ProtectUK

Tactic DB2: Search immediate parking areas and review access to them

Information and Intention

An access control system is only as good as the procedures and the people that govern its use. To ensure the security of your site, you should consider the use of an access control checklist. This can help to enhance control of any immediate parking areas and help control access to them. Control can be further enhanced through application of a CCTV checklist, which will serve to assist identification of suspicious behaviour or hostile reconnaissance, well as post incident evidence gathering.

To be effective, access control systems require active management, as well as appropriately trained staff. This also includes the need for a good security culture which will help ensure your site remains secure whilst continuing to be accessible to your employees, visitors or customers.

Method

Following an increase in threat, Organisational Requirements (OR) should be implemented that enable the safe, systematic and controlled search of all (private and public) parking areas. This should be carried out by appropriately trained staff, under the control of the organisation, and in accordance with the information/intelligence provided. These searches can be conducted either overtly or discretely, but should be always be carried out in a way that maintains effectiveness and deterrence, whilst minimising risk and delivering reassurance.

The following should be considered:

- Specify what searches are intending to find (e.g. explosive or incendiary devices of at least a particular size; electronic devices posing an espionage risk) and how often they should be conducted.
- Decide on the appropriate response of your site. Establish if the threat is external or internal.

- Implement your emergency response plan, which may include evacuation, invacuation, lockdown and/or the use of protected spaces. Deciding upon and initiating evacuation, invacuation, lockdown and/or the use of protected spaces should be the responsibility of the identified lead individual. Access key checklists for procedures and key information that needs to be recorded.

- Open communications between your security team and centralised control room staff (if applicable).

- Report any suspicious activity to police immediately and alert people within the site/location. Do not wait for all the information before alerting the police.

- Locate, track and monitor intruders/hostiles (e.g. via CCTV) and communicate this to the police. They will require different information for different scenarios. The ETHANE model (see ETHANE checklist) may help staff communicating with emergency services about what may be required.

- Instruct staff, visitors and contractors on what they should do and where they should go. This direction could be directive or simply to leave the area by their nearest exit.

- Reduce the number of potential causalities by deterring or, where possible, preventing people/vehicles entering the parking areas or site. Clear communications will be the most critical part of the delivery of this element.

- Deal with any injured when it is safe to do so.

- Remember to record and justify key actions and decisions taken.

Simultaneously, you should review your existing access controls to parking areas, ensuring you know who and what is allowed to go where. You should allocate passes to reflect this, with access restrictions implemented as required. If you determine the need for vehicular access, you should:

- Assess how effectively existing barriers are able to delay and discourage attackers.

- Ensure existing barriers are configured to offer the longest delay possible.

- Understand what to look for in relation to defending against the identified threat.

- Ensure search procedures are consistent with the threat.

- Issue vehicle passes for vehicles requiring regular access.

- Ensure vehicles without passes that require entry do so with prior arrangement and confirmation of vehicle and occupant identity.
- Consider enhancing access control by application of Hostile Vehicle Mitigation (HVM).

Administration

Policy and procedures should mention the access, search and review of parking areas should the threat level be raised, or following an incident.

Identify ownership of the incident and governance of the search regime, as well as the review of access controls, including who is responsible for their management and coordination, what records are kept, and how their effectiveness is assured.

Ensure staff understand processes and procedures to be adopted, including action and contingencies (e.g. recovery of a suspect package; identification of suspicious behaviour; identification of suspicious vehicle).

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 the items that need to be detected – either to prevent them from entering the parking areas, or detect them if they have already been placed in the parking area. Risk assessments should clearly define a duty of care to staff and others on both an organisational and individual level. 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.

Communications

Internal Stakeholder Engagement:

Certain aspects of your search and review regime at your site may not necessarily be communicated to all your staff. However, staff members should be briefed on what to do should they observe suspicious activity or items, and they should be encouraged to identify and report any suspicious activity or item they observe, or that they know about.

It is necessary to ensure points of contact are known to staff internally, and partners externally. Any information regarding security planning and deployment should be disseminated internally through the communications function.

All security management/security staff should understand where security staff should be positioned and what the search and review procedures are. Internal communications should encourage security awareness by general staff and a positive security culture should be encouraged through internal communications.

You must provide 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 consider what messages you want them to share with 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 include basic information regarding the security workforce deployment if it impacts on neighbours. However, specific information on search criteria and review processes should not be shared externally.
Early identification and engagement with key external stakeholders are 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 the plan, and consideration should 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.

Under no circumstances should a suspicious item found during a search be touched or moved in any way; the police should be informed immediately and will ensure an appropriate response.

External Media Engagement:

Engagement with the media should be limited, and only undertaken when required. By making search procedures for car parks public knowledge, you could be providing valuable information to attackers on how to overcome the security at your site. However, if there are any traffic delays or congestion caused by the searching procedures at the car park, you should have a statement prepared for the media in case you are questioned about this.

Health and Safety/Other Legal Issues

Ensure compliance with the requirements of Health and Safety and other legal issues, 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 search and review 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 search and review processes. 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.

Search and review processes must include consideration of relevant legislation as well as details of your organisation’s insurance policies. Consideration must be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
EMERGENCY PLANNING
CCTV
ACCESS CONTROL
REPORTING
THREAT