Counter Terrorism Protective Security Advice

for Hotels and Restaurants

produced by

NaCTSO

National Counter Terrorism Security Office

■foreword

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 CTSA network and monitor its effectiveness.

• Build and extend partnerships with communities, police and government stakeholders.

• Contribute to the development of CT policy and advice.

■ one introduction

This guide provides protective security advice to those who own, operate, manage or work in hotels and restaurants. It aids those who are seeking to reduce the risk of a terrorist attack and limit the damage an attack might cause. It highlights the vital part you can play in the UK counter terrorism strategy.

Terrorist attacks in the UK are a real and serious danger. The terrorist incidents in the Haymarket, London on Friday 29th June 2007 and at Glasgow Airport on Saturday 30th June 2007 indicate that terrorists continue to target crowded places; as they are usually locations with limited protective security measures and therefore afford the potential for mass fatalities and casualties. Furthermore, these incidents identify that terrorists are prepared to use vehicles as a method of delivery and will attack sites outside London.

Hotels and restaurants worldwide have been subject to terrorist attacks on several occasions. It is possible that your hotel or restaurant could be involved in a terrorist incident. This might include having to deal with a bomb threat or with suspect items left in or around your premises or sent through the post.

In the worst case scenario your staff and customers could be killed or injured, and your premises destroyed or damaged in a 'no warning', multiple and co-ordinated terrorist attack.

It is recognised that there is a need to maintain a friendly and welcoming atmosphere within the hotel and restaurant environments and this guide is not intended to create a 'fortress mentality'. There is however a balance to be achieved where those responsible for security are informed that there are robust protective security measures available to mitigate against the threat of terrorism, e.g. protection from flying glass and vehicle access controls into crowded areas, goods and service yards and underground car parks.

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. These have in the past been targeted at various premises in the UK.

Law, Liability and Insurance.

There are legal and commercial reasons why your premises should plan to deter such acts, or at least to minimise their impact. They are:

Criminal prosecution and heavy penalties under health and safety laws for companies and individuals who own or run hotels and restaurants are a real possibility in the wake of a terrorist incident, especially if it emerges that core industry standards and statutory duties have not been met. Particularly relevant to protective security in hotels and restaurants 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 the identified risks, even where they are not of your making and are outside your 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. **The commercial tensions which naturally arise between landlords and tenants, and between neighbouring organisations who may well be in direct competition with each other, must be left aside entirely when planning protective security.**

- **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.

Insurance against damage to your own commercial buildings from terrorist acts is generally available but typically at an additional 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 members of the public 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 uninsured pocket could set your business back several years.

Business continuity planning is essential in ensuring that your premises can cope with an incident or attack and return to **'business as usual'** as soon as possible. An attack on a crucial contractor or supplier can also impact on business continuity. This is particularly important for smaller operations that may not have the resources to withstand even a few days of financial loss.

Reputation and goodwill are valuable, but prone to serious and permanent damage if it turns out that you gave a less than robust, responsible and professional priority to best protecting people against attack. Being security minded and better prepared reassures your customers and staff that you are taking security issues seriously.

Do you know who your neighbours are and the nature of their business? Could an incident at their premises affect your operation? There is limited value in safeguarding your own business premises in isolation. Take into account your neighbours' plans and those of the emergency services.

A number of organisations have adopted good practice to enhance the protective security measures in and around their premises. This document identifies and complements such good practice measures.

This guide recognises that hotels and restaurants differ in many ways including size, location, layout and operation and that some of the advice included in this document may have already been introduced at some locations.

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

It is essential that all the work you undertake on protective security is conducted in partnership with the police, other authorities as appropriate, and your neighbours if your premises are to be secure.

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

Access control

Keep access points to a minimum and make sure the boundary between public and private areas of your operation is secure and clearly signed. Invest in good quality access control systems operated by magnetic swipe or contact proximity cards supported by PIN verification. See Access Control Guidance on page 21.

Security passes

If a staff pass system is in place, insist that staff wear their passes at all times and that their issuing is strictly controlled and regularly reviewed. Visitors to private areas should be escorted and should wear clearly marked temporary passes, which must be returned on leaving. Anyone not displaying security passes in private areas should either be challenged or reported immediately to security or management. Consider introducing a pass system if you do not have one already.

Screening and Patrolling

The screening of hand baggage is a significant deterrent that may be a suitable protective security consideration for your hotel or restaurant at certain times or leading to specific 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. Ideally, keep non-essential vehicles at least 30 metres from your building.

For site specific advice and guidance you should contact your local police CTSA. See also Vehicle Borne Improvised Explosive Devices on page 43.

Doors and windows

Good quality doors and windows are essential to ensure building security. External doors should be strong, well-lit and fitted with good quality locks. 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 to those hotels or restaurants that have an external search / screening operation 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.

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 co-ordinated 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 www.acpos.police.co.uk. 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 and maintained.

See CCTV guidance on page 23.

■ 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 hotel or restaurant 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 hotel or restaurant 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 CTSA.

- Utilising effective CCTV systems which 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.

■ 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 in hotels or restaurants 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	