ProtectUK

Tactic IB5: Actively monitor CCTV/VSS at all times and review out-of-hours footage

ProtectUK publication date
14/12/2023

Information and Intention

Closed-Circuit Television (CCTV) is a system in which images are monitored and recorded for surveillance and security purposes. TACTIC IB6 should be considered together with this tactic.

It is important to understand that CCTV will not prevent criminal action, but may deter or detect a criminal action. CCTV should always be used alongside other security measures to provide a coordinated security solution.

Site CCTV systems as detailed within ProtectUK - CCTV and NPSA - CCTV are generally deployed to achieve the following functions:

- Deter an attempted intrusion by causing an adversary to reconsider the site due to enhanced probability of detection.
- Detect an attempted intrusion to the site using video analytics.
- Verify and further investigate an alarm event from a Perimeter Intruder Detection System (PIDS).
- Tracking of an intruder when they have breached the perimeter.
- Recording of digital image evidence suitable for use in an investigation or court proceedings (see guidance below for retention policies).
- Overlooking Access Control area.

It is also important to recognise the difference between the monitoring and review of CCTV within the workplace and CCTV within the perimeter of a site as well as the implications when it comes to storage and retention of recorded CCTV images.

As detailed in control room security personnel capability there are a number of things to encourage and enable that can be applied to those involved in the monitoring and review of CCTV:

- Foster an environment of checking and verifying as information received may be inaccurate and can be influenced by biases of interpretation and personal perception.
- Establish open communications and good relationships within the control room, and between the control room and the security officers on the ground to reduce barriers to reporting.
- Encourage the team to understand human and technical limitations, and work together to ensure maximum coverage of eyes and ears on the ground.
- Do not rely on technology; for example, if logging technology does not enable all relevant information to be captured ensure that an alternative logging repository is available.

In organisations with multiple control rooms, it is essential to establish good communications between them. This can be facilitated by ensuring:

- Common maps: ensure all stakeholders have a common map view.
- Camera positions: understand the camera positions and views available to each control room to establish areas of support, for example when tracking an individual behaving suspiciously.
- Cross control room working: enabling an operative trained for one control room to work within another existing control room can help communications between both control rooms.

In addition, it is important to ensure a common understanding within the security team, that the perspective of the security officers on the ground is markedly different to the perspective of the control room operator. Security officers on the ground have a 3D view from ‘inside the map’, whereas the control room have a 2D ‘overhead’ view ‘onto the map’. Being aware of these differences in perspective is beneficial when giving or receiving information.

Method

Monitoring and regularly reviewing recorded images will assist in the identification of suspicious activity or hostile reconnaissance. When operators are monitoring CCTV screens, they should monitor for a period of 20 minutes and then take a break. This allows them to retain their sustained vigilance when they return to their position.

For further information regarding human factors in CCTV control rooms, see NPSA - Human factors in CCTV control rooms - best practice guide.

In order to identify these activities, cameras should be placed in positions across the site that will

offer the clearest images to the viewer. Should an intrusion or incident be detected, the CCTV system can then be used to monitor and track an individual. This information would likely assist both the responding emergency services and any post-incident investigation.

The access points to a site may provide the best opportunity to identify individuals or vehicles as they enter or exit the site, or other areas that are critical to the safe management and security of your operation. This tactic is linked to TACTIC IB6; ensure that CCTV is focused on all communal areas and vulnerable points.

When actively monitoring the CCTV and reviewing out-of-hours footage, you may be provided with information/intelligence associated with the increased risk which will assist with your task. As such you should direct your resources to:

- Provide general oversight of open space. This will enhance your situational awareness and help you detect potential issues before they occur, while also providing an extra level of support to ground based security personnel.
- Monitor pedestrian routes and vehicle movements.
- Detect and monitor unexpected or unwanted activity.
- Track people and items around your site. This helps you both protect them and track any suspicious activity.
- Provide situational awareness to both security control room and response personnel.
- Provide additional coverage/resources to supplement those provided by perimeter and building CCTV systems.
- Potentially extend and integrate CCTV with existing site alarm systems.
- Enhance the deterrent effect of existing CCTV.

You should also bear in mind the following considerations to ensure that requirements are appropriate:

- Will the images potentially be used as evidence in a court of law? If so, the requirements must ensure sufficient image quality and reliable record and storage.
- Integration with existing control room systems, processes and procedures. Existing staffing levels should also be reviewed to confirm they will be able to cope with additional complexity.
- Integration with existing CCTV systems at the site.
- Will there be any need to supplement or enhance existing lighting systems?
- Are the prevailing weather conditions suitable for the type of CCTV being proposed?
- Are there plans for development of the site, potentially with the erection of new structures and/or removal of existing ones? If so, the requirements should take account of these.

Remember that landscaping activities also have the potential to obstruct current fields of view.

- Additional vegetation management plans may be required to ensure that fields of view remain clear.
- Can the CCTV see beyond the site perimeter? If so, consider the requirement for operators to be appropriately licensed and for the masking of images where they would otherwise overlook private residences.
- Requirements associated with relevant legislation such as the Data Protection Act.
- Will the system be pro-actively monitored or set to alarm on detection? If not, then it cannot help you prevent issues occurring, but might provide a retrospective view of what took place.

For successful CCTV coverage, your site should be kept clear of random obstructions wherever possible – do not give intruders a hiding place. To catch an intruder in the act, your cameras must be monitored.

Administration

If CCTV is an existing element within the security and management strategy, make sure there is a CCTV policy describing how it is managed in compliance with the Data Protection Act and General Data Protection Regulation (GDPR). If a system of 'contracted-in' surveillance CCTV operators is used, they must be licensed by the Security Industry Authority (SIA).

Go to the Data Protection Act CCTV guidance webpage.

Check whether your systems adhere to GDPR guidance.

The SIA Licensing CCTV webpage offers help on licences and licence holders.

Policy and procedures should always mention active monitoring of CCTV and review of out-of-hours footage, should the threat level be raised or following an incident.

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 records keeping, and how its effectiveness is assured.

Ensure staff understand processes and procedures to be adopted, including action and contingencies.

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 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 and the individual duty of care to staff and others. The risk assessment process relating to CCTV should consider all risks relating to existing and future CCTV systems. These could include risks involving potential breaches of GDPR as a result of incorrect operation of the system.

It is important that the process concerning maintenance and installation of systems is robust and complies with all regulations/legal requirements.

CCTV is 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 Operational Requirement statement of need for each camera in each location. The OR will then enable you to design your CCTV system and consider the various types of CCTV surveillance technologies available on the market.
- Carry out an audit of your cameras 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 Operational Requirement will determine the technical design of the CCTV system in order for it to have effective detection capabilities in the right areas, to deter, disrupt or detect hostile reconnaissance and criminal activity.

Communications

Internal Stakeholder Engagement:

Dedicated channels should be established, with backups if access to the organisation’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.

Certain aspects of active monitoring of CCTV and review of out-of-hours footage 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, and they should be encouraged to identify and report any

suspicious activity they observe, or that they know about.

It is necessary to ensure points of contact regarding CCTV matters are known to staff internally, and partners externally. Any information regarding active monitoring of CCTV and review of out-of-hours footage should be disseminated internally through the Communications function.

All security management/security staff should understand where CCTV cameras are positioned and what the monitoring 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 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 include basic information regarding the active monitoring of CCTV and review of out-of-hours footage if it impacts on neighbours. However, specific information on such monitoring and review 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 forums who may already have identified ‘best practices’ and lessons learned from similar sites within the business area the site operates within.

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 and approval.

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 active monitoring of CCTV and review of out-of-hours footage, 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
- General Data Protection Regulation (GDPR)
- SIA Licensing CCTV

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

The Information Commissioner Office (ICO) is responsible for regulating and enforcing data protection law, namely the GDPR and the Data Protection Act. It has published detailed guidance on data protection impact assessments (DPIAs) for general processing which you should read.

All organisations in the UK must comply with data protection law, and in certain cases, carrying out a DPIA is a mandatory requirement.

When considering the deployment of a surveillance camera system, you must have a clear understanding of your responsibilities under data protection law. If you are making decisions around capturing personal data as a controller, or joint controllers, you are responsible for compliance with data protection law, including the requirement to carry out a DPIA.

It is recommended that data protection impact assessments are carried out when:

- New systems are installed.
- Cameras are added or removed from systems.
- Cameras are moved or change position.
- Whole or parts of systems are upgraded.
- Where systems that include biometrics capabilities such as automatic facial recognition are in use.

KEYWORDS
CCTV
ACCESS CONTROL
SECURITY
PERIMETER