ProtectUK

Tactic VB3: Ensure that perimeter fencing and security lighting is checked

ProtectUK publication date
14/12/2023

Information and Intention

As detailed within ProtectUK Physical Security guidance, there should be measures in place to ensure that a venue or site can exercise a degree of control over the activities that take place within their property boundaries. Defensible space is created by deciding which areas around a property are public and which areas are private. Simply put, boundaries should clearly define the difference between public and private space. This is particularly important when challenging protests and unlawful activity.

The NPSA Operational Requirements process helps organisations make intelligent investments in security, enabling them to implement measures which are proportionate to the risks they face. By following the process, security managers and practitioners are able to assess, develop and justify the actions their organisation needs to take, and the investments they need to make, to exercise control over hostile activities and protect their critical assets against security threats.

Two areas which contribute to your protective security are fencing and lighting. However, there is little point in these measures if they are not routinely checked to ensure they remain operational and effective.

Fencing:

Fencing is often used as a perimeter, providing a line of demarcation; it is an important security measure, both for deterring criminal activity and enhancing safety. Once installed, it should be regularly checked to ensure that it is in good repair and fit for its intended purpose. Perimeter Intrusion Detection Systems (PIDS) may be used at the perimeter to alert security officers that the perimeter has been breached.

Lighting:

Security lighting plays an important part in any site's security regime. Good quality and well-planned lighting will fulfil a number of roles, including:

- Providing a deterrence effect.
- Increasing the uncertainty and vulnerability of an intruder during an intrusion.
- Enabling detection and verification via CCTV.
- Supporting a response force.

Method

To achieve success, a hostile will attempt to identify and exploit weaknesses within your protective security measures. The principles of Deter, Detect and Delay, supported by an effective response plan, will help to frustrate and disrupt any potential hostile.

Fences and walls provide only limited delay against a determined or skilled attacker. They can also be vulnerable to attackers if they are not correctly designed, installed or maintained.

Where applicable, organisations must ensure that perimeter fencing is checked, especially during times of increased risk. Where scaling of the perimeter is identified as a threat then 'toppings' can be utilised. These are designed to increase the difficulty of climbing a fence by snagging/entangling the intruder and providing additional deterrence when using barbed tape coil (BTC). A topping should not aid an intruder by providing a firm hand or foothold and must always be specified and installed in accordance with the relevant legal and safety standards.

It is recommended that the perimeter barrier is combined with additional security measures, such as security lighting, electronic surveillance e.g. CCTV and PIDS, electric/power fencing (which provides a deterrent and acts as a detection system) and regular patrols by the guard force. When developing the design of each of these measures, no one element should be treated in isolation. Instead, they should be treated as an integrated scheme that is designed to deliver a particular effect. Unfortunately, it is all too common for individual security elements to be considered in isolation, often leading to reduced effectiveness and overly costly schemes.

Further detailed information is provided by NPSA within Physical defences at the perimeter.

In relation to lighting, organisations must also ensure that they are regularly reviewed, especially during increased risk. NPSA have produced a guide on lighting, which covers advice on lighting types, levels and standards, see: Security Lighting Guidance for Security Managers.

In addition, maintenance of the lighting system should fulfil 3 distinct functions, namely:

- Corrective Maintenance: suitably qualified and security vetted technicians should be available to respond by attendance to carry out on-site emergency repair or replacement of lamps and luminaires. Response time will depend on how critical the lighting is to the site. A log should be maintained of which lamps are being replaced. This can identify design issues (column vibration, temperature issues etc.), and if some lamps fail more often than others.
- Preventative Maintenance: routine servicing and preventative maintenance of the system should be undertaken, typically annually (this should be done in late summer/early autumn before the longer nights start). Luminaires should be cleaned, and any defective lamps replaced. During maintenance broken lamps or luminaries should be regarded as suspicious and any sudden ‘misalignment’ should be investigated. If the log of replaced lamps indicated an increasing failure rate, then consideration must be given to replacing all remaining lamps.
- Planned Refurbishment Cycle: managed, planned refurbishment and replacement programmes to renew all principal system components on a repetitive cycle should be implemented. This should include the principle of ‘block lamp replacement’ which would be undertaken as part of the preventative maintenance visit. The length of this cycle will depend on the predicted life of the lamps, recognising that some lamps don’t fail ‘catastrophically’ but suffer decreasing lumen output and for LED lamps this would involve replacing the luminaire.

Further detailed information is provided by NPSA within Intruder Detection, Tracking, Monitoring and Lighting.

Administration

Policy and procedures should mention that perimeter fencing and security lighting is checked, if applicable, should the threat level be raised or following an incident. Identify ownership of the responsibility and governance of the decision making, including who is responsible for the management, coordination and strict compliance, together with the relevant records keeping, and how its effectiveness is assured. Ensure staff understand processes and procedures to be adopted, including action and contingencies.

An Operational Requirement (OR) allows an organisation to identify the need and intended purpose of perimeter fencing and lighting as well as the need to regularly review and maintain each. This will drive its subsequent design and make sure the interdependent systems are sufficiently flexible and appropriate for its specific needs.

The OR should address:

- The purpose of the perimeter fencing and lighting system.
- The requirement for fencing and lighting and what specification is needed from each element at each specific location.
- The maintenance routine required in respect of both fencing and lighting.

The OR process assists organisations to invest proportionately in their security measures, enabling them to implement an integrated approach to security and identify security measures appropriately to the risks faced.

A clear policy should be in place regarding the disposal of lamps as many of them will contain toxic metals and other material. These present a hazard not only to personnel but also to the wider environment.

Risk Assessment

This risk assessment can be used to define the issues that need to be addressed; either to prevent them from affecting the organisation or detect them if they have already manifested themselves.

Risk assessments should clearly define organisational as well as individual duty of care to staff and others. The risk assessment process relating to perimeter fencing and lighting should consider all risks relating to existing and future use. It is important to ensure that the process concerning maintenance and installation of systems is robust and complies with all regulations/legal requirements.

Fencing and lighting are only part of a holistic security system. However, there are a number of stages to undertake when planning new or auditing existing security projects. These include:

- Understanding and identifying the security risks your organisation faces.
- Considering the nature of hostile reconnaissance, where it may be conducted in or around your site, and what you can do to deter or detect it.
- Developing an OR statement of need for fencing and lighting. The OR will then enable you to design your fencing and lighting and consider the various types of designs and technologies available on the market.
- Carrying out an audit of your fencing and lighting against your Operational Requirement.

By completing this process, the organisation will be able to assess, develop and justify the financial

investment needed to protect critical assets. The OR will determine the technical design of the fencing and lighting systems in order to have effective capabilities in the right areas, to deter, disrupt or detect hostile reconnaissance and criminal activity.

Communications

Internal Stakeholder Engagement:

The principles of undertaking a maintenance programme for supporting technologies, which protect the organisation, should not be shared with all staff. This information should be contained to those involved in the processes and need to know.

Dedicated channels should be established, with backups if access to the organization's intranet or message channels is limited (for example if the intranet is restricted due to criminal investigations), if the network is overloaded, or if it has been the target of the attack. You must provide information for your staff and resources so that they can help deliver the plan.

Your internal audience will inevitably cross over into your external audience, so you should consider the messages you wish 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:

Details of critical supporting technologies which enable the protection of your organisation should not be shared with external organisations. However, 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 forums 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:

After a terrorist incident has occurred, organisations should not communicate directly with the media or external audiences on anything related to the incident, without prior consultation and agreement with the police. In addition, avoid revealing details about the incident through social media without prior police consultation.

An appropriate individual should be identified in the organisation to liaise with the police in order to disseminate approved information which is accurate, and which will not compromise the criminal investigation.

Health and Safety/Other Legal Issues

Businesses/organisations that are implementing checks of perimeter fencing and security lighting should ensure that all activities are assessed in line with Health and Safety and other legal/policy frameworks, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- Employment Rights Act 1996
- BS7671 – Institute of Electrical and Electro-Mechanical Engineers current Edition.

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. 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
OPERATIONAL
FENCING
LIGHTING
PERIMETER
CCTV
INTRUDER