ProtectUK

Tactic RB5: Ensure that all staff are briefed on roles and responsibilities during an incident in line with response plans and procedures

ProtectUK publication date

14/12/2023

Information and Intention

Prior to any briefings, staff should be made aware of the differences between incident response and incident management. This to ensure they have a full understanding of the different roles and responsibilities during an incident.

ProtectUK provides a helpful summary of these differences, see: Managing Risk and Business Continuity.

Information relating to the importance of roles and responsibilities is outlined in NPSA's Crisis Management for Terrorist Related Events.

Incident response deals with the immediate impact of an incident. It is a relatively short-term phase that focuses on escalation and activation in order to make sure people and the environment are supported and made safe wherever possible.

Incident management refers to how the organisation will manage the consequences of the business interruption at the scene through command, control, co-ordination and communication. This includes coverage of key areas, such as who is in charge, how to keep stakeholders informed, escalation processes, and co-ordination of resources.

By planning in advance, having relationships and initial key outputs in place, organisations can ensure they are taking a leadership position as soon as a crisis occurs which will serve to ensure that staff are:

- Empowered: staff should know how they can contribute to security in terms of precautionary action, ongoing maintenance and response to incidents.

- Aware: staff should understand the need for security, how it will impact on their role and responsibility and what to do if they suspect a problem.
- Collaborative: strong relationships should be cultivated at all levels within the business, and with external stakeholders including contractors, suppliers, local authorities, the police and other emergency services, community groups and nearby businesses.

Method

Staff briefings should take place at the start of each shift and should always include content in relation to observing, detecting, and responding to suspicious activity. These briefings will allow your security officers to understand the importance of proactive engagement with individuals and they should be encouraged to be proactive where practical and reasonable to do so. They should also be briefed on their roles and responsibilities during an incident in line with response plans and procedures.

In addition to staff briefings, you should use existing staff communication channels to reinforce the message (such as the use of posters, staff publications, and the intranet) and to inform your staff what suspicious activity may look like. Encourage them to report anything suspicious immediately to management/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.

Supervisors/managers should also:

- 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.

For further information, see: ProtectUK - Advice for security managers during a heightened threat level

As part of a self-briefing process, staff should be encouraged to undertake free online training courses which cover understanding and identifying suspicious activity. These include:

- ACT Awareness e-Learning
- NPSA - SCaN (See, Check and Notify)

Importantly, staff should be debriefed at the end of their shift to ensure that incidents of suspicious activity have been recorded and investigated.

If the briefing or training input on suspicious activity was delivered to staff, then it should be recorded in their personal record, to evidence the fact they have undertaken this.
It is also good practice to provide feedback to staff on previously reported suspicions as this will instil the belief that their observations and response make a difference.

One of the most effective measures to deter terrorists and criminal activity is a competent security guard force who are 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.

Administration

Policy and procedures should mention that staff are briefed on roles and responsibilities during an incident in line with response plans and procedures should the threat level be raised or following an incident. Identify ownership of the incident 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 action and contingencies (e.g. mail handling, courier deliveries, receiving of visitors).

Risk Assessment

A risk assessment should identify threats which could have an impact on the business and its vulnerability. 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 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.

A key action for a business is to create a Crisis Communication Plan (TACTIC EB4). This should be a core component of its risk preparations. It should be developed following a detailed risk analysis looking at potential issues and possible solutions. Typically, these issues relate to an organisation's people, assets, property and operations, and the plan is there to guide action and communications.

Communications

Internal Stakeholder Engagement:

Certain aspects of your briefing to staff on their roles and responsibilities during an incident, in line with response plans and procedures, may not necessarily be communicated to all your staff. However, staff members should be briefed on what to do in order for them to fulfil their roles and responsibilities.

It is necessary to ensure points of contact regarding this action are known to staff internally, and partners externally. Any information regarding this briefing should be disseminated internally through the Communications function.

All security management/security staff should understand their role and function following such briefings and the person delivering the briefing should check their understanding. Internal communications should reinforce and encourage security awareness by staff and a positive security culture should be encouraged through internal communications.

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:

Specific information on staff roles and responsibilities should not be shared externally. However, engagement with neighbouring businesses should be on a regular basis and should be constructive.

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 on any crisis response outcomes, and consideration should also 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:

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

Businesses/organisations 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

Your actions must be justified, necessary and proportionate to the threat you are facing.

Briefings should be thorough and clear in its messaging. Consideration must be given regarding the personal health and safety of all staff in the performance of their duties. There must be well defined governance arrangements and records must be kept of the issues, decisions made, and the reasoning behind these decisions. Records will provide evidence to any investigations, coroner's inquiries and public inquiries 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.