ProtectUK

# Tactic IB1: Ensure that staff are briefed on Threat and Response Levels

**ProtectUK publication date**

14/12/2023

## Information and Intention

There are 5 levels which form the UK National Threat Levels:

- Critical
- Severe
- Substantial
- Moderate
- Low

These threat levels are designed to provide a broad indication of the likelihood of a terrorist attack and are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities.

Those who own, operate, manage, or work in venues and public spaces are reminded that Substantial and Severe Threat Levels indicate a high level of threat and that an attack might well come without warning.

Information about the National Threat Level is available at UK Threat Levels.

Dependent on the Threat Level, a building should adopt a commensurate Response Level. There are 3 types of building Response Level:

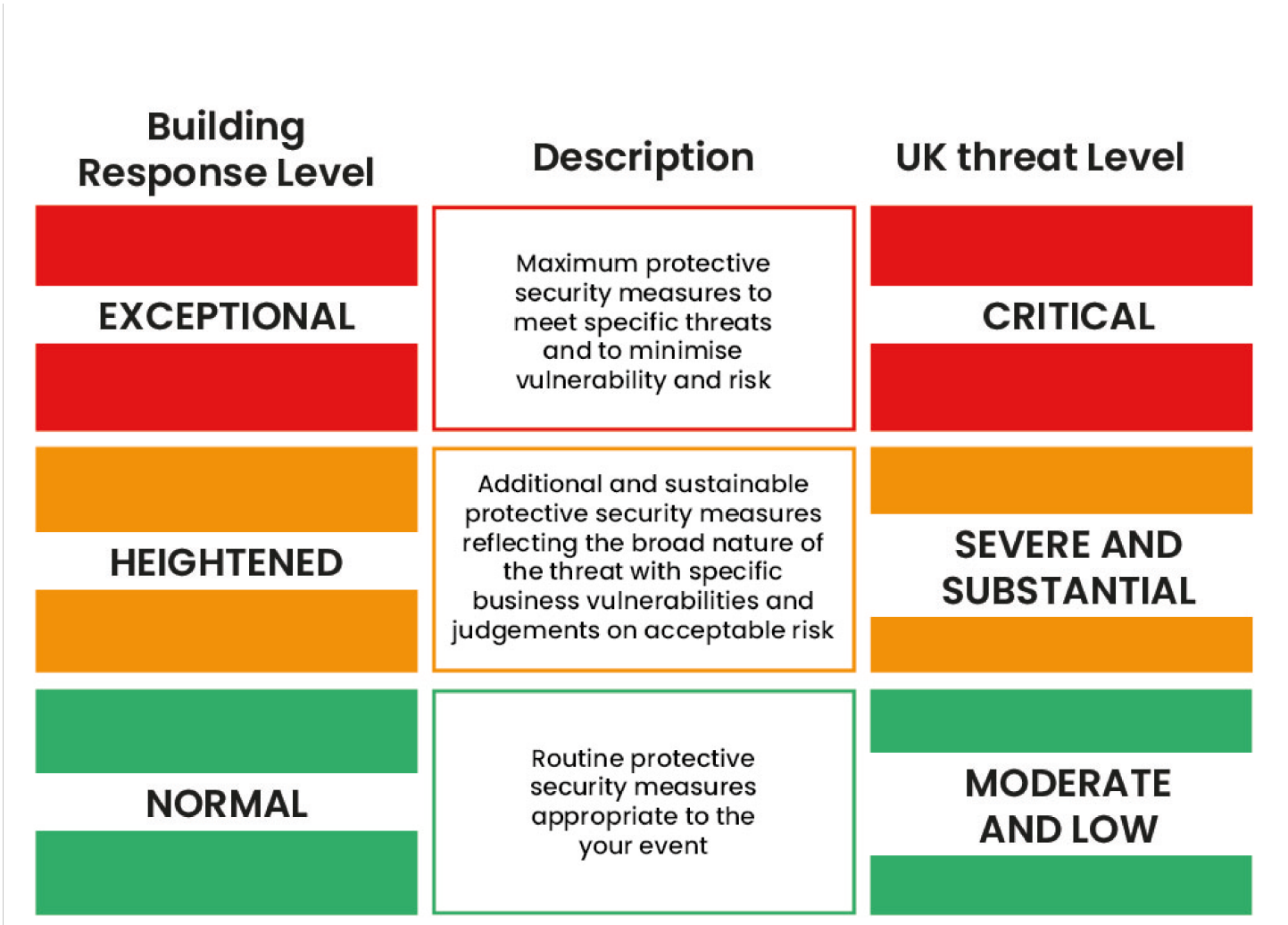
- Exceptional
- Heightened
- Normal

Response Levels provide a general indication of the protective security measures that should be applied at a given time. They are informed by the National Threat Level, but also take into account specific assessments of vulnerability and risk.

There are a variety of site-specific security measures that can be applied in each building Response Level, although the same measures will not necessarily be found at every location. The security measures deployed at different Response Levels should not be made public, in order to avoid informing terrorists about what we know and what we are doing about it.

All protective security measures should be identified in advance of any change in threat, and building Response Levels should be clearly notified to staff who are responsible for ensuring compliance.

The Threat Levels and appropriate Response Levels are shown below:




**Source: ProtectUK – Threat Level and Building Response Level**

## Method

Briefings on Threat and Response Levels can be achieved in a number of ways. These include:

- Providing security staff with a counter terrorism briefing at the start of each shift. This should include information about the current UK Threat Level and the relevant building Response Level. Staff should be informed as to what security measures are to be applied to the relevant building Response Level.
- Signage informing staff of the building Response Level should be clearly displayed, though this should not be displayed in public areas or within their sight.
- Information regarding Threat and Response Levels can be incorporated into staff information circulars, both in hard copy and electronic.
- Briefings on Threat and Response Levels and protective security measures can be incorporated into any training delivered to staff.

In order to keep the Threat Level information interesting and relevant, the briefing should also include information about any suspicious incidents detected recently, e.g. potential hostile reconnaissance.

Information about forthcoming major events or visits should also be included (although specific and detailed security information regarding these matters should be on a need-to-know basis).

## Administration

Strategic responsibility for ensuring that staff are briefed regarding Threat and Response Levels should rest with a member of your organisation’s senior management team. Practical responsibility for delivery should lie with the head of security, working in conjunction with the organisation’s communications team, to ensure the information is disseminated to staff using every medium possible.

All protective security measures should be identified in advance of any change in Threat and building Response Levels and should be clearly notified to those staff who are responsible for ensuring compliance. The protective security measures to be implemented at each building Response Level are a matter for individual premises or organisations and will differ according to a range of circumstances.

When staff members receive formal briefings regarding Threat and Response Levels, and they are provided with instructions on what their responsibilities are regarding this, they should have this information recorded (e.g. attendance record for briefing, personal record etc.).

It is important to test and exercise your response activity for each Response Level and that a record is kept of the results of the test.

## Risk Assessment

A risk assessment should identify threats which could have an impact on the business and its vulnerabilities. This risk assessment can be used to define the actions that are required to be taken regarding the use of Threat and Response Levels. Such risk assessments should clearly define organisational as well as individual duty of care to staff and others.

For terrorist-related incidents, reputational damage will be caused if the organisation fails to handle the incident correctly. For example, if briefings do not contain the appropriate or relevant information regarding Threat and Response Levels, and the actions of staff thereafter is insufficient due to a flawed briefing.

In addition to reputational risk, a failure to respond appropriately, and successful exploitation of vulnerabilities by terrorists, could lead to loss of life or serious physical damage to the site. These risks must also be acknowledged. It is important to record current and emerging risks, risk management and mitigation measures, reminding those under your charge of their duty of care to themselves and others.

A site or venue specific risk assessment should be carried out to help identify a range of practical protective security measures appropriate for each of the building Response Levels. Different attack types should be considered.

## Communications

Early identification and engagement with internal and external stakeholders is important in developing a holistic briefing process, from assessing the risk, through to developing appropriate responses. Agreement must be sought in relation to the roles and responsibilities of all those involved.

**Internal Stakeholder Engagement:**

It is essential that Threat and building Response Level information is communicated to your staff, and that they know what to do should there be a Threat or Response Level escalation. It is necessary to ensure points of contact are known to staff internally, and partners externally. This could be achieved internally through the Security and Communications functions.

You must provide regular information for your staff so that they can help deliver on the security plan. Your internal audience will inevitably cross over into your external audience, so you should consider the messages you want them to convey to their external networks, e.g. families and friends. Remember that social media is a potential area where this crossover may occur.

**External Stakeholder Engagement:**

Early identification and engagement with key external stakeholders is important. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering the plan, and consideration should be given to engaging with any working groups or forums who may already have identified ‘best practices’ and lessons learned from similar sites within the business area the site operates within.

There are a number of key principles that should be applied when engaging with stakeholders:

- The engagement should be different for different stakeholders, at different times – it should be flexible as one type of engagement process does not necessarily suit all stakeholders.
- It should be a two-way engagement process, where information and knowledge are shared.
- Communications should be genuine and timely, where there is the ability to influence outcomes, dependent on feedback.
- Engagement with stakeholders should be open and transparent.

As with all matters relating to security and policing, the relationships with the police are key. The contact may be with either the local police or those specifically tasked with providing policing to certain sites.

**External Media Engagement:**

Organisations should not provide information regarding building Response Levels directly with the media or external audiences, as this information can be used by terrorists or other hostiles in the planning of an attack. In addition, avoid revealing details about Response Level actions through social media, as this can also provide essential information to terrorists preparing an attack.

## Health and Safety/Other Legal Issues

Businesses/organisations that operate Threat and Response Level processes should ensure that all activities are assessed in line with Health and Safety and other legal/policy frameworks, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- Employment Rights Act 1996

It is important to consider any briefing related activities with regards to justification, proportionality, necessity, and legality. Incorrectly responding to a Threat or Response Level could lead to legal

issues and all options should be considered as potential mitigation measures in the risk assessment process.

You should ensure that there are well-defined governance arrangements and that records are kept of the issues, decisions made and the reasoning behind those decisions which involve Threat and building Response Levels. Records will provide evidence to any investigations, or public enquiries and assist in defending against legal action, criminal charges or civil claims.

The importance of keeping accurate records and having well defined governance arrangements has been demonstrated during the Manchester Arena Inquiry.

**KEYWORDS**
THREAT
THREAT LEVEL
RISK ASSESSMENT
COMMUNICATIONS
NATIONAL THREAT LEVEL