ProtectUK

Advice for security managers during a heightened threat level

ProtectUK publication date
27/08/2021

This advice will provide advice to security managers of Publicly Accessible Locations following a change of the threat level to CRITICAL. There are a number of operational and tactical options to consider.

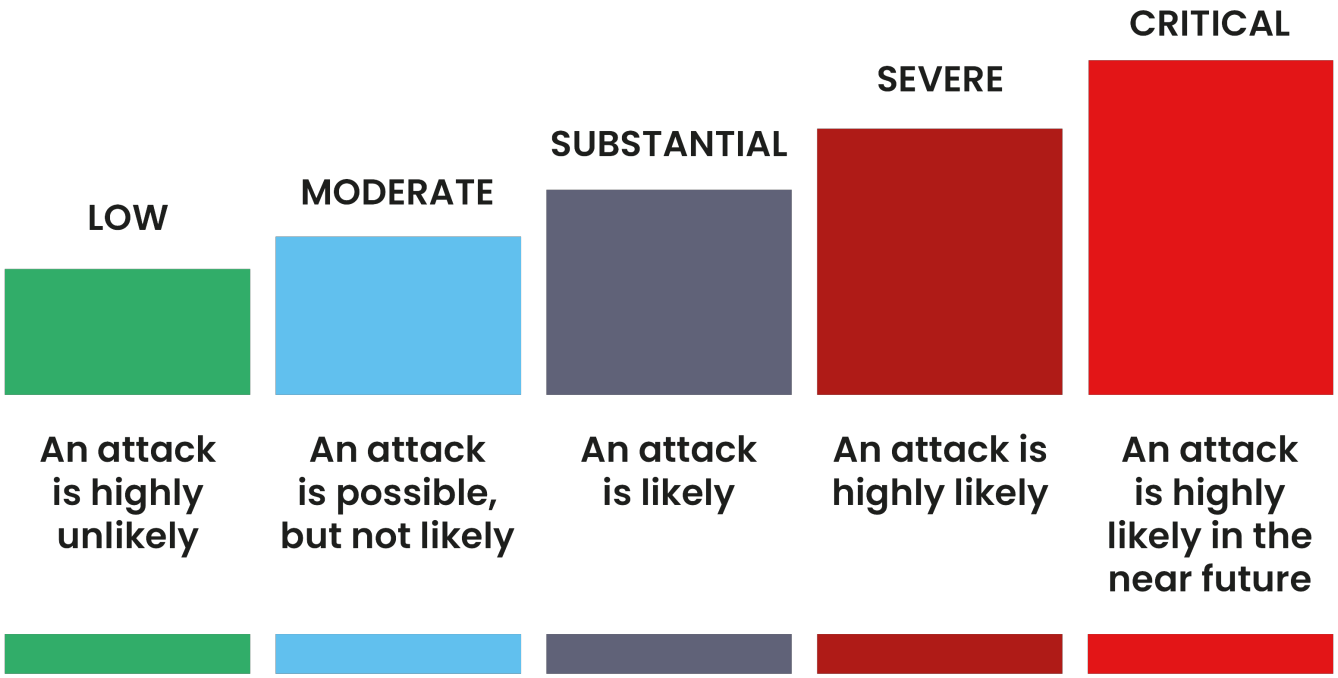
1. Introduction

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

Information about the national threat level is available on the threat level page.

2. Threat level definitions

There are five levels of threat which are defined below:



Should there be a change in the threat level, it is recommended those responsible for security review their plans and operations. They may also wish to consider the options outlined below.

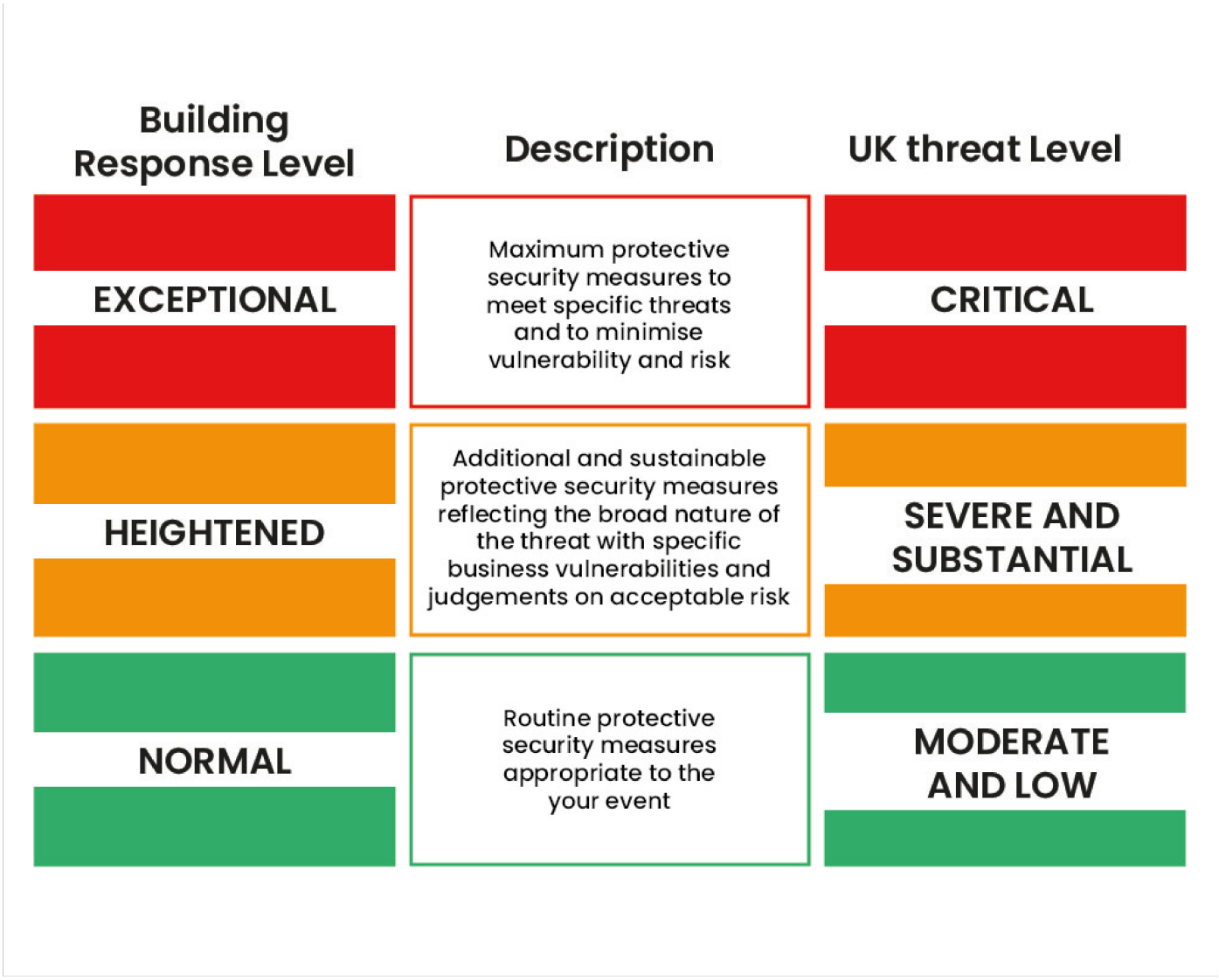
3. Building response levels

Building response levels within an organisation provides a general indication of the protective security measures that could be considered and applied to a site or building. They are informed by the UK threat level, but also take into account specific assessments of vulnerability and risk. In the event of an incident or change to the UK threat level, individual sites or buildings should conduct their own dynamic risk assessments and apply appropriate protective security measures.

There are three levels of response: **EXCEPTIONAL**, **HEIGHTENED** and **NORMAL**.

Response levels equate to threat levels and 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 each response level, 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 is known and what action are being taken.

The security measures deployed by a site / building at the different response levels should not be made public. This is to avoid equipping terrorists should they be conducting hostile reconnaissance



4. Additional information

There are practical actions you can take to improve the security of a venue:

4.1 Risk assessment

- carry out a risk assessment that is specific to the venue

4.2 Building response level

- regularly review the response level for the site or venue at security meetings
- clearly display signage informing staff of the building response level. This should not be

displayed in public areas or be within their view

5. Security guard force: posture and activity

Proactive engagement and staff briefings: One of the most effective measures to deter terrorists and wider criminality is a competent security guard force who appear vigilant and proactively engaged with the public. Terrorists and criminals generally feel uncomfortable and exposed when approached by a security officer, albeit politely, particularly if they are conducting hostile reconnaissance. This intervention casts doubt about the success of their attack planning. Staff briefings will allow your security officers to understand the importance of proactive engagement and they should be encouraged to do this where practical and reasonable to do so. For example, should security use a vehicle, and patrol areas such as car parks, then park and leave the vehicle for a short period in order to engage with people. This may be as simple as saying, “good morning”.

Unpredictable security measures: Unpredictability results in the uncertainty and erosion of confidence in the mind of the terrorist, who needs to encounter predictable security arrangements in order to feel assured of success. Wherever possible, introduce unpredictability into the security regime; for example, change patrol patterns, timings and search regimes.

'Recruit’ staff to be vigilant and immediately report suspicious activity and items: use existing staff communication channels, such as shift briefings and the intranet, to inform your staff what suspicious activity may look like. Encourage them to trust their instincts and report anything suspicious immediately to the security control room/police. In these communications, reinforce the message that reports will be taken seriously and be investigated. Where possible, highlight examples where previous staff reporting has led to positive outcomes; this helps promote confidence.

The protective security measures implemented at each building response level are a matter for each individual premises or organisation and will differ according to a range of circumstances. It’s advised a menu of options should be identified in advance of any change in national threat level or building response level, and should be clearly notified to those staff who are responsible for ensuring compliance. It is important to train staff and to conduct rehearsal exercises for each building

response level.

The checklists below provide a number of protective security options you may wish to consider.

6. Security checklist

6.1 Initial actions

- Review security plans
- identify the risks based on the current UK threat level
- review Business Continuity Plans
- decide what is needed to protect, identifying critical operations and functions
- increase staff vigilance – through appropriate briefing mechanisms
- review evacuation, invacuation and lockdown procedures. Make sure there are plans for vulnerable staff and visitors. Have you designated marshals to support this activity?
- identify ‘protected spaces’
- review your Emergency Assembly Point

6.2 Preparedness

- make sure first aid kits are fully stocked and staff know where they are kept
- make sure Crisis Incident Kits (grab bags) are available and up-to-date

6.3 Communication

- brief staff – make sure they understand their roles and responsibilities
- engage with neighbours, partners and suppliers
- make sure staff and visitors can be alerted of any imminent or immediate threat or incident
- provide prior notification to staff and visitors of enhanced security measures, encouraging them to arrive in plenty of time and encourage them to bring minimal possessions
- monitor news and media channels
- develop pre-scripted messaging and alerts and determine how these will be communicated to staff and visitors

6.4 Personnel

- maintain an up-to-date list of personnel. Do HR update leavers and joiners?
- consider staffing requirements. In some instances, this may include the requirement to alter or extend staff shifts, or the cancelling of leave
- consider cancelling non-urgent business or visitors where appropriate
- identify whether there is sufficient staff for critical roles such as in the control room
- review requirements for Personal Protective Equipment (PPE) for security staff

6.5 Training

- ensure all staff understand how to respond to a terrorist incident. See the ETHANE checklist.
- are staff first aid trained?
- review and deliver training to staff and conduct rehearsal exercises

6.6 Staff vigilance

- do all staff understand how to respond effectively to reports of suspicious activity and items when reported by the public? Are they clear who they should report to internally and when to report to police using 999? Do staff understand the HOT protocol?
- disrupting hostile reconnaissance: make sure staff understand how to identify suspicious behaviour. Is a challenge culture promoted amongst staff?
- make sure all staff and visitors wear passes
- where entry is restricted, check the visitor's identification prior to permitting access to the site

6.7 Physical security

- enhance security presence where appropriate. Consider staff patrolling in high visibility clothing
- make sure CCTV is working effectively and that it is suitably monitored
- review the site's access control measures. Where appropriate close any unnecessary entrances to prevent unauthorised access
- make sure infrastructure, such as signage, lighting, floor level signs, stairs etc. are clearly marked and labelled
- prepare floor plans
- establish if the control room is capable of being operationally effective against different attack types and can be secured and protected
- check critical systems and equipment such as PA systems
- make sure control rooms have alternative means of communication such as mobile phones with spare batteries, chargers etc.
- consider the protection requirements for any queues of people created by additional search measures (CCTV, position of the queue etc.).

6.8 Search and screening

- search, screening and looking for prohibited items should, when done well, provide a good capability to detect larger threat items concealed on a person
- there will be a finite amount of security and screening resources; focus on addressing the highest priority threats
- be clear about what the search process is aiming to detect and where the process will be conducted
- define a list of prohibited items. Communicate this both to customers and personnel conducting the search
- make sure advanced notification (at point of sale or media) of your site’s extra security measures and encourage people to arrive early. This will smooth peaks and allow safe and effective searching
- provide effective public address messaging to people as they approach, asking people to prepare for additional search and screening. This will help to reduce delays
- consider initial search and screening on the approach to, or outside the venue, for example a visual check inside jackets and bags
- conduct search and screening measures efficiently, effectively and politely. Aim to maximise screening throughout (to minimise queues that may be targeted) without compromising the required level of security
- bags and other items should be searched to the extent required to provide confidence that no items of concern are present. Manual bag searches should be proportionate, systematic, consistent and safe for the person conducting the search
- manual person searches should be considered to the extent required to provide confidence that no larger threat items are present. Consider the privacy needs of the individual
- make sure the site or venue is searched on a regular basis, but not at predictable times or in a predictable way
- make sure you maintain the search regime for the lifecycle of the event including prior to its commencement, during and post event

- determine whether vehicles are allowed into your venue and if whether they are to be searched
- train search staff to search safely and effectively
- make sure all staff are aware of the response when they locate threat items
- there are a number of other tactical options available for search and screening. Specialist advice should be sought from the NPSA website, or your local Counter Terrorism Security Advisor

6.9 Security personnel

Depending on their responsibilities, security personnel must be able to demonstrate they can respond competently to a number of scenarios:

- respond effectively to reports of suspicious activity and items when reported by the public. Knowing who to report to internally and when to report to police using 999, 101 or the Anti-Terrorist Hotline 0800 789 321
- as an initial responder to a terrorist incident. See the ETHANE checklist.
- the maintaining of an effective search and patrol regime for the lifecycle of an event, including prior to, during and post event. Consider a patrol sweep of the public areas before, during and after an event for suspicious items and behaviours. Patrol areas may include areas close to the site, pick up zones and transport hubs. Ensure they are able to communicate effectively with their control room
- respond to the different activities required should there be an increase to the UK threat level or building response level
- patrol effectively to disrupt hostile reconnaissance activity, identifying and responding to suspicious behaviour
- respond effectively to suspect items, including knowledge of the ‘four Cs’ protocols and the HOT protocol
- chemical, biological and radiological incidents, how to recognise and respond using REMOVE.REMOVE.REMOVE.

- respond to firearms and weapons attacks and the importance of Run. Hide. Tell.
- understand evacuation, invacuation and lockdown procedures
- search a site effectively
- apply the basic principles of good housekeeping and how it reduces the opportunities for an attack
- respond appropriately to a bomb threat
- use emergency first aid equipment such as defibrillators etc.
- use of incident logs and checklists, in order to facilitate an effective response to incidents such as terrorist incidents and bomb threats etc.

6.10 Good housekeeping

- where the risk assessment determines it is necessary, examine opportunities to reduce reasons for crowds to develop, such as reducing, removing or relocating activities that are attractive, such as street entertainers and mobile food outlets. Consider increasing patrols in those areas. Carefully consider where these activities take place and the security posture around it
- review the use and location of all waste receptacles in and around your venue or event, taking into consideration their size, proximity to glazing and building support structures? Consider repositioning and securing within areas which are not crowded.
- are bins emptied regularly?
- are external areas, entrances, exits, stairs, reception areas and toilets kept clean, tidy and well lit? Where possible, reduce areas where items can be concealed
- is furniture kept to a minimum to provide little opportunity to hide devices, including under chairs and sofas?
- use seals/locks to secure maintenance hatches, compactors and industrial waste bins when not required for immediate use
- consider arranging vehicle deliveries for times where the fewest number of people are on site.

Consider adopting time windows where no deliveries will be accepted

- is all your mail screened and can the mail processing area be isolated?
- has testing and exercising for a terrorist incident been carried out within the last 12 months? Do staff understand their roles and responsibilities?
- are relevant staff and deputies trained and competent in managing bomb threats?
- is the content of first aid kits, crisis management packs and firefighting equipment regularly checked?
- check CCTV to make sure it is working effectively and has sufficient coverage both internally and externally?
- have the location of street vendors (e.g. flower sellers, news-stands and refreshment stalls) been taken into account so that there is no impact upon evacuation routes, assembly points, exits or entrances?
- are cycle racks and lockers positioned away from crowded areas? Is CCTV monitoring necessary?

For further information visit:

- NaCTSO
- NPSA (formerly CPNI)
- Cabinet Office
- Emergencies: preparation, response and recovery
- Emergency planning

KEYWORDS
THREAT
SCAN
PHYSICAL SECURITY
PERSONAL SECURITY
PERIMETER
RISK MANAGEMENT

PAGE CATEGORY
SECURITY