Tactic IB6: Ensure that CCTV is focused on all communal areas and vulnerable points

ProtectUK publication date
14/12/2023

Information and Intention

Closed-Circuit Television (CCTV) and video surveillance systems play an important role in the early identification of criminal or suspicious behaviour, and the investigation of crime and critical incidents, as well as post-incident evidence gathering and forensic analysis.

Monitoring and regularly reviewing recorded images will assist in the identification of suspicious activity or hostile reconnaissance.

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 IB5.

Method

The Home Office has published useful guidance documents relating to CCTV, aimed to assist those responsible with the design of their systems.

Further information can be found on ProtectUK and NPSA websites.

Using these guides will assist organisations to work alongside the CCTV contractor, to achieve a

system that is:

- Fit for purpose.
- Allows the police to gather evidence.
- Meets the needs of the organisation.

Administration

An Operational Requirement (OR) allows an organisation to identify the need and intended purpose of a CCTV system. This will drive its subsequent design and make sure the system is sufficiently flexible and appropriate for its specific needs.
The OR should address:

- The purpose of the CCTV system.
- The requirement for cameras and what information is needed from each camera at each specific location.
- The level of detail required for each camera, including how images will be stored and for how long.

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.

The NPSA Operational Requirements webpage provides further guidance on completing this process. If CCTV is an existing element within the security and management strategy, ensure there is a CCTV policy describing how it is managed in compliance with the Data Protection Act and General Data Protection Regulation (GDPR), see ICO - Domestic CCTV Systems and ICO - UK GDPR Guidance and Resources.

If a system of ‘contracted-in’ surveillance CCTV operators is used, they must be licensed by the Security Industry Authority (SIA), see SIA Licensing CCTV.

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 as well as 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 OR 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.
- Carrying 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 OR will determine the technical design of the CCTV system in order to have effective detection capabilities in the right areas, to deter, disrupt or detect hostile reconnaissance and criminal activity.

Organisations may use the Surveillance Camera Commissioner's self-assessment tool to satisfy themselves that they meet the principles of the Surveillance Camera Code of Practice. This will assist the identification of any additional work required for compliance, see Surveillance Camera Commissioner.

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.

Information on the placing of CCTV to cover communal areas and vulnerable points 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 for CCTV matters are known to staff internally, and partners externally. Any information regarding CCTV placement and coverage 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 CCTV placement and coverage, as the cameras covering communal areas may impact 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 or other incident involving a security breach 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 utilizing CCTV which is focused on all communal areas and vulnerable points, 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 ICO is responsible for regulating and enforcing data protection law, namely the General Data Protection Regulation and the Data Protection Act 2018. 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
RISK ASSESSMENT
GDPR
RISK
SECURITY
HOSTILE RECONNAISSANCE