ProtectUK

Tactic RB3: Ensure that lockdown procedures are known, tried and tested

ProtectUK publication date
14/12/2023

Information and Intention

In the event of a terrorist attack, you will be faced with a number of options to keep your staff and other members of the public safe. One of these options is to instigate a lockdown of your premises. This involves locking doors and other physical barriers (such as turnstiles) to restrict entry to and/or exit from a site, or one or more zones within a site. It is sometimes referred to as ‘dynamic lockdown’.

The aims of lockdown are to reduce the immediate threat of harm by:

- Delaying attackers’ progress in finding and killing victims.
- Preventing people inadvertently putting themselves into the path of the attacker.

Lockdown may be implemented in many ways. It is important when discussing lockdown with others, to clarify exactly what is meant. A poorly implemented lockdown can actually increase the risk to personnel and members of the public.

Guidance is provided on the ProtectUK website: Evacuation, invacuation, lockdown, protected spaces

Additional guidance is also available in NPSA publication: MTA Supplementary Guidance: Lockdown

Guidance is provided at a ‘generic’ level due to the diversity in size and types of venues the guidance will apply to. It should state what the tactic deployed is intended to achieve and the parameters of such deployment.

NPSA have also produced an animation which discusses the application of lockdown at sites and the

complexities of lockdown management. It contains the key principles and considerations required regarding a dynamic lockdown.

Method

When deciding whether and how lockdown would function in the event of a terrorist attack, your organisation should consider:

- The impact a lockdown could have to reduce casualties.
- The risks of a lockdown increasing casualties.
- What form a lockdown would take.
- What type of lockdown could be technically achieved for your site using its existing systems.
- Under what circumstances lockdown should, or should not, be instigated.
- Any investment required in infrastructure to enable lockdown.

Lockdown procedures should be developed, tested, and refined to ensure that they will protect people as intended. Keeping records of what you are aiming to achieve with lockdown and why, how it will be implemented, procedures to be followed, and the outcomes of tests and rehearsals will assist your planning and refinement process.

The planning should:

- Identify all access and egress points within both the public and private areas of the site. Access points may be more than just doors and gates.
- Identify how to quickly and physically secure access/egress points. Consider both the design of the locking device at these points and whose role it would be to secure them.
- Identify how lockdown can be quickly reversed should the need arise (such as in the event of fire).
- Identify how to disable lifts without returning them to the ground floor.
- Identify how to stop people leaving or entering the site and direct people away from danger.
- Identify how your site can be zoned to allow specific areas to be locked down.
- Include staff roles and responsibilities and train staff in these.
- Processes need to be flexible enough to cope with and complement evacuation, invacuation and movement to protected spaces.

Dynamic lockdown, especially during the ingress phase of an incident, may lead to people being ‘locked outside’ and more vulnerable to the perceived threat. However, allowing continued ingress may permit the threat to enter the venue and make those inside more vulnerable. Each case must be

assessed on the information known at the time. Good internal and external information, and communications systems, are crucial.

Administration

Lockdown procedures should be developed, tested, and refined to ensure they will protect people as intended. This should form part of an Emergency Response Plan, designed using the ‘deter, detect, delay’ principles. The aim of the plan is to minimise casualties in the event of an incident.

As part of lockdown procedures, route assignments, such as floor plans, workplace maps and protected/safe or refuge areas should be included. Further details of what should be included in an Emergency Response Plan can be found on ProtectUK.

Keeping records of what you are aiming to achieve with lockdown and why, how it will be implemented, procedures to be followed, and the outcomes of tests and rehearsals will assist your planning and refinement process.

Risk Assessment

A risk assessment should identify threats which could have an impact on the business and its vulnerabilities. Organisations must complete a risk assessment when considering a dynamic lockdown. A lockdown can reduce the risk to people in the event of a terrorist attack. However, consideration must also be given to the risks to people which are caused by lockdown. Necessary adjustments should be made to reduce this risk.

Such risk assessments should clearly define organisational as well as individual duty of care to staff and others. Legal obligations, such as compliance with fire safety legislation, may be at odds with lockdown requirements. These conflicts can be resolved, but they must be carefully managed by considering immediate threats to life and whether taking a particular form of action is likely to increase or reduce the number of lives lost. You should consult with your organisation’s legal and safety departments, as well as your local fire service.

Communications

Internal Stakeholder Engagement:

In the event of a lockdown at your site, it is essential that this information is communicated to staff and others present, and that they know what to do in such an eventuality. Staff should understand when lockdown is initiated (typically achieved using announcements), and the circumstances in which this would take place. In addition, they should understand when it is cancelled, and the process

involved in this. Alternative methods to public announcements should also be considered.

Staff with the authority to initiate lockdown should be identified. The integrity of the lockdown should be monitored, and the effectiveness of announcements made should be recorded.

Dedicated channels should be established, with backups if access to the organisation's intranet or message channels is limited, 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:

It is important that your response plan is co-ordinated and compatible with those of your neighbours, particularly if you rely on a shared space.

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 and approval.

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 dynamic lockdown 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
- 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 relating to the lockdown such as decisions made, and the reasoning behind those decisions. Records will provide evidence to any investigations, coroner's enquiries and 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. Consideration must always be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
EMERGENCY PLANNING
EVACUATION
COMMUNICATIONS
SECURITY
ATTACK