ProtectUK

Tactic EB2: Join up resources with neighbouring businesses and contacts

ProtectUK publication date
14/12/2023

Information and Intention

Joining up resources with neighbouring businesses and contacts can improve your protective security and preparedness to deal with an incident. In addition, after an incident has occurred (such as a terrorist attack), businesses could potentially offer their premises as shelter for injured persons from their own or adjacent premises or provide space/services as part of Business Continuity Management, should one business become unavailable due to the incident.

Such a collaborative approach makes areas ‘target hardened’ to threats, provides a deterrent effect to hostiles and provides opportunities to enhance resilience. This can be reinforced using security minded communications.

To be employed successfully, there is a need for close cooperation with the police in order to obtain relevant and up-to-date intelligence regarding threats and terrorist related incidents.

Method

It is recommended that businesses/organisations make arrangements to join up resources in advance of any change to the threat level, intelligence or incidents.

Joining up resources can include:

- Rotating and sharing external patrols with other security companies.
- Widening patrol areas.

- Ensuring response plans are co-ordinated and compatible with those of your neighbours, particularly if you rely on a shared space.
- Co-ordinate communications so that neighbours can be notified, in quick time, that an attack is underway. Speed is of the essence.
- Developing a joint communication system to use with neighbours in the event of a major incident (similar to the City of London Bridge Call).
- Share counter terrorism training opportunities with neighbouring businesses.
- Test and exercise jointly, with resources from neighbouring businesses also involved.

It is necessary to ensure arrangements are reviewed at pre-agreed intervals.

Administration

The appropriate policy and procedures should mention the joining up of resources with neighbours, in the event of a raised threat level or a terrorist incident, and how this is managed. Identify ownership of the information sharing process with other organisations, what records are kept, and how 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, and how this looks when working with staff from other businesses.

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.

By joining up resources with neighbouring businesses and contacts, you enhance 'perimeter' security and therefore strengthen risk management protocols. In addition, this provides an enhanced response regarding potential 'grey space' that exists between buildings.

Communications

Internal Stakeholder Engagement:

Unless the information is particularly sensitive or involves personal data, all relevant information relating to the pooling of resources with neighbours in the event of a raised threat level, or in response to a terrorist incident should be shared with your staff members. Staff should also be briefed on what to do in the event of the above circumstances.

It is necessary to ensure points of contact for liaison with other neighbours 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 the pooling of resources with neighbouring businesses and contacts 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 also be given to engaging with any working groups or fora 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 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 joining of resources with neighbouring businesses and contacts 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
- 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 of the issues, decisions made and the reasoning behind those decisions, which involve the joining of resources with neighbouring businesses and contacts. 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.

Such changes that affect visitors, contractors and the organisation must include consideration of your organisation’s insurance policies. This is especially relevant when looking at combining your resources with neighbours. If one or more of your neighbour's staff members are injured while performing a joint activity, there needs to be a clear understanding of where liability lies, and what the insurance implications are in this event. Consideration must always be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
MAJOR INCIDENT
SECURITY
COMMUNICATIONS
HEALTH & SAFETY