ProtectUK

Tactic DB1: Close non-essential access and egress points

ProtectUK publication date
14/12/2023

Information and Intention

Whether your organisation is accessed by first entering via a perimeter or checkpoint, or immediately through the building itself, it is vulnerable to a wide range of hostile activity.

Access points provide channels for people, vehicles and materials to move through your organisation's perimeter. This will often be the first opportunity for you to project an impression to staff and visitors of both the business and the site security posture.

Where there is no external secure perimeter, the site or building is likely to be the first point of engagement with both clients and also adversaries. Therefore, it is extremely important to get the security requirements right, to ensure that vulnerability is kept to a minimum and that should an attack occur, its impact is minimised.

Effective mitigation against this broad range of threats requires a holistic approach to physical, personnel, procedural and cyber security. Indeed, when the threat increases, closure of non-essential access and egress points will enhance the effectiveness of your mitigation measures.

Method

Through the closure of non-essential access and egress points, your organisation may continue to operate effectively, even during periods of increased threat. As part of this process, you may wish to consider:

- Perimeter and/or checkpoints
- Reception Area
- Emergency Exits

- Goods & Delivery Areas - Bulk Delivery, Mail and Courier Delivery

By identifying and controlling essential access points, your organisation can continue to function, safely and securely, by ensuring staff and visitors adhere to documented Operational Requirements (OR). Such procedures can be enhanced through use of signage, CCTV and internal memoranda, each influencing positive organisational behaviour and enhancing the security culture.

Perimeter and/or checkpoints:

All perimeters will require points of access. This provides an optimal opportunity for authorised personnel to control access and secure your organisation's perimeter.

When seeking to control access, you should consider the following issues:

- Design of the access point to limit the vulnerability to reconnaissance and to minimise the effects of blast or other weapons.
- Surveillance, monitoring and lighting systems to support detection and tracking of hostile acts.
- Access control measures to permit the entry of authorised personnel and procedural control measures to permit the entry of vehicles, materials and deliveries.
- Search and screening of people, their belongings, vehicles, materials and deliveries.
- Hostile Vehicle Mitigation.
- Measures to protect employees and security staff from attack, including blast or ballistic resistant guard houses, body armour etc.
- Use of pedestrian perimeter barriers to support access control measures, permit the closure of the entry point when non-operational, or to reinforce security during certain threat scenarios (see also TACTIC DB2).
- Guarding and response force requirements.
- Emergency egress/access requirements e.g. evacuation (see also emergency exits below).
- Contingency requirements e.g. blocked entry/exit point.

Reception Area:

Reception areas are the point where all visitors, and in many cases the majority of staff, will enter a building. There is usually a corporate requirement to make these spaces welcoming and to ensure that they convey a positive image of the organisation to all. However, at the same time, they need also to fulfil the following security functions:

- Deliver a single area where surveillance can be undertaken.
- Provide a focal point for visitors to report, enabling credentials to be checked and authorised visitors to be booked into the building.
- Location for entry control(s) so that only authorised persons, either staff or visitors, can proceed beyond the reception area.
- If the threat level dictates, provide a space where additional measures such as screening of people and their belongings can be undertaken.

If a reception area does not usually contain search and screening equipment, it is important that suitable locations are pre-prepared to support rapid deployment of the capability when required.

Emergency Exits:

Emergency exits need to comply with local building regulations and the requirements of emergency services for evacuation of personnel while remaining secure. There should be additional surveillance and oversight at each location which may be supplemented by alarms and Intrusion Detection System (IDS).

Procedures must be put in place to ensure these do not become weak spots in the perimeter during either a site evacuation or during daily operation of the building.

Goods & Delivery Areas:

Bulk deliveries (e.g. office, catering or cleaning supplies) can provide a means for getting explosives,

weapons and other threat items through a site’s security 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.

Allowing suppliers’ and third-party deliveries on site can significantly increase the risk of prohibited items and weapons entering your site. Screening for these materials within your organisation’s perimeter can also increase the risk of harm to your business, employees and security personnel. You should therefore undertake off-site screening where possible. Where this is not feasible or appropriate, deliveries should be off-loaded and screened at the site perimeter.

Administration

In the event that the threat level is raised, or in the event of an incident, policy and procedures should mention the closure of non-essential access and egress points. You should identify ownership of the incident and governance of the decision making, including who is responsible for the management, coordination and strict compliance, together with the relevant record keeping, and how its effectiveness is assured. Ensure staff understand processes and procedures to be adopted, including action and contingencies e.g. mail handling, courier deliveries, receiving of visitors.

Risk Assessment

A risk assessment should identify threats which could have an impact on the business and its vulnerability. This risk assessment can be used to define the items that need to be detected – either to prevent them from entering the facility or detect them if they have already been placed in the building.

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 closing non-essential access and egress points at your site may not necessarily be communicated to all your staff. However, staff members should be briefed on what to do should access to non-essential access/egress points be closed.

It is necessary to ensure points of contact regarding this action are known to staff internally, and partners externally. Any information regarding closure of non-essential access and egress points should be disseminated internally through the communications function.

All security management/security staff should understand where security staff should be positioned and what the patrolling 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 full consideration should be given to the messages you wish to be conveyed to external networks, e.g. family and friends. Remember that social media is a potential area where this crossover may occur.

External Stakeholder Engagement:

Basic information regarding the closure of non-essential access and egress points should be provided if these measures have an impact on neighbouring businesses.

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.

External Media Engagement:

Engagement with the media should be limited, and only undertaken when required. By making access and egress arrangements public knowledge, you could be providing valuable information to attackers on how to penetrate the security at your site. However, if there are any traffic delays or congestion caused by closing access to non-essential access/egress points, 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

Your actions must be justified, necessary and proportionate to the threat you are facing.

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 closure of non-essential access and egress. 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.

Security positioning and patrolling 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 EXITS
EVACUATION
MAIL HANDLING
SECURITY
RISK ASSESSMENT