ProtectUK

Tactic RB7: Prepare alerts, alarms and pre-scripted messages

ProtectUK publication date
14/12/2023

Information and Intention

Terrorist attacks are intended to cause fear and, in many cases, to cause serious harm to people. Communication has a key role to play in keeping everyone as safe as possible through:

- Providing information about the nature of the threat.
- Keeping people away from the threat or other hazards or other methods to keep people as safe as possible.
- Summon assistance (e.g. police or first aid).

It should be remembered that while terrorist attacks are rare, they are likely to have a very high impact when they do occur. Systems should be in place that support communications through Business-as-Usual (BaU) operations and during the response to an attack when the requirements of communications technology are likely to be different. The benefits of using the same system during all phases are:

- Staff will be familiar with its use and therefore more likely to use it during an incident.
- Staff will be better at using the system, be more practised, and more likely to follow the defined protocols that they know work effectively. Reducing the burden on staff will enable a better quality of communication.
- An attack may start with a BaU issue (e.g. abandoned bag), so communications might start as usual and then escalate as the incident develops. The system should be able to expand to manage the anticipated surge in demand.
- A single system will be the most cost-effective.
- The amount of equipment that needs to be carried will be minimised.

The response to any terrorist incident is split into several phases, each requiring of messaging and alerts to staff. These phases are set out within the NaCTSO guidance titled Managing Risk and Business Continuity.

However, this Menu of Tactical Option (MoTO) is focused on the incident response and incident management phases, with more detailed information being provided within NPSA publication Developing Effective Command and Control.

Method

Organisations should consider how the communications methods intended for use during the immediate response to an attack can be developed and improved. When conducting a review of existing capabilities, organisations and businesses should consider how they communicate with both those within their own and their neighbouring sites.

Incident response deals with the immediate impact of an incident. It is a short phase that focuses on escalation and activation, ensuring people and the environment are supported and made safe wherever possible. This period will cover a site's immediate response and the attendance of the Emergency Services to resolve the incident.

Incident management refers to how the organisation will manage the consequences of the business interruption at the scene through command, control, coordinate and communication. This covers who is in charge, how to keep stakeholders informed, escalation processes, coordination of resources, etc.

Each phase will overlap; the tasks relevant to one phase are likely to be running as the tasks relevant to subsequent phases have been activated. The nature of communication during each phase will change. During the BaU phase, there is likely to be a lower intensity of communication. This will be focused on routine and non-urgent activity. There is likely to be a rapid and significant increase in communication as an incident is identified and the incident response phase commences. The communications technology used within your organisation can be used across each of the phases. However, the effectiveness will vary. It is likely to be the number, type and method of communication that changes.

Command and control capability will vary considerably from site to site. However, the site should have plans in place to enable a comprehensive response to a terrorist incident with procedures introduced that are straightforward and easy to implement.

The level of automation or operational involvement required is an important consideration when selecting a communications system. Automation is likely to be of considerable benefit where there is little or no Security Control Room capacity. The use of any system is likely to require:

- Staff to be trained in its use.
- Systems to be reliable and regularly updated, tested and maintained.
- An element of operational input when responding to an attack or another incident.

Careful planning is required to introduce the most appropriate communications systems for sites. Each site should define their requirements for communications capability before deciding which solution they need.

Whichever system is used for alerting and messaging staff, you should consider the following in your approach/plans to ensure effectiveness:

- What type of message is being shared?
- In the event of an attack, what information should be immediately communicated?
- Who is delivering it?
- Who are messages being communicated to? (Staff, Management, Visitors, Neighbours, Public)
- How do they receive the message? Do they have disabilities (deaf or hearing impaired/blind or partially sighted)? Do they understand English?
- Are you communicating to other organisations who may have their own control room or individuals who may be working alone?
- How many people need to receive the message (capacity)?
- How quickly do people need to be alerted to the message being sent?
- Where does the message need to be delivered to (coverage)?
- Is a response required?
- How is the message being delivered?
- Will there be permanent monitoring of the system?
- How will systems be affected by a surge in communications?

Sites should also consider:

- How much time will a system take to administer and keep up to date?
- What is the user training requirement? Sites with a high turnover of staff will need to develop a training plan that is able to provide new staff with the information they require.
- How are data protection risks being managed?

In addition to the above, staff briefings, which are an effective way of alerting and communicating, 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.

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.

Organisations may also seek to:

- Engage with neighbours, partners and suppliers.
- Make sure contractors 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 suspicious activity as this will instil the belief that their observations and response make a difference.

Administration

Policy and procedures should mention preparation of alerts, alarms and pre-scripted messages 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.

Risk Assessment

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

The business or organisation should consider how to communicate effectively with their staff through the provision of alerts, alarms and pre-scripted messaging. Staff briefings should communicate the importance of communication during incident response and incident management phases and why such activities should be identified and responded to in order to facilitate understanding and compliance.

It is necessary to ensure reporting procedures are known to staff internally, and partners externally. Internal communications should also encourage security awareness by general 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:

Engagement with neighbouring businesses should be on a regular basis and should be constructive. The sharing of information with neighbouring businesses and contacts during the phases of incident response and incident management will contribute to overall resilience and effectiveness of the security plan.

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 relationship with the police is 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 that are implementing the preparation of alerts, alarms and pre-scripted messages 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.

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
INCIDENT MANAGEMENT
SECURITY
ACCESS CONTROL
RISK