ProtectUK

Tactic IB2: Ensure that staff are briefed in observing, detecting and responding to suspicious activity

ProtectUK publication date

14/12/2023

Information and Intention

The information gathered from people, places and websites is typically used by hostiles to assess the state of security and likelihood of detection, to assess vulnerabilities in security, and to assess likelihood of success. These commonalities in information requirements mean that measures put in place to disrupt hostile reconnaissance can be effective over a wide range of threats. Physical hostile reconnaissance is a key part of this process.

Understanding hostile reconnaissance/suspicious activity and the attack planning process gives security managers and staff a crucial opportunity to disrupt the hostile in two main ways:

- Denying them the ability to obtain the information they need from their research because they simply cannot obtain it, or they could but the risk of detection to achieve this is too high.
- Promoting failure, both of their ability to conduct hostile reconnaissance (they will not be able to get the information, they will be detected) and of the attack itself.

These effects can be achieved because in the process of conducting hostile reconnaissance the hostiles are making themselves vulnerable to detection.

Protective security strategies can therefore be focussed in the following manner to:

- **DENY** the hostile the opportunity to gain information.
- **DETECT** them when they are conducting their reconnaissance.

- **DETER** them by promoting failure through messaging and physical demonstration of the effective security.

This approach will play on the hostiles' concerns of failure and detection. For more information, see NPSA - Disrupting Hostile Reconnaissance.

Staff Briefing is a critical element in raising awareness of hostile reconnaissance and suspicious activity by individuals at your premises and the message must be reinforced regularly amongst staff.

Method

One of the most effective measures to deter terrorists and wider criminality is a competent security guard force who appear 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.

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.

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, to inform your staff what suspicious activity may look like. Encourage them to trust their instincts and report anything suspicious immediately to the 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.

In addition to briefing staff regarding observing, detecting and responding to suspicious activity, and being aware of their roles and responsibilities, 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 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.

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 delivered to staff is done with the normal shift briefing process, 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.

Administration

Policy and procedures should mention staff briefing being used as a tool to observe, detect and respond to suspicious behaviour should the threat level be raised or prior to/following an incident. Identify ownership of the responsibility 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 vulnerabilities. This risk assessment can be used to define the actions that need to be carried out, either to prevent them occurring or to detect the behaviour or those responsible if they have already been carried out. 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.

Communications

Internal Stakeholder Engagement:

The business or organisation should consider how to communicate effectively with their staff on incidents of suspicious activity/hostile reconnaissance which have occurred on the premises. Staff briefings should communicate the importance of 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.

Dedicated communications channels should be established, with backups if access to the organisation’s intranet or message channels is limited (e.g. if the intranet is restricted due to criminal investigations), 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:

Engagement with neighbouring businesses should be on a regular basis and should be constructive. The sharing of information with neighbouring businesses and contacts regarding suspicious incidents is desirable, as the individual(s) involved may be undertaking hostile reconnaissance in neighbouring businesses as well.

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:

Detailed information relating to an incident of hostile reconnaissance or suspicious activity should not be communicated directly to the media or external audiences without prior consultation and agreement with the police (there may be an active investigation ongoing). In addition, avoid revealing details about the incident through social media without prior police consultation.

After an instance of hostile reconnaissance has occurred and been reported to the police, an appropriate individual should be identified in the organisation to liaise with the police in order to disseminate approved information, which is accurate, and would assist any criminal investigation.

However, 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 and demonstrating a collaborative security approach between businesses, 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

Businesses/organisations that are operating a system for reporting suspicious activity/hostile reconnaissance 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 the operation of a system for reporting suspicious activity/hostile reconnaissance 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. 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.

Such changes that affect 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
HOSTILE RECONNAISSANCE
SUSPICIOUS ACTIVITY
RISK ASSESSMENT
SECURITY MINDEDNESS
SUSPICIOUS BEHAVIOUR