ProtectUK

Tactic DB8: Implement a regular and unpredictable search sweep rota across site, including areas hidden from surveillance

ProtectUK publication date
14/12/2023

Information and Intention

The purpose of a search regime is to help reduce the likelihood of threats entering your site(s), and to help you detect threats that may already be present at your site, including areas hidden from surveillance. It should address a clearly defined operational requirement that reflects the current and emerging needs of your organisation and site(s).

When developing a search regime, it is important to understand the threats to your business. This will enable you to identify and mitigate risks more efficiently and effectively.

This tactic is designed to help you understand the purpose of having a search regime and focuses on:

- **People**: screening people and their belongings at entry points can help reduce the likelihood of explosive devices, weapons, hazardous or prohibited items or materials being brought into buildings or onto sites.
- **Vehicles**: screening vehicles and their contents at site entry points can help reduce the risk of explosive devices or weapons or people being brought onto sites.
- **Mail**: terrorists and others wishing to cause harm or disruption have long used postal and courier services to deliver hazardous items to target recipients.
- **Deliveries**: in a similar way to 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.
- **Buildings and Areas:** if the threat is already on your site, it is important to have an effective

search regime to detect any placed explosives, identify weapons, or people that may have hostile intent.

It is important to note that visible search measures may also serve as a deterrent to those with hostile intent. Therefore, it must be done regularly and in an unpredictable manner so that people that might want to cause harm do not understand and exploit your security search methods.

Method

Search Regime Overview:

Having a developed search regime for the organisation and your site(s) will allow you to implement and escalate your searching and screening in response to any threats. This regime will define what, where or who (e.g. visitors and contractors) is searched; what the aims of the search regime are; as well as establishing the authority for conducting it.

The regularity and scale of searches must be unpredictable, and should reflect the current threat, be proportionate to the risks faced by the organisation and site, and correspond with other security measures in place. It may be appropriate to implement a layered approach to the searches so that quick searches for large threats take place on the periphery of the site, with more detailed search procedures closer to critical areas or assets. Searches across the site should include areas hidden from surveillance.

Consider the health and safety of staff conducting the searches and of anyone being searched. If any tools or equipment are to be used to aid search, make sure they address a defined requirement, are fit for purpose, well maintained, and staff are effectively trained in their use.

All staff involved in carrying out searches should be fully trained in the site’s search procedures including escalation and emergency response procedures. They should also understand the aims of the search and the site’s specific detection priorities. As well as comprehensive initial training, staff should receive regular refresher training and be briefed if there are any changes to the search priorities or procedures. Where casual staff are used, it is particularly important that they are trained to understand the requirements and procedures at the specific site.

Search Regime Implementation:

Once implemented, the search process should be monitored and reviewed (regularly and in response to any incidents or changes) to ensure it continues to address the current threats and identified risks.

Criteria for searching buildings and physical locations differs to that of searching people, vehicles, mail, and deliveries.

For People

- Consideration should be given to the different groups of individuals entering the premises such as staff, visitors, contractors, or the public, and any different types of items they may wish to bring in. It may be considered appropriate, given differing risk profiles, for some individuals (for example visitors as opposed to credentialed staff), or different sizes or types of bags, to undergo different screening regimes.
- Consider the arrival rate of people and volume of possessions and assess how this demand might vary at different times of day, seasonally, or for particular events.
- Consider the space required and optimum location for the search process.
- Make sure the search process is aligned and integrated with other aspects of the entry process and that it does not interfere with emergency exits.
- Make sure the search area has the necessary infrastructure (e.g. power, lighting, tables and shelter).
- Provide prior notification about the search process (and any items that are prohibited from the site) and communication to people as they approach to encourage them to prepare, which can help reduce delays and maximise visitor flow.

For Buildings

- The overall objective is to make sure that the entire area, including grounds, are searched in a systematic and thorough manner, so that no part is left unchecked.
- Consider dividing the site or venue into manageable sectors for searching.
- It may be appropriate to define different search regimes for different areas or sectors, for example searching critical areas of a site more frequently than other areas.
- Ideally, searches should be conducted in pairs to make sure searching is systematic and thorough.
- Test and exercise your search process regularly and learn from the outcomes.

- If evacuation is considered or implemented, then a search of the assembly areas, the routes to them and the surrounding area should also be considered where possible.

For Vehicles

- Identify if vehicle-borne improvised explosive devices (VBIEDs) are concealed within or under the vehicle (can include being concealed within personal belongings in vehicles).
- Establish if other weapons may be concealed (such as knives, firearms, liquids, etc.).

For Mail

- Understand indicators for suspicious deliveries or mail.
- Understand indicators for explosive or incendiary devices.
- Understand indicators for chemical, biological and radiological (CBR) threats.
- Establish what you would do upon discovery of any suspicious delivered item.

Administration

Clear polices will need to be in place that define what, where or who is searched, the aims of the search, and the authority for conducting it.

The appropriate policy and procedures should mention the implementation of a regular and unpredictable search sweep rota across site (including areas hidden from surveillance), 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 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

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 implementation of a regular and unpredictable search sweep rota across site (including areas hidden from surveillance) 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 implementation of a regular and unpredictable search sweep rota across site (including areas hidden from surveillance) 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

The Policy and Procedures within a business will detail the process for carrying out searches: building, people, vehicles, mail etc. This document must include the extent of searches and the relevance of the threat level on the searches – more extensive searches during an increased threat level for example.

Any actions carried out regarding the implementation of a regular and unpredictable search sweep

rota across site (including areas hidden from surveillance) may be governed by legislation, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Fire Safety Order 2005
- The Fire (Scotland) Act 2005
- The Data Protection Act 2018
- Employment Rights Act 1996

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 organisations insurance policies. Consideration must always be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
COMMUNICATIONS
VULNERABILITIES
BUSINESS