ProtectUK

Tactic RB4: Ensure suitability of egress routes and muster points

ProtectUK publication date
14/12/2023

Information and Intention

Those with responsibility for buildings and other premises should consider the threat from a broad range of terrorist attack methodologies. Such methodologies may include vehicle as a weapon, marauding attacks with either bladed weapons or firearms, and improvised explosive devices (IEDs).

Planning your emergency response requires consideration of a range of plans and procedures, including emergency evacuation, ‘invacuation’ and lockdown procedures, and the use of protected spaces.

The initial decision-making regarding the invoking of an emergency response is usually made by the management of the premises. For outdoor festivals and other events, this may be the event/crowd safety manager in conjunction with the promoter/organiser. During an incident, initial decision-making should not be delayed pending instruction or action from the police. The speed of decision-making and implementation during an incident is critical.

Police will provide support, advice and guidance as soon as they are able, however this may not be immediate. In exceptional cases, the police may insist on evacuation, although they should always do so in consultation with the security manager or responsible individual. This decision must always be documented.

Actions taken by your site should be reasonable, necessary and proportionate, based upon the circumstances, particularly when they are necessary to protect life.

Communication without alerting attackers is generally preferable, hence any use of code words either over public announcement systems or over radios would need to be included in your sites planning, training and exercising.

Evacuation in non-fire scenarios is not the same as evacuation due to fire. Buildings and events will

have long established fire evacuation procedures and staff, contractors and visitors are likely to be familiar with the principles and practice of fire drills including evacuation. However, most will be unfamiliar with the procedures in relation to bomb evacuations.

The sudden movement of large numbers of people creates its own risks. This movement may arise from the fear of a terrorist attack as well as an actual threat. People may be frightened, and the surrounding crowd may move in conflicting directions and/or in a rapid or disorderly fashion. Disorderly movement may also increase the risk to those more vulnerable such as children, elderly, or people with impairments.
It is important that you regularly review your Emergency Assembly Point.

Security managers must understand what is required for evacuation, invacuation and lockdown procedures, especially in the event of a heightened threat level.

Method

In the event of a suspected device being found, a cordon must be established at various distances depending on the size of the suspected device:

- Bag/suitcase: 100m minimum
- Car: 200m minimum
- Large Vehicle: 400m minimum

In reality, these distances may not be achievable. During the planning phase, it may be worthwhile agreeing in advance some assembly points that can be achieved that are supported by risk assessment. Include these points in any briefing or documentation to duty staff.

A directional evacuation may be beneficial if a specific area is, or is likely to become, dangerous, or if an alternative route would result in people passing through or near to the area of threat. Selection of this strategy may increase the overall evacuation time but could improve safety. For this method of evacuation to work effectively, it would require staff and visitors to be familiar with the different routes and the names of the exits, which should be clearly labelled and communicated, e.g. Exit A, blue exit, floor 1.

A full site evacuation would be appropriate when directed by police and/or it is reasonable to assume the attack or threat is credible, and when evacuation will move people towards a ‘place of relative safety’. You may wish to direct people to ‘evacuate to their nearest exit’ and disperse, or direct them to specific exits. It is important to note that the safety of particular routes may change during the course of an attack. For example, the use of lifts (in non-fire scenarios) may reduce evacuation times, but send people to an area where attackers may be located.

For chemical, biological and radiological (CBR) incidents, consider evacuating uphill and upwind, staying away from the building heating and ventilation systems should the incident have occurred inside a building.
The suitability (e.g. with regards to trip hazards, lighting, pinch-points etc.) and capacities of evacuation routes and exits should be regularly assessed. Knowing the limitations of a particular route or exit is helpful in decision-making in order to determine how quickly your crowds can safely exit.

In some emergency scenarios, the appropriate response may be not to evacuate. If the threat is outside your venue, or the location is unknown, people may be exposed to greater danger if the evacuation route takes them past the threat (e.g. a suspect device, contaminated environment or an ongoing external attack) and a dynamic reassessment is required. Since glass and other fragments from IEDs may kill or injure at a considerable distance, moving people inside is often safer than evacuating them onto the streets.

Where evacuation may be required, the evacuation response may differ to that of a fire. For example, people may be directed to specific exits or to avoid a particular route or area. For this reason, it is suggested the activation of the fire alarm to initiate evacuation should be avoided to reduce the possibility of an incorrect response.

Public Address (tannoy) systems, if available, may provide more flexibility to provide information and instructions appropriate to the scenario and to provide positive confirmation to staff and visitors that the emergency is real. This will help to reduce any potential delay in response.

In addition to the threat from items emplaced within or in close proximity to a building or site, the organisation should also consider whether there is a risk of personnel being targeted at, or on their way to, any assembly point(s) used in the event of an evacuation. Where this is a concern, regular searches of assembly points and evacuation routes should be considered. Staff should be encouraged to be particularly vigilant during evacuations.

Beware of secondary devices. If possible, a search of any muster point should occur, using dogs and trained responders.

Review Evacuation, Invacuation and Lockdown procedures, ensure that you have plans for vulnerable staff and visitors (as well as designated marshals to support this activity). Ensure external activity does not impact upon evacuation routes, assembly areas, exits or entrances.

Administration

The appropriate policy and procedures should mention the evacuation of your building, how this is achieved, the location of the external assembly areas, and the routes to be used to get to these

areas. Identify ownership of the information sharing process with other organisations, what records are kept, and how its effectiveness is assured. For large organisation, there should be a senior manager responsible for the strategic issues, and a more junior manager should sit under them who will oversee tactical/operational level issues. For smaller organisations, these roles could be combined and undertaken by one person.

It will be necessary to ensure all staff understand processes and procedures to be adopted, and how this looks when working with staff from other businesses.

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 key vulnerabilities or situations, and how these should be mitigated against. 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.

By joining up resources with neighbouring businesses and contacts, you enhance 'perimeter' security and therefore strengthen risk management protocols. In addition, this provides an enhanced response regarding potential 'grey space' that exists between buildings.

Communications

Internal Stakeholder Engagement:

The general principles of undertaking an emergency response and how this is to be achieved should be shared with all staff, and they should be briefed on what to do in the event of the above circumstances. However, for certain parts of the planning activity, such as radio codes used, or specific assembly site locations, you may decide to keep this information amongst those who will be involved in implementing the process and need to know. The location of assembly areas is the type of information terrorists would be seeking, in order to potentially place secondary devices at these locations.

It is necessary to ensure points of contact for evacuating the premises are known to staff internally,

and partners externally. Internal communications should 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 regarding your evacuation processes is essential to making the system work. However, you may decide to keep sensitive parts of your evacuation plans within your own organisation.

Early identification and engagement with key external stakeholders is 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 security 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:

Specific engagement with the media regarding evacuation processes and specific evacuation related information is not recommended. However, more general engagement with the media should be encouraged to allow a positive and deterrent message to be disseminated to the general public, as part of a Security Minded Communications strategy. By positively reinforcing a security deterrence message, it is likely that this may deter potential attackers when they carry out online hostile

reconnaissance as part of the attack planning process.

Health and Safety/Other Legal Issues

Any actions carried out regarding the evacuation of your building may be governed by legislation, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- The Fire Safety Order 2005
- The Fire (Scotland) Act 2005

It is important to consider any change to security processes and/or activities with regards to justification, proportionality, necessity and legality.

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, which involve the evacuation of your building. Records will provide evidence to any 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.

Such changes that affect visitors, contractors and the organisation must include consideration of your organisations insurance policies. This is especially relevant when looking at evacuation. If one or more of your staff members are injured while following evacuation guidelines, there needs to be a clear understanding of where liability lies, and what the insurance implications are in this event.

Consideration must always be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
IMPROVISED EXPLOSIVE DEVICE
IEDS
EMERGENCY PLANNING

SUSPICIOUS ITEM

EVACUATION

CBR