Tactic IB4: Implement communication links with surrounding premises to pass on information and suspicious activity

ProtectUK publication date

14/12/2023

Information and Intention

Strong relationships should be cultivated at all levels within a business, and with external stakeholders including contractors, suppliers, local authorities, the police and other emergency services, community groups and nearby businesses. The NPSA has developed a document which provides guidance in relation to Crisis Management for Terrorist Related Events.

However, it is a good idea to look beyond the organisation and the crisis team in order to build sustainable relationships with nearby residents or businesses. They will also be affected in the event of an attack and may look to your organisation for guidance and reassurance.

Creating target hardened environments is one way of managing the threat from terrorist attack, and this can be achieved by neighbouring organisations working together to share threat-related and other information. This can be achieved slow-time via bulletins and circulars, and quick-time through radio communication or telephone contact.

The ultimate aim is to ensure that organisations are doing all they can to deter potential hostile actors from targeting them and are fully prepared if an incident does happen.

Method

To achieve the aim of implementing communication links with surrounding premises in order to pass on information and instances of suspicious activity, it is necessary to build up mutually beneficial communication arrangements with neighbouring organisations.

If existing ‘business watch’ bodies or crime prevention groups are already established, these could form the basis for your communications and information sharing network. If such bodies do not exist, then approaches will need to be made to other neighbouring organisations and some form of communications forum requires to be established.

A major concern for many organisations is the improper and unauthorised sharing of information, and the potential punitive penalties that could result from such actions. This may deter certain organisation from sharing information or intelligence with others. In order to overcome this difficulty, an Information Sharing Protocol and Memorandum of Understanding should be created and signed by all participants.

The sharing of information and intelligence needs to be controlled and it is necessary to validate any information/intelligence that is being shared with other organisations. A single point of contact should be identified who will control and coordinate any information sharing activities. Physical records should be kept of the information passed along with any results arising from this information sharing process.

Information regarding incidents can take two forms. Firstly, the information can relate to something that happened some time before, where the suspicious person or offender is no longer there. The second set of circumstances is where the suspect is actually present and carrying out some form of suspicious activity at that time. In this case there is an urgency in tracking down the individual and speaking to them to confirm the situation.

Where a suspicious person is no longer present, information regarding them could be passed via a written communication throughout the information sharing network. In the case of a suspect still being present, radio instructions should be sent to security personnel to challenge them and establish the reason for their behaviour.

Many businesses are members of crime prevention radio networks where different businesses have the ability to communicate with each other on various radio frequencies.

Additionally, it would be helpful if a managers' forum was created, where managers from each of the businesses in the area met and discussed security related issues.

Administration

The appropriate policy and procedures should mention the establishment of communication links with other premises and how this is managed. 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, including how to go about reporting suspicious activity or other serious issues.

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.

Communications

Internal Stakeholder Engagement:

The relevance and sensitivity of information coming from the multiple business communications networks should be considered and shared with appropriate staff members. Staff should also be briefed on what to do should they observe suspicious activity, and they should be encouraged to identify and report any suspicious activity they observe, or that they know about.

It is necessary to ensure points of contact for the communications network 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 suspicious persons or circumstances is essential to making the system work.

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 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:

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.

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

Any actions carried out regarding the communication of information relating to suspicious activity 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
- General Data Protection Regulation (GDPR)

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 sharing information regarding suspicious activity with other businesses. 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.

KEYWORDS
CRISIS MANAGEMENT
RISK ASSESSMENT
AWARENESS
SECURITY
ATTACK