ProtectUK

National Stakeholder Menu of Tactical Options

ProtectUK publication date

14/12/2023

This document outlines a set of options which can be used by the private sector and security industry to enhance the wider national security posture at times of raised threat or in response to a terrorist incident.

Contents

Introduction

The National Stakeholder Menu of Tactical Options can be implemented independently by an organisation or can be deployed at the request of police following an extraordinary Security Review.

The tactical options included in this guidance are not exhaustive and it is anticipated that this guidance will be reviewed periodically to ensure it is fit for purpose in meeting the ever-changing threat from terrorism to the UK.

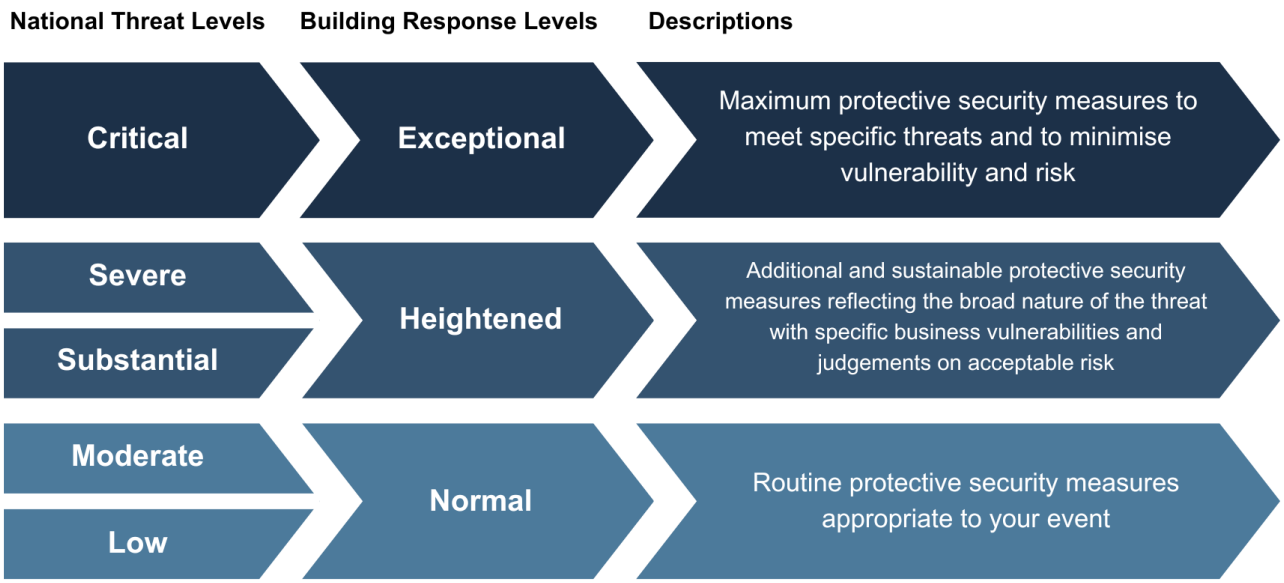
1. Threat level

Since 2006, information about the national threat level has been available on the Mi5 and Home Office websites. In September 2010, the threat levels for Northern Ireland-related terrorism were also made available.

In July 2019, a single national threat level system was implemented which aimed to reflect terrorist threat posed to the UK irrespective of ideology, which includes threats from Northern Ireland, Islamic extremism, left-wing and right-wing terrorism.

This single system of threat assessment allows the Government to examine the terrorism landscape facing the UK and determine the threat against five tiered levels, namely **Critical**, **Severe**, **Substantial**, **Moderate** and **Low**. This was designed to provide a broad indication of the likelihood of a terrorist attack.

These national threat levels, along with other considerations, inform the building response level, which are categorised as **Exceptional**, **Heightened** and **Normal**. Building response levels provide a general indication of the protective security measures that should be applied at a given time. Changes in the national threat level may not necessarily produce a change in building response level.



How threat level changes

In general, when the threat level has been raised, it has been post-incident and as a result of something happening (whether domestically or overseas) which has impacted mainland UK. This occurred, for example, in August 2014 when the threat level was raised from Substantial to Severe.

It should be noted that an increase to the highest tier of Critical has a significant impact on the UK, the resources across all agencies and potentially business and industry. It is therefore unlikely to remain in place for long periods of time.

Information about the current threat level is available on Mi5's website.

2. Responding to the threat

Overall strategy

In respond to a terrorist attack and increase in threat level, the overall business strategy is:

- To understand the type of threat posed – Why did the threat level increase? What was the attack methodology used?
- To consider the operational requirement, appropriate level of response, and range of tactical

options that are best suited to continue business-as-usual, in the parameters of this heightened state of alert

Even if a business has a robust security strategy in place, it is essential that they fully prepare for a Move To Critical (MtC) state to avoid complacency. By way of example, within 48 hours of the November 2015 Paris attacks, firms were unable to recruit any more skilled security guards to increase their security posture as they had failed to organise this in advance.

Attack methodologies

There are several types of attack methodologies, such as:

- Marauding attack (with firearms or bladed/blunt force weapons)
- Vehicle as a weapon
- Improvised Explosive Devices (IEDs)
- Fire as a weapon
- Chemical, biological and radiological (CBR)
- Cyber

Some types of attack methodologies are more prominent and more readily used by terrorist in the UK than others.

Operational requirement

When planning your business' response to an increase of threat level, it is important to complete the following strategic actions:

- To agree a menu of site-specific tactical options that are suitable for the organisation. Refer to the Menu of Tactic Options below
- Regularly exercise the plan to make sure that key stakeholders and staff are aware of the

impact on their area of work should a change be necessary

- Make sure that staff have been consulted and agreements in place if options impact on staff working practices

Appropriate and standardised practices are also important when reacting to an increase in the threat level:

- Escalate and quickly engage with key stakeholders
- Consider a range of options relevant to reduce the likelihood of the threat posed
- Continually review the tactical options to make sure they remain suitable to meet the threat posed
- Make sure that any change to tactical options will provide reassurance to staff rather than cause alarm
- Implement communication strategy that provides advice to staff around changes to planned events, deliveries or changes to access points
- Only react to information from official sources such as government, security services and police
- Have an immediate holding plan available to allow a more permanent solution to be found
- Consider implementing a command-and-control approach using the **Strategic**, **Tactical** and **Operational** planning system (formerly gold, silver, bronze system) which is similar to that of the emergency services and first responders
- Minimise disruption to business and promote recovery at the earliest time

3. Menu of Tactical Options

The following list of tactical options should be considered to support your business during an increase in threat level or following an incident or attack.

The tactical options are categorised in accordance to the DRIVES model which denotes the following:

- **D**etect and Deny
- **R**espond
- **I**nformation and Intel sharing
- **V**isibility and Deterrence
- **E**nabling Activity
- **S**pecialist Capabilities

It is acknowledged that the continuance of these measures may be unsustainable in the long-term and therefore suitable for informed revision when the threat level decreases.

In addition, the relevance of each of the tactical options will depend on existing practices and security

maturity of your business. Conducting risk management is therefore essential to identifying, assessing and controlling risks to your organisation.

The full list of Menu of Tactical Option is as follow:

- DB1 - Close non-essential access and egress points
- **DB2** - Search immediate parking areas and review access to them
- **DB3** - Ensure that all visitors and contractors provide at least 24 hours' notice, prior to attendance
- **DB4** - Ensure that visitors and contractors are accompanied at all times
- **DB5** - Cancel or postpone events
- **DB6** - Ensure all staff are challenged and their ID checked
- **DB7** - Check all vehicles and personnel on entry, including emergency services
- **DB8** - Implement a regular and unpredictable search sweep rota across site, including areas hidden from surveillance
- **DB9** - Restrict and only accept deliveries that are essential
- **DB10** - Scan all mail and ensure that postal procedures are robust
- **RB1** - Review and communicate incident response and business continuity plans with staff and neighbouring businesses
- RB2 - Ensure full adherence to incident response and business continuity planning checklist
- **RB3** - Ensure that lockdown procedures are known, tried and tested
- **RB4** - Ensure suitability of egress routes and muster points
- **RB5** - Ensure that all staff are briefed on roles and responsibilities during an incident in line with response plans and procedures
- RB6 - Ensure contents of crisis response and PAcT kits are up-to-date, secure and easily accessible
- RB7 - Prepare alerts, alarms and pre-scripted messages

- **IB1** - Ensure that staff are briefed on Threat and Response Levels
- **IB2** - Ensure that staff are briefed in observing, detecting and responding to suspicious activity
- **IB3** - Ensure that any suspicious activity is reported in a timely manner
- IB4 - Implement communication links with surrounding premises to pass on information and suspicious activity
- IB5 - Actively monitor CCTV/VSS at all times and review out-of-hours footage
- IB6 - Ensure that CCTV is focused on all communal areas and vulnerable points
- **VB1** - Ensure a strong security posture through Security Minded Communications
- **VB2** - Review patrol and positioning of security staff
- **VB3** - Ensure that perimeter fencing and security lighting is checked
- **EB1** - Implement emergency change to shift patterns and agree plan with staff in advance
- **EB2** - Join up resources with neighbouring businesses and contacts
- **EB3** - Cancel all non-essential training and meetings
- **EB4** - Ensure a communication strategy is agreed and document all decisions including rationale
- **EB5** - Ensure supporting technology, such as access control systems, are in working order
- **SB1** - Establish or review a C-UAV/UAS Plan

KEYWORDS
NATIONAL STAKEHOLDER MENU
TACTICAL OPTIONS
PROTECTIVE SECURITY
PROTECTIVE MEASURES
THREAT
MOTO

PAGE CATEGORY

SECURITY