ProtectUK

Tactic EB3: Cancel all non-essential training and meetings

ProtectUK publication date
14/12/2023

Information and Intention

An increase in the National Threat Level to 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.
It should also be noted that the tactical option included in this document is not just for use after the threat level has risen to Critical.

Cancelling non-essential training and meetings can ensure your business'/organisation's resources and staffing levels are managed effectively and efficiently following a change in the threat, intelligence or an incident. Experience has identified keys areas to consider:

- Review your resources and have a back-up team in place if possible, from a partnership organisation, other parts of your own organisation, or an external source such as Local Resilience Forum (LRF).
- Support your communications team and ensure consistent internal communications.
- Do not be over reliant on online networks, have a plan B for technological failures.
- Ensure there are clear roles, responsibilities and sign-off procedures, for both internal and external communications.
- Do not underestimate the scale of an incident including the level of interest from the media (national and international) and the public, nor its duration.

It is also a good idea to look beyond the organisation and the crisis team and build relationships with any nearby residents or businesses. They will also be affected in the event of an attack and will look to their organisation for guidance and reassurance.

Method

The decision of which training and meetings are cancelled are at the discretion of the individual business or organisation and will differ according to a range of circumstances. This can be further classified based on significance, resources, vulnerabilities and attendee numbers.

However, once such a decision has been made the following measures may support implementation of the tactic whilst ensuring business continuity:

- Access an up-to-date list of personnel (does HR update leavers and joiners?).
- Consider your staffing requirements. In some instances, this may for example include the requirement to alter or extend staff shifts, or the cancelling of leave.
- Consider cancelling non-urgent business or visitors where appropriate to your venue.
- Identify whether you have sufficient staff for critical roles such as your control room and security detail.
- Review requirements for Personal Protective Equipment (PPE) for security staff.
- Ensure Business Continuity Management (BCM) plans are in place and activated when required.

Administration

Policy and procedures should mention the requirement to cancel all non-essential training and meetings at times of heighted threat. Identify ownership of the policy and governance of the decision making, including who is responsible for the management, coordination and strict compliance, together with the relevant records keeping and how its effectiveness is assured.

Ensure staff understand processes and procedures to be adopted, including actions and contingencies.

It is good practice to identify and communicate with the resource allocation manager who should deploy resources in accordance with demand profile for the organisation.

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 items that need to be detected; either to prevent them from entering the facility or detect them if they have already been placed in the building.

Such risk assessments should clearly define organisational as well as individual duty of care to staff and others. Staff, contractors and visitors may have different responses to the same incident and therefore you should risk manage the impact of staff, contractors and/or visitors as well as members

of the public not following or directly contradicting instructions.

Communications

Internal Stakeholder Engagement:

Dedicated channels should be established, with backups if access to the organisation's intranet or message channels is limited (for example if the intranet is restricted due to criminal investigations), if the network is overloaded, or if it has been the target of the attack.

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 are 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 communication strategy, and consideration should be given to engaging with any working groups or fora 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:

After a terrorist incident has occurred, organisations should not communicate directly with the media or external audiences on anything related to the incident, without prior consultation and agreement

with the police. In addition, avoid revealing details about the incident through social media without prior police consultation.

An appropriate individual should be identified in the organisation to liaise with the police in order to disseminate approved information which is accurate, and which will not compromise the criminal investigation.

Health and Safety/Other Legal Issues

Any decisions regarding the cancellation of non-essential training and meetings should be made 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
- Employment Rights Act 1996

Any change to shift patterns as a result of such cancellations should be justified, proportionate, necessary and legal.

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. Records will provide evidence to any potential 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
STAFF
SECURITY
EMERGENCY PLANNING
INCIDENT MANAGEMENT