ProtectUK

Tactic IB3: Ensure that any suspicious activity is reported in a timely manner

ProtectUK publication date
14/12/2023

Information and Intention

Organisations face a variety of threats, be it from terrorists, hostile state and corporate espionage or criminals who are scrutinising potential targets. Irrespective of their aims, hostiles are united in their desire to succeed.

By using online research, on-site visits and, on occasion, insider knowledge, the hostile will seek to obtain sufficient and detailed information to carry out their attack. Hostile reconnaissance is the information gathering phase by those individuals, or groups with malicious intent, and is a vital component of the attack planning process.

Understanding hostile reconnaissance 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.

Suspicious activity/hostile reconnaissance can be identified in 3 ways:

- It can be reported to a staff member by a member of the public.
- It can be observed directly by a member of staff.
- It can be identified by surveillance using the CCTV system.

However, it is not just about taking the report and dealing with the person reporting, but it is also

about how that report is dealt with by the organisation. Unless staff know how to respond to, and deal with, a report of suspicious activity from the public, the public's vigilance will be limited in effectiveness.

Staff need to know how to escalate a report of suspicious activity to their manager, security and the police. They also need to know how to respond to the member of the public who has taken the time and effort to report.

However, staff members themselves also need to proactively look for anything they see in and around the site that might give them cause for concern. It is people that work at the site regularly that are the most likely to notice anything out of the ordinary. Whichever route is used to elicit information, there needs to be feedback on such reporting to instil confidence and trust. This will serve to further promote and enhance a positive security culture.

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 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 effective security.

Method

In managing the reporting of suspicious activity at your venue, a system known as the '3 Cs' can be employed. These are:

- Contact – knowing how/where to report.
- Confidence – that something will be done about it.
- Convenience – belief that reporting will not be inconvenient.

In addition, if you provide people with a range of reporting mechanisms (e.g. phone, email, SMS) they will be more likely to act.

Two essential actions staff should take if someone reports something suspicious to them are:

- Escalate it to their manager and security/police immediately.
- Acknowledge the person reporting for coming forward and to say 'thank you', e.g. "Thank

you for taking the time to report this to me. I will pass this on immediately to our security personnel/control room". Saying thank you for reporting is vital for building confidence in the member of the public who has taken the huge step to report.

The 'See it, Say it, Sorted' campaign employed in the rail transport sector is an extremely effective way of encouraging the public to report any suspicious activity immediately. Posters are displayed on trains and in railway stations encouraging the public to report suspicious activity immediately. This type of active campaign could potentially be adapted for other organisations, as the most critical aspect of detecting suspicious activity/hostile reconnaissance is the immediate reporting, so that security staff or the authorities are able to check out the individual(s) involved in the activity.

This poster campaign can be backed up by the use of tannoy messages, which encourage the public to report anything that does not look right. The wording is not alarmist, but it engages well with the wider public.

The use of internal communications is also important, and it can be used to communicate these messages to internal audiences. Staff can be the 'eyes and ears' for the organisation and the campaign messages are equally appropriate for them. It has been found that the public are likely to report to staff who are not necessarily security professionals (e.g. staff working behind the bar at a concert venue). It is therefore important to ensure all public facing staff are clear about what to do if the public report suspicious activity or unusual behaviour to them. See NPSA - Promoting public vigilance and reporting at sites for more information.

Guidance should also be reinforced to staff on what immediate actions they should take if suspicious activity is reported to them, or if they observe suspicious activity. If the suspect(s) are still on the premises, consideration should be given to approaching them and engaging them in conversation. This has several benefits, namely it shows that the security personnel on your premises are pro-active in their approach to security and this in itself could potentially deter further hostile reconnaissance activity.

It also allows the individuals to be better identified and their explanations can be verified. However, any approach should be considered from a personal safety perspective, as there is always the possibility for the individual to be argumentative or violent.

Once a report of suspicious activity is made to a staff member, or the staff member witnesses this activity themselves, it should be escalated to a supervisor and the control room, as the CCTV operators could potentially record the individual on CCTV. If deemed appropriate, the police should also be contacted.

A report should be completed regarding the incident, and this should be retained with the relevant

manager with responsibility for managing incidents of hostile reconnaissance and suspicious activity. The incident should thereafter be incorporated into shift briefings and potentially disseminated electronically as well.

Administration

Policy and procedures should refer to ‘Reporting of Suspicious Activity/Hostile Reconnaissance’. This practice should be encouraged at all times and not only when the threat level is raised, or following an incident. Identify ownership for the management, coordination and strict compliance of the reporting process, together with the relevant record keeping, and how its effectiveness is assured.

Ensure staff understand processes and procedures to be adopted, including receiving and recording a report of suspicious activity and escalating this report through the organisational chain of command.

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 should be taken to challenge individuals acting in a suspicious manner and to disrupt any potential hostile reconnaissance activity that is being carried out.

In addition, it should include the process in place to report such activities to the police and the management of this information. 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 ensure that suspicious activity within their premises is reported at the earliest opportunity. Staff briefings should communicate the importance of why such activities should be identified, responded to, and reported as soon as possible in order disrupt any potential hostile activity.

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 on 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 or policy frameworks, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- 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 organisation’s insurance policies. Consideration must always be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
SUSPICIOUS ACTIVITY
REPORTING
CCTV

HOSTILE RECONNAISSANCE

SECURITY

DETER THREATS