ProtectUK

Tactic DB10: Scan all mail and ensure that postal procedures are robust

ProtectUK publication date
14/12/2023

Information and Intention

Postal and courier services have long been an attractive target for terrorists. With most businesses receiving a large amount of mail and other deliveries, these routes offer a potential means of gaining access to a site or building, or delivering a hazardous item to a target recipient.

Possible contents of concern are detailed on the Screening Mail and Courier Deliveries page.

It is important to understand all of the routes by which post is received and ensure that urgent items do not circumvent the system.

Method

All incoming post (including courier and hand delivered items) should be channelled through a post room or other screening systems. Make sure all sources of incoming mail are included within the overall screening process. 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.

A basic but extremely worthwhile level of protection can be achieved by post room staff looking out for suspicious items, or better still inspecting each item briefly. Post room staff should be well aware of the possible indicators that a delivered item may be of concern, and the appropriate action upon discovery of any suspicious delivered item. Indicators of suspicious deliveries or mail are listed on the Mail Handling page of ProtectUK.

Clear procedures should be in place that set out the actions to take, in the event that a suspicious

item is discovered during a search. These are likely to include a resolution procedure, an escalation procedure and an emergency response procedure, with the exact steps to be taken depending on the nature of the item discovered, its location, and the context in which it is found. All personnel involved in carrying out searches or responding to any such incidents should be fully aware of these procedures.

Administration

The appropriate policy and procedures should mention the intention to scan all mail and ensure that postal procedures are robust, especially in the event of a raised threat level or a terrorist incident. Policies and procedures should also clearly outline roles and responsibilities and the management of any screening processes.

You should identify ownership of all information sharing processes including those with other organisations. You should also identify what records are kept and how the effectiveness of any arrangements are 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

Consider the organisational response should there be any changes to the organisation’s risk assessment or mail streams.

Make sure mail handling areas can be promptly evacuated. Rehearse evacuation procedures and routes as well as communication mechanisms which would be used throughout the incident.

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 scanning of all mail whilst ensuring that postal procedures are robust 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.

Make sure that all staff who handle mail are briefed and trained how to recognise and respond to the threats the organisation faces, and the possible indicators of concern. Include reception staff and encourage regular correspondents to put their return address on each item, and in particular to provide advance warning of unusual items to help reduce false alarms. Ensure that staff are aware of the usual pattern of deliveries and to be briefed of unusual deliveries.

It is necessary to ensure points of contact for liaison with other businesses 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 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 associated businesses and contacts should be on a regular basis and should be constructive. The sharing of information regarding the scanning of all mail whilst ensuring that postal procedures are robust 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 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

Businesses/organisations should ensure that all mail handling procedures are assessed in line with Health and Safety and other legal/policy frameworks, such as:

- 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
MAIL HANDLING
EVACUATION
COMMUNICATIONS
BEST PRACTICE
SECURITY