Tactic VB2: Review patrol and positioning of security staff

ProtectUK publication date
14/12/2023

Information and Intention

Physical security is important to consider when protecting against a range of threats and vulnerabilities, including terrorism. When planning the introduction of any physical security measures, it is imperative both safety and emergency responses are considered.

A strong security culture within your organisation, beginning with senior management, will assist your guardforce to prepare, disrupt, and respond effectively should an incident occur. It is therefore recommended that your security guardforce:

- Understand the importance of situational awareness.
- Understand how to identify hostile reconnaissance.
- Communicate effectively.

Respond effectively, and with confidence, when responding to suspicious items, bomb threats and major incident.
It is important that patrol regimes for sites and events look beyond the business/organisation perimeter before, during and post-event. To the observer, these patrols should be unpredictable. This will complement any security minded communications already in place to deter those conducting hostile reconnaissance. Supervisors are key to ensure high levels of vigilance are maintained throughout the life cycle of an event.

Method

Routine searching and patrolling of premises represents another level of security and may cover both internal and external areas. Ensure that patrols are carried out regularly, but at unpredictable times. Staff must have clearly defined roles and responsibilities which are linked to clear policies and

procedures for them to follow. Such measures must be underpinned by training, rehearsal and exercising.

For more information see: Personnel security training and good practice.

The following elements should be considered in order to deliver an effectively trained, security-minded workforce:

- Training should be based upon your current policy and standards.
- Organisational training requirements should be based on an assessment of risk and the existing skills of your workforce.
- Training and leadership should be provided for supervisors in order to facilitate ongoing staff development. This will assist in ensuring people understand their roles in the event of a security incident and that all staff receive initial training and timely refresher training.
- Training plans should look 12 months ahead, building in a timeline for initial and refresher training.
- Training activity should be flexibly delivered in various formats, including within a formal classroom setting, online (internal or external to the workplace), practical scenarios or face-to-face briefings. We all learn differently.
- Staff should be trained before you put them through rehearsal and validation exercises.
- Counter terrorism (CT) awareness training should be included as part of your organisation's induction programme. This could be in the form of ACT Awareness e-Learning or, for larger organisations, may involve input from a local Counter Terrorism Security Advisor (CTSA).
- Security awareness should be included on your staff induction day. Set out your expectations as an employer from the commencement of employment and create a strong security and positive reporting culture within the organisation.
- Briefings and organisational security updates should be provided to all personnel. This may be supported through your organisation's intranet site (if available). If the security update/briefing involves a change in security policy, it is essential that details of staff being provided with this change are recorded either physically or electronically.
- Training should be provided on a continuous basis to prepare staff.

Importantly, all training undertaken by staff should be accurately recorded (and signed off when undertaken) in staff personnel/training records. Refresher training dates should be identified and adhered to.

Administration

Policy and procedures should mention security patrols and positioning of security staff, should the

threat level be raised or following an incident. You should also identify ownership for the management of the security staff, their deployment and patrolling regimes. This includes the maintenance of relevant records. Ensure staff understand processes and procedures to be adopted, including actions and contingencies.

Keeping records of what you are aiming to achieve through security patrols and positioning of security staff, how it will be implemented, procedures to be followed, and the outcomes of tests and rehearsals will assist your planning and refinement process.

It is important all staff with security responsibilities understand their roles and are properly tasked, trained and participate in regular exercising. Regular briefings should include Standard Operating Procedures, a clear explanation of lines of command and emergency procedures.

Security supervisors are key to a motivated, effective, and high performing guardforce. Effective leadership demonstrated by individuals during recent terrorist attacks have saved lives.

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 actions that are required regarding the deployment of, and patrolling by, security personnel. Such risk assessments should clearly define organisational as well as individual duty of care to staff and others.

For terrorist-related incidents, reputational damage will be caused if the organisation handles the issue badly, for example, communicating insensitively, poorly, or not at all. In addition to reputational risk, a failure of security and successful exploitation of vulnerabilities by terrorists could lead to loss of life or serious physical damage to the site and these risks must also be acknowledged. It is important to record current and emerging risks, risk management and mitigation measures, reminding those under your charge of their duty of care to themselves and others.

Communications

Internal Stakeholder Engagement:

Certain aspects of security patrolling and deployment at your site may not necessarily be communicated to all your staff. However, staff members should be encouraged to identify, and briefed on how to report, suspicious activity.

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

All security management/security staff should understand where security staff should be positioned and what the patrolling procedures are. Internal communications should encourage security awareness by general staff and a positive security culture should be encouraged through internal communications.

You must provide 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 wish these individuals to communicate 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 include basic information regarding the security workforce deployment if it impacts on neighbours. However, specific information on security guarding should not be shared externally.

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 plan, and consideration should 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:

Engagement with the media should be limited regarding patrol and positioning of security staff, as possession of this information could be of benefit to potential attackers. However, a general message relating to the fact that security staff are vigilant and always on patrol can positively reinforce a security deterrence message. It is likely that this may deter potential attackers when they carry out

hostile reconnaissance as part of the attack planning process.

Health and Safety/Other Legal Issues

Businesses/organisations that are operating security patrols and deploying security personnel 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

It is important to consider any security patrolling and deployment 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 security patrolling and deployment. 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.

Security positioning and patrolling must include consideration of relevant legislation as well as details of your organisations insurance policies. Consideration must be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
SECURITY
HOSTILE RECONNAISSANCE
STAFF
AWARENESS
TRAINING