ProtectUK

Tactic EB5: Ensure supporting technology, such as access control systems, are in working order

ProtectUK publication date
14/12/2023

Information and Intention

There are a number of supporting security related technologies which play a role in the security operations of an organisation. These include:

- Perimeter Intrusion Detection Systems (PIDS);
- Access Control Systems;
- Close-Circuit Television (CCTV);
- Communications Systems;
- Door Alarms;
- Control Room;
- Security Lighting;
- IT infrastructure; and
- Vehicle Access Barriers.

However, many of these technical systems also rely on a human element to make them work, e.g. CCTV systems. It is therefore essential that the technology is not looked at in isolation and that the associated people processes are also reviewed, and any vulnerabilities are rectified.

It is also important that when each of the technologies is examined, a review is carried out as to what role they would play in the event of a raised threat level or terrorist related incident.

A regular systems and asset maintenance programme should already be in place for the various technology systems. However, in the event of a raised general threat level or specific threat to the business, additional maintenance arrangements should be considered.

The issue of cyber-attacks on technological systems is a real and ever-growing threat and organisations should consider the use of the National Protective Security Authority (NPSA)'s Cyber Assurance of Physical Security Systems (CAPSS) programme. CAPSS is about gaining confidence in the 'cyber' components of electronic security products which, while robust in the physical security domain, could potentially be compromised by a hacker externally.

The primary aim of CAPSS is to provide a mechanism by which organisations can gain a good level of confidence that the software and hardware security solutions they have in place, or are considering purchasing, have strong and effective cyber mitigations at the core of their development and operation.

By utilising CAPSS assured products, sites can ensure that their systems are more robust, preventing an attacker gaining entry to the wider corporate network, or manipulating and circumventing the physical security systems.

Method

It is important to identify and carry out an audit of all technical systems which play a role in the security operations of your organisation. Review the maintenance programme for each technology, and also the contractual arrangements with suppliers in the eventuality of it breaking down (e.g. if there is a high threat, you cannot have your access control system out of commission for weeks).

Perimeter Intrusion Detection Systems:

Your first line of defence if your business is located on a site, is the site perimeter. There are a number of Perimeter Intrusion Detection Systems that you should consider, and which should be selected after an appropriate Operational Requirement has been created for them. These include:

- Barrier mounter PIDS;
- Ground-based PIDS;
- Free-standing PIDS; and
- Rapidly Deployable.

Like other technologies, it is essential that you establish a comprehensive maintenance schedule to ensure system effectiveness and to prevent gradual reduction in PIDS performance. Maintenance regimes should be performed by the PIDS operators or site maintenance team to minimise false alarms. Requirements should include:

- The ground in and around the PIDS, barriers and/or detection zone should be kept clear of foliage and vegetation.

- The site should be kept clean and tidy.
- Wildlife should be prevented from interacting with the barrier or detection zone.
- Vegetation should be kept cut back to reduce the possibility of causing false alarms and long grass should be avoided.

Access Control:

Access control remains one of the most important technologies in maintaining the security of your premises from unauthorised intrusion. An access control 'system' contains a number of elements – Automatic Access Control System (control panel), token/reader/keypad (the 'key' to the door), BAACS (Biometric Automatic Access Control Systems e.g. fingerprints). Points to consider include:

- Reviewing your access control methods.
- Ensuring a robust visitor entry and exit policy.
- Consider a zoning policy.
- Consider obscuration products (obscuration prevents hostile surveillance into a building).

CCTV:

CCTV is a good example of the importance of an interface between technology and people, where both are interdependent and essential. The first stage of ensuring a CCTV system is fit for purpose is by creating an Operational Requirement for it. It is also critical that your CCTV system is legally compliant with data protection requirements. ProtectUK have a CCTV checklist which covers some of the main areas which need to be considered when looking at putting in place a maintenance programme, see ProtectUK - CCTV Checklist.

Similar approaches should be applied to the other security technologies listed above, such as security lighting, communications systems and vehicle access barriers.

Procedural Security:

As well as ensuring that the technology works, it is also important to look at procedural security as well, For example:

- Have you cancelled access cards for staff who have left?
- Do you cancel access cards when they have been reported lost?
- Do you change access levels when an employee moves roles and does not require the access levels they had in their previous roles?
- How often do you audit permissions given to staff?

Human/Technical Interfaces:

The human/technical interfaces of security systems are sometimes overlooked. While the technical systems may be fully maintained and serviced, if there is no consideration of the human element, the overall system could be vulnerable. Therefore, the associated people processes should also be reviewed, and any vulnerabilities should be rectified. An example would be the importance of people in a CCTV ‘system’, including their training and specialist knowledge/skillsets.

Cyber Attack:

Cyber-attacks are an ever-increasing threat to the UK's critical national infrastructure and the wider business sector.

It is essential that software and hardware security systems have the full set of threat mitigations at the core of their functionality and are utilised by a site for maximum effect. The NPSA CAPSS programme is designed to assist security managers in focussing on key areas when it comes to protecting against cyber-attacks. It covers both physical and cyber security.

Administration

The appropriate policy and procedures should mention how supporting technologies, which assist in the protection of the organisation, are maintained to ensure they remain in good working order.

Ideally there should be a senior manager responsible for the strategic oversight of the policy and processes, and a more junior manager should sit under them who will oversee tactical/operational level issues. However, 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.

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:

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.

However, 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:

Details of critical supporting technologies which enable the protection of your organisation should not be shared with external organisations. If hostiles were able to obtain this information, it could assist them in identifying organisational vulnerabilities and would help in any attack planning.

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:

The aforementioned information should not be shared with the media.
However, general engagement with the media should be encouraged to allow a positive and deterrent message to be disseminated to the general public, as part of the Security Minded Communications strategy.

By positively reinforcing a security deterrence message, 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

Any actions carried out regarding maintenance and testing of support technologies may be governed by legislation, 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 change to the technology maintenance programmes 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 maintenance and testing of support technologies.

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 the maintenance and testing of support technologies must include consideration of your organisations insurance policies. Consideration must always be given regarding the personal health and safety of security staff in undertaking duties regarding the above.

KEYWORDS
CCTV
ACCESS CONTROL
ALARMS
SECURITY
COMMUNICATIONS