Tactic DB9: Restrict and only accept deliveries that are essential

ProtectUK publication date

14/12/2023

Information and Intention

Like postal and courier deliveries, bulk deliveries (e.g. office, catering and cleaning supplies) can provide a means for getting explosives, weapons and other threat items through a site's secure perimeter.

While bulk deliveries share some similarities to the challenges posed by postal and courier deliveries, there are also some significant differences.

Bulk deliveries (as their name suggests) will tend to be large, offering space for the concealment of larger explosive devices or larger weapons/quantities of ammunition. Their size and shape may make deliveries difficult to search efficiently and effectively.

Method

Consider processing all incoming mail and deliveries at one point only. This should ideally be off-site or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the building.

Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual deliveries. Checking the drivers' and vehicles' credentials and turning away unexpected deliveries, may significantly reduce the risk.

Measures may include only accepting expected deliveries (e.g. matching delivery to a specific purchase order number; checking the consignment broadly matches the order/delivery note (e.g. correct number of boxes or pallets); checking delivery for signs of tampering or damage; delivery on a certain day or within a time window; known delivery vehicle and/or driver) for more thorough assurance of the supply chain.

Administration

There should be a policy developed that caters for the searching, screening and control of deliveries on to the business premises. This should be led by leadership in partnership with the person with responsibility for security.

The appropriate policy and procedures should mention the restriction and acceptance of deliveries to only those that are essential in the event of a raised threat level, or in response to a terrorist incident, 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, and how this looks when working with staff from other businesses.

Risk Assessment

All activity relating to mail handling and deliveries should be risk assessed in line with existing business/organisational policies.

There should be the capacity to turn away unwanted vehicles (i.e. a rejection lane where available).

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:

Unless the information is particularly sensitive or involves personal data, all information relating to the restriction and acceptance of deliveries to only those that are essential 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 business and contacts 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 that you want 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 associated businesses and contacts should be on a regular basis and should be constructive. The sharing of information regarding the restriction and acceptance of deliveries to only those that are essential is important to making the system work.

Early identification and engagement with key external stakeholders is also crucial. Local organisations whose sites are nearby, or have shared use of the site being protected, are 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 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 restriction and acceptance of deliveries to only those that are essential may be governed by legislation, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts

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.

KEYWORDS

DELIVERIES

RISK

STRATEGIC

STAFF

THREAT