Risk control

Martyn's Law

The Protect Duty: A Checklist

In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Martyn's Law
The Protect Duty: A Checklist

Introduction

The UK response to the threat of terrorism is contained in an integrated counter terrorism strategy called CONTEST[1]. The strategy's expressed ambition is to "reduce the risk to the UK and its interests overseas from terrorism, so that people can go about their lives freely and with confidence." The strategy is organised around four work streams, each comprising a number of key objectives:

- **Pursue**: to stop terrorist attacks
- **Prevent**: to stop people becoming terrorists or supporting terrorism
- **Protect**: to strengthen our protection against a terrorist attack
- **Prepare**: to mitigate the impact of a terrorist attack

It is also appropriate for organisations to prepare their own documented strategy detailing their own response.

Duty to Protect

The 'Protect Duty' will require eligible locations where qualifying activities take place to improve security measures to protect the public against terrorist attack. It aims to do so by implementing a duty which requires the owners or controllers of these locations to:

- Assess the risk of terror attacks at crowded public places
- Implement measures, so far as is reasonably practicable, to reduce the risk of terror attacks
- Have in place robust plans to respond to a terror attack

The fundamental responsibility and accountability will be the person or persons in control of the premises.

Terminology

There are a few terms used which are relevant:

- **Public spaces** are open public locations which usually have no clear boundaries or well-defined entrances / exit points (e.g. city centre squares, bridges or busy thoroughfares, parks, and beaches)
- **Public venues** are permanent buildings (e.g. entertainment and sports venues) or temporary event locations (such as outdoor festivals) where there is a defined boundary and open access to the public
- **Public accessible locations** are any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission

Public accessible locations may include a wide variety of everyday locations such as: sports stadiums; festivals and music venues; hotels; pubs; clubs; bars, casinos; high streets; retail stores; shopping centres and markets; schools and universities; medical centres and hospitals; places of worship; Government offices; job centres; transport hubs; parks; public squares and other open spaces. This list is not exhaustive.

An important principle of protective security is that it should, wherever possible, use simple and affordable interventions that protect and reassure the public, while deterring would-be attackers with minimal adverse impact on the operations, activities, or people's experiences.

A Tiered Approach

The legislation will introduce a tiered model that is linked to the type of activity that takes place at the eligible locations and the number of people (occupancy) that the location can accommodate at any time.

The requirements for each tier are:

- **Standard:** Persons responsible for a standard tier premises, i.e. qualifying premises where it is reasonable to expect that between 200 and 799 individuals may be present at the same time from time to time, will be required to:
  - Notify the regulator Security Industry Authority (SIA) of their premises
  - Have in place appropriate and reasonably practicable public protection procedures
- **Enhanced:** Persons responsible for an enhanced tier premises or event, i.e. qualifying premises or event where it is reasonable to expect that more than 800 individuals may be present at the same time, will be required to:
  - Notify the Security Industry Authority (SIA) that they are responsible for the premises or event
  - Have in place appropriate and reasonably practicable public protection procedures that could be expected to reduce the risk of physical harm being caused to individuals if an attack were to occur there or nearby
  - Have in place appropriate and reasonably practicable measures that could be expected to reduce both (i) the vulnerability of the premises or event to an act of terrorism occurring, and (ii) the risk of physical harm being caused to individuals if an attack were to occur there or nearby. For example, an enhanced duty premises will be required, as far as reasonably practicable, to implement measures relating to the monitoring of the premises and their immediate vicinity

— Document the public protection procedures and measures in place, or proposed to put in place, and provide this document to the Security Industry Authority (SIA).

To ensure that Martyn's law is agile and responsive, Governments will have the ability to adjust capacity thresholds in response to changes in the nature of the terrorist threat.

Eligible Locations

The Protect Duty will apply to eligible locations which are either:

— A building (including collections of buildings used for the same purposes, e.g. a campus); or

— A location / event (including a temporary event) that has a defined boundary, allowing capacity to be known

Eligible locations whose maximum occupancy meets the above specified thresholds will be then drawn into the relevant tier. This would include, for example, music festivals, and other outdoor events where there are known and controlled boundaries in place.

Risk Management Process

Organisations are likely to have already established risk management processes in place.

It is anticipated that risk assessments required by the duty should demonstrate:

— The range of threats that have been considered

— The steps that have been subsequently taken to mitigate these threats

— The steps that have been taken to prepare for and / or respond in the event of an attack

— Where steps have not been taken, the reasons why

Risk assessments will need to be reviewed by the duty holder at least once a year, and as and when circumstances or contextual factors change. For example:

— **External risk context** - A significant terrorist attack in the UK, a change in the Government's national terrorism threat level assessment, or a change to threat methodologies

— **Internal risk context** - Following an expansion of an organisation's premises and / or staff numbers, or a change in the business model, such as a restaurant starting to serve customers outside

Developing an evidence base to support these risk assessments ensures that organisations have the information to assist a formal inspection regime.

Supporting evidence might include:

— A summary of risks and actions considered and subsequently taken

— Completion certificates from appropriate staff training courses

— Evidence of physical security measures implemented, such as door locks, roller shutters and gates

— Evidence of attack response plans and their testing with staff

Vulnerability Risk Assessment

To prepare a vulnerability risk assessment organisations require up-to-date information on threats. Counter Terrorist Security Advisors (CTSA's) are individuals who work within local police forces as officers and staff. Their primary role is to provide help, advice, and guidance on all aspects of counter-terrorism protective security to industry sectors and others.

Support can also be provided by a local authority, access to the Counter Terrorism Business Information Exchange sub-sectors, and attending the ACT Corporate: National events.

Regular briefings by a dedicated CTSA enables them to release information from any counter terrorism investigation that identifies that an organisation is being targeted.

Organisations can then produce appropriate risk assessments based upon all available information. The risk assessment should cover all current threat spectrums. Although security measures may not be necessary for the least serious risks, it would be expected to include assessments for most attack types and justification for not implementing specific mitigations or CTSA recommendations.

This risk assessment should include a pre-written plan for mitigation actions and be understood by all key staff throughout the site.

Risk Treatment

The Protect UK website provides checklists[2] that organisations will find useful and offers suggestions on security risk treatments that can be deployed.

Active Security

— The nature of a location may make it possible to layer active measures

- As a public facing business that actively engages with customers or service users, the site could use deterrence messaging in communications
- At the access points, a search and screening process could be implemented, for example, using a modern, proportionate high footfall screening approach
- If there is an active control room with live CCTV feed, the opportunity for hostile behaviour detection can be achieved more efficiently than in other sites
- All the active measures require staff to deliver, which will require the development of a security culture and the implementation of measures (e.g. by employment screening) to minimise insider threat

Physical Security

- The site should have physical measures[3] and associated policies and processes in place to control access to the site by vehicles and pedestrians
- Where there are key assets, measures should be taken to minimise their vulnerability, typically through adding appropriate additional layers of security
- There should be measures to reduce the risk of using a vehicle as a weapon both within and on the approach to the site. This protection should include an appropriate mix of hostile vehicle mitigation[4], traffic control measures and deterrence

Response Plans

The main motivation for implementing the Protect strategy was the realisation that even after events like the Manchester Arena bombing in 2017 many organisations were still not prepared. An essential element of the duty will be ensuring response plans have been prepared and tested.

Engagement

Readiness testing encourages organisations to think about weaknesses. If a readiness exercise has not been undertaken before, it can be imagined as a slightly more 'live' risk management process that is undertaken nearer to an event (or annually for a venue). It sits between long-term risks and event checks to test processes, people, and equipment, and make sure organisations have what is needed to welcome visitors.

Collaboration

If organisations begin readiness planning a number of months before the big event or are in a perpetual planning cycle for a venue, there is time to be collaborative. Build out readiness programmes broadly across the organisation and in partnership with SAGs (Safety Advisory Groups) and local authorities. These different perspectives are essential, as there is reliance on these groups on event day, so it is essential that they are fully integrated into readiness plans.

Action

For readiness programmes to be effective, organisations must test, learn and act - it is no good doing only one or two of those things. A three-step plan to respond to terrorist incidents called Guide, Shelter and Communicate needs to be in place. Test that plan, learn from what went well and what did not, and act to make the plan function more effectively when it is tested again. Action should be taken to address any weaknesses.

Training

Readiness is a training exercise[5]. It is about testing anything that impacts on the management of a venue: processes, places, equipment, and people. Use the readiness testing as a training exercise for staff to conduct the processes that have been devised in that plan. Especially when introducing new policies, allow the staff who will be working on event day to get familiar with this work and build up experience.

Review Checklist

The following checklist can help organisations to identify potential weaknesses in arrangements:

Plans and Strategies

- Review vulnerability risk assessments based on the current threat level
- Review current Security and Business Continuity Plans
- Review Fire Risk Assessments to include Marauder Terrorist Attacks (MTA) and Fire as a Weapon (FAW) attacks
- Review employment screening to minimise the insider threat
- Have a Guide, Shelter and Communicate plan that responds to incidents
- Enhance security presence as identified by the risk assessment

Deterrence

- Review deterrence messaging to all that access your premises
- Remind staff to be extra vigilant
- Ensure staff positively engage with non-employees and report any suspicious activity to security or police
- Ensure Security officers are a visible presence with their ID badges clearly on display
- Provide high visibility clothing for patrolling staff

Security Arrangements

- Review the control of access points to premises
- Ensure CCTV is fully operational and that staff members are trained to operate it
- Remind staff how to deal with suspicious items
- Check that staff know the HOT principles, i.e. has the item been **H**idden, **O**bviously suspicious and is it **T**ypical for the location

Physical Measures

- Check that layers of security remain effective.
- Monitor vehicles parked close to buildings or inside perimeters
- Notice any abandoned vehicles or those occupied for extensive periods of time
- Challenge vehicles tailgating other vehicles at vehicle access control points
- Look out for Trojan vehicles made to look like legitimate vehicles
- Look for any altering or weakening of barriers or security systems
- Ensure arrangements are in place to escalate fire safety checks in the event of an increased threat level

Responding to a Situation

- Review the location and identification of emergency assembly points as they may be an easier target point than inside a building
- Review the emergency and evacuation procedures
- Ensure all necessary equipment, including first aid supplies, are readily available
- Review evacuation, invacuation, and lockdown procedures
- Ensure there are plans in place for vulnerable staff and visitors with designated marshals available to support
- Conduct readiness testing to train staff what to do in response to an incident
- Check that staff training has been completed, refreshed, and evidenced

It is never too late to check that arrangements are effective in preventing a terrorist act, protecting those exposed to the threat and ensuring an effective response if the unthinkable does happen.

References

1. The United Kingdom's Strategy for Countering Terrorism
2. Security Checklist for Businesses
3. National Protective Security Authority
4. National Protective Security Authority - Hostile Vehicle Mitigation
5. Action Counters Terrorism (ACT) e-learning

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

contact@rmpartners.co.uk

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

FP425-2025