ProtectUK

Purple Guide Chapter on Counter Terrorism - Threat Levels

One of the lessons from the Manchester Arena Inquiry was that those in charge of the event did not seem to acknowledge this fact in their planning. It is essential that the threat level is considered when planning the measures that may be necessary and proportionate to the event.

The level has not dropped below substantial since before 2006 when records were made public on the MI5 website. Where does the threat level come from? MI5 publish a national threat level to help the public plan for appropriate levels of security.

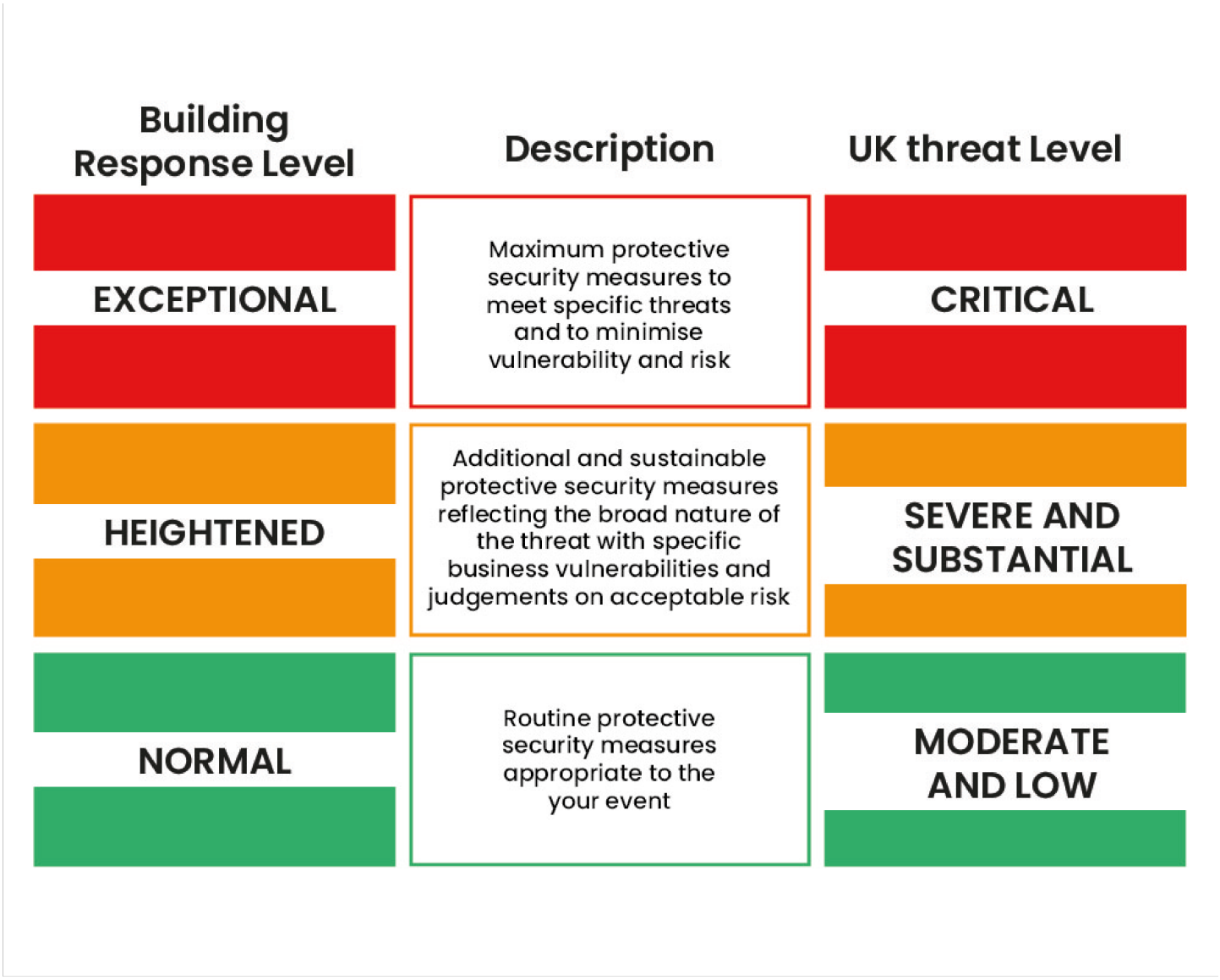
Further information on the threat level to the UK can be found here.

The threat level is decided by the Joint Terrorism Analysis Centre (JTAC) and the Security Service (MI5). Threat levels do not have an expiry date and they can change at any time as different information becomes available. This needs to be considered when planning measures. Any plan should be flexible enough to take into account changes in the threat level.

When deciding the threat level, the following will be taken into account;

- Available Intelligence
- Terrorist Capability
- Terrorist Intentions
- Timescale

Response levels should provide a general indication of the protective security measures that need to be applied at a given time depending on the current UK national threat level and any specific assessments of vulnerability and risk in relation to the event being planned. Response levels tend to apply to sites whereas threat levels tend to relate to areas of activity.



Further advice around threat levels at crowded places can be found here.

Understanding the threat facing the event is key to ensuring that protective security measures and mitigations are proportionate, effective and responsive.

Counter Measures

Deter/Detect/Delay/Mitigate/Respond

When developing a proportionate plan for an event, it is essential to understand the principles of protective security. The measures should cover the deterring, detecting, delaying, mitigating and responding to an attack. It is not always appropriate to consider all of these aspects but an understanding of how these work together is essential.

Deter involves discouraging adversaries from conducting an attack by making each element appear

too physically or technically difficult to achieve. An example of this could be highly visible security patrols around the outside of the event.

Detect involves being alert to potential attack behaviours at every stage, from planning and reconnaissance to deployment. The deployment of behavioural detection operatives or encouraging staff to be aware of hostile reconnaissance behaviour are examples of detection methods.

Delay involves implementing measures that increase the time it takes for attackers to get to the location of vulnerability once the attack starts. This could be ensuring that the right type of perimeter fencing is used to ensure it is harder to penetrate.

Mitigate involves the use of measures to minimise the impact of an attack. The use of a hostile vehicle mitigation system to prevent vehicular access and provide appropriate stand-off is an example of this.

Respond involves ensuring that measures are in place to respond to an incident. This is crucial in ensuring that harm is kept to a minimum. Appropriate training of response staff and a credible response plan are key to ensuring that any incident is dealt with professionally.