessary period.

The emergency co-ordinator should keep in regular contact with the police and security. If nothing suspicious is found, the all clear should be given. Liaison with the police is essential in this decision making process.

5.7 EVACUATION

Evacuation Plans

The emergency co-ordinator should have up-to-date plans and drawings of evacuation routes, especially when there are a number of exits

and proposed evacuation routes. The plan is needed to:

- Evacuate the building or move staff into safer areas as quickly and efficiently as possible
- Provide alternative routes for evacuation so that people can leave the building or move to safer areas without being placed in danger by passing close to the suspect device.

External Safe Areas

Evacuation plans should advise staff to move a specific distance from the affected area and to move in a specific direction. Two alternative 'muster' points, at least 500 metres from the building, must be identified.

Reciprocal safe arrangements with other companies or other building should be made.

Be aware of the space the responding emergency services might require.

Internal Safe Areas

These are assembly areas within the building designed to afford staff the best protection should the external evacuation of the building be considered undesirable or impractical.

The designation and identification of an area within a building, as an internal safer area, **requires specialist advice** to be sought before being designated as such.



(continued overleaf)

FURTHER INFORMATION

Details of Caller

Man Woman Child Old/Young Not Known

Speech

Intoxicated Irrational Rambling Laughing
Speech Impediment Serious Accent

Distractions

Any noise on line? Coin operated phone box
Operator? Interruptions Anyone in background

Other Noise

Traffic Talking Typing Machinery
Aircraft Music Children Other

Name of person receiving call

Number of telephone on which call was received

Time Police informed

By whom

**NOW GIVE THIS SHEET TO YOUR LINE MANAGER.
BE AVAILABLE FOR AN INTERVIEW WITH THE POLICE**



In association with

