ProtectUK

CCTV

Original publication date
02/11/2020

1. Introduction

This section is designed to assist those with responsibility for the security of Venues & Public Spaces (VaPS) and small and medium-sized enterprises (SMEs) in relation to CCTV and video surveillance systems. Given all sites have their own unique characteristics, rather than being a rigid set of rules, this guidance instead provides generic advice and principles.

CCTV Checklist

2. CCTV guidance and operation

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, including post-incident evidence gathering and forensic analysis. Such systems are also invaluable when investigating health and safety concerns and in the event of public liability claims.

Monitoring and regularly reviewing recorded images will assist in the identification of suspicious activity or ‘hostile reconnaissance’. Hostile reconnaissance refers to the planning phase of a terrorist attack. In order to identify these activities, cameras should to 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 individuals. This information would likely assist both the responding emergency services and any post-incident investigation.

3. Can we improve the efficiency and effectiveness of video surveillance in a counter-terrorism role?

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.

See the NPSA Operational Requirements for further guidance on completing this process.

4. Planning new or auditing existing security projects

There are a number of stages to undertake when planning new or auditing existing security projects:

- 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
- carry out an audit of your cameras against your OR

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.

Go to the Surveillance Camera Commissioner webpage.

5. Technical design of CCTV systems

Newly installed CCTV systems can be poorly designed. This is often due to inadequate consideration at the OR stage. The Home Office Centre for Applied Science and Technology (CAST) and the National Police Chief's Council (NPCC) have published useful guidance documents relating to CCTV, aimed to assist those responsible with the design of their systems. NPSA (formerly CPNI) have also published CCTV guidance.

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, and meets the needs of the organisation.

Go to the Government CCTV guidance webpage.

Go to the NPSA (formerly CPNI) CCTV guidance webpage.

5.1 Factors to consider

When choosing the number and type of CCTV cameras, as well as their location, it is important to consider the following:

- the type of CCTV camera and lens. One of the challenges when setting up a CCTV system is choosing the right lenses for the cameras. Different lenses provide different fields of view, and zoom
- the view on the monitor for the operator, including the distance from the target, the angle of view, the lighting conditions and the varied weather conditions
- the operability of the CCTV camera. Is a camera that can pan, tilt and zoom required to support fixed cameras?
- if the CCTV system is monitored, or there is remote access to the system, what software or other technology is available to support and provide an alert or additional information, for example automatic number plate recognition (ANPR)?

Each of these considerations will impact on the live and recorded image quality. If they are not considered in line with your OR, the system may not meet your needs.

Modern cameras produce images and have superior colour to that of previous, older systems, meaning that they are more effective at capturing important details over a larger field of view. CCTV with a higher resolution means significantly more data will be captured and compression technology may need to be used. When considering the use of compression technology, bear in mind there may be a reduction in the saved or recorded picture quality compared to the operator's live view.

However, without the compression of images, storage requirements may significantly increase. This may influence the length of time that recorded images are retained for evidential purposes. Consider the costs and benefits of both options.

The movement from traditional analogue surveillance technology to IP (digital) surveillance technology has given security professionals access to a much broader functionality such as traffic monitoring, car parking control and enforcement linked to ANPR. Video analytic software is now affordable to SMEs and can provide a host of features, allowing operators to do more with surveillance footage, including the quick identification and tracking of suspects.

5.2 Selecting a reputable and diligent contractor

When selecting a CCTV installer, check they are registered with a UKAS accredited inspectorate. This will ensure they operate to the highest level of business excellence, comply with the relevant British and European (BS and EN) Standards and work to an approved code of practice for the design, installation and maintenance of systems.

An approved, reputable and diligent contractor will provide a technical specification for the system and should perform an audit and commissioning test of the system to prove that the system meets your operational requirement and your design criteria.

The Surveillance Camera Commissioner has a statutory role to provide the CCTV industry with a current list of recommended standards and requires CCTV operators to comply with their Surveillance Camera Code of Practice.

5.3 Will my system allow the prosecution of offenders?

Image quality

CCTV camera evidence can be compelling, though issues of image quality are a factor if CCTV images are used in court. The OR and technical design should consider the nature of the activity to be observed. The purpose of the observation can be for:

- identification: matching a face to a database
- recognition: differentiating between objects within a scene
- observing: some characteristic details of the individual, while the view remains sufficiently wide to allow activity surrounding an incident to be monitored
- detection: of objects within the scene

Testing the System

The Rotakin target, a device to test CCTV camera performance, was developed by the Home Office and is specified in BSI EN 50132-7: 1996. It is commonly used by the installer to audit and commission the CCTV system against the specified OR.

The Centre for Applied Science and Technology (CAST) provide guidance on testing CCTV systems.

Individuals and vehicles

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.

Seizure of images for evidential purposes

If recorded images are seized by police for evidence, consider the 'continuity of evidence' (the way the evidence has been handled from the moment that it is found, seized, or produced, to the point that it is presented in court as an exhibit). When a police officer takes possession of a CCTV data recording, a statement of continuity will be required from the system operator.

Location of recording equipment

Recording equipment should be placed in a secure area with restricted access. The system should have sufficient storage capacity to retain good quality images for as long as can be justified and requirements laid out at the OR stage. Some sites may decide to hold data for longer periods; such as ATM locations or where the data may be reviewed on a regular basis rather than actively monitored. If downloaded, all recordings on removable media should be kept in a secure place.

Copying of captured Images

If an incident occurs, the images should be copied onto removable media. A record should be kept of movement of the CD or CDR disk, SD card, or other media showing an identification number, times, dates and names of those handling the media. All used media should be destroyed or disposed of securely.

5.4 Is your CCTV system legally compliant?

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 GDPR. If a system of 'contract-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.

6. Incident response

Not all Venues & Public Spaces and SMEs will have an efficient, functioning, well-sited CCTV system with trained operators proactively looking for suspicious activity, ready to direct security officers or police.

However, bear in mind the following:

- if there is an increase in threat level to a location, business sector, or major event, can staff be deployed to actively monitor the CCTV system?
- do you monitor or regularly review recorded images to identify suspicious activity on, or adjacent to your site?
- is a record made, and staff briefed if suspicious activity may constitute hostile reconnaissance, and what procedure is in place to report that information to the police?
- if a suspicious incident is noticed, how quickly can staff monitor and review the CCTV while staff engage with suspicious people or item(s) or deal with the incident?

7. Training

While CCTV, thermal imagers and video analytics are useful technology, they all rely to some extent, on the effectiveness of the control room and the security staff. Action Counters Terrorism (ACT), Counter Terrorism Awareness training is a national police initiative for businesses to protect our cities and communities from the threat of terrorism.

ProtectUK's E-Learning page.

Contact your local Counter Terrorism Security Advisor for further information.

8. Data Protection Impact Assessment (DPIA)

The ICO is responsible for regulating and enforcing data protection law, namely the General Data Protection Regulation and the Data Protection Act 2018.2 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 captured 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
PUBLICLY ACCESSIBLE PLACES
HOSTILE RECONNAISSANCE
SECURITY
CYBER
PALS GUIDANCE
PALS
PUBLICLY ACCESSIBLE LOCATIONS