Third Party Closed Circuit Television (CCTV) Standard- Good Practice

Issue 1

Date: 29/07/2016,

BT Security

Contents

1. Introduction

1.1. General

This document lays out general good practice guidance for the use of CCTV by third party suppliers.

1.2. Background

The use of CCTV has become increasingly widespread throughout the UK over recent years. Originally deployed for protecting large establishments and monitoring city centres, CCTV systems are now installed routinely within offices, shops, schools, and even individual vehicles on the public transport network. Additionally, the market has undergone a rapid transition from analogue to digital recording technology, which has had a significant impact on the design and functionality of CCTV systems.

The focus of the document remains the same: to provide clear guidance to non-technical users wishing to buy a CCTV system that is fit for purpose. However, the issues of recorded image quality and data archiving that are essential parts of any digital CCTV system, but are often neglected when writing the specification.

Analogue CCTV recording systems were relatively simple to design as they relied mainly on the use of VHS tapes to capture the images. Digital recording systems, by contrast, are much more complex to specify. They record onto a hard drive, which can only store a limited amount of video; when it is full the oldest material will be overwritten with new. Therefore when specifying a system thought must be given to the capacity of the hard drive, the provision of a suitable method to create a permanent record of any key incidents (e.g. DVD writer) and the use of compression (which will affect the recorded image quality). Many of these issues are inter-related; thus improved recorded picture quality and higher frame rate may come at the expense of a reduced retention time on the system. One of the key aims of this document is to provide some guidance on these complex factors.

1.3. Additional Materials and Advice

UK HMG provides a high level advice sheet for the provision of CCTV:

CCTV Operational Requirements Manual	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378443/28_09_CCTV_OR_Manual2835.pdf

The Centre for the Protection of National Infrastructure (CPNI) also provides guidance on cyber protection, and includes sections on the use of CCTV, such as:

Closed Circuit Television (CCTV)	http://www.cpni.gov.uk/advice/Physical-security/CCTV/

The Information Commissioners Office (ICO) provides a code of practice on CCTV:

In the picture: A data protection code of practice for surveillance cameras and personal information	https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

The British Standards Institute (BSI) also have a code of practice which can be purchased from them:

BS 7958:2009 CCTV management and operation code of practice	http://shop.bsigroup.com/Browse-By-Subject/Security/Electronic-Security-Systems/cctvstandards/

BT Supplier Security Requirements:

BT Supplier Security Requirements V1.1	http://www.selling2bt.com/working/BTSupplierSecurityRequirements/index.htm

Security Industry Authority (SIA) has information on public space CCTV operative licence requirements:

Public Space Surveillance CCTV	http://www.sia.homeoffice.gov.uk/Pages/licensing-cctv.aspx

2. Objectives

2.1. The purpose of this document is to provide generic security advice in order to assist you as a supplier to BT with good practice guidance on the use of CCVTV systems in your premises, and makes reference to other sources of useful information to assist you.
2.2. As a supplier to BT you will be contractually obliged to ensure that any BT or BT customer information entrusted to your care is adequately protected in order to ensure any confidentiality and security obligations. You must comply with these and should refer to your contract and the BT Supplier Security Requirements (see Section 1.3 above) for details.
2.3. CCTV should form only part of any security system; it should not be used on its own. It cannot replace security staff, although it may permit a reduction in their number or their redeployment to other security activities.
2.4. In its simplest form a CCTV system consists of a television camera joined by a transmission link such as a cable to a monitor sited in the guard room or central control point. More complex systems use several cameras and monitors or a single monitor with a switching system to display camera pictures in sequence. Additional facilities such as recorders, automatic switching in response to an alarm signal may be used.
2.5. Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations, but only if the images are good enough to identify what happened and be used by law enforcement, or to satisfy you, BT or third parties that incidents are being dealt with properly.
2.6. External lighting will help security staff and improve the capabilities of CCTV systems if it is carefully designed and used. Effective CCTV systems may help to deter an incident or even identify planning activity. Good quality images can provide crucial evidence during the course of an investigation and an aid to law enforcement. It can also be used as an alarm if associated with ‘motion detection’.
2.7. If you have contracted-in staff who operate CCTV equipment, you must ensure they are appropriately licensed by the Security Industry Authority (SIA) and these licences continue to be in place while they operate CCTV equipment for you. Failure to have such required licences is a criminal offence. This will particularly be relevant if the CCTV equipment is deployed into fixed positions or has a pan, tilt and zoom capability and where operators: proactively monitor the activities of members of the public whether they are in public areas or on private property; use cameras to focus on the activities of particular people either by controlling or directing cameras to an individual's activities; use cameras to look out for particular individuals; use recorded CCTV images to identify individuals or to investigate their activities.
2.8. The use and purpose of the CCTV system should be recorded as part of your security policy, which should be documented and retained to demonstrate compliance. A suggested list of topics for this policy to cover is contained at Appendix A.

3. Quality of Recorded Images

3.1. Before installing a CCTV system you should have a clear idea of what you want the system to do and how it should perform. This should include exactly what you want to see and where, e.g. recognise the face of someone walking through a doorway, read a vehicle registration number or record a particular type of activity, such as walking across a room, exchange of money or an assault.
3.2. The appropriate resolution, level of compression and number of pictures per second will be determined by what you wish to see in the recording. If you can’t see it then it’s not fit for purpose. It should not be expected that enhancement features, such as zoom controls, will provide extra detail.

3.3. A good way to ensure that the system is capable of achieving the requirement is to do a subjective test. Set-up a camera and get a volunteer to walk through the door or park a car in the place of interest and record the pictures. This should be done under the conditions that the system is intended to be used – performance of the system may be different when there are a number of cameras being recorded.
3.4. The quality of the recorded or printed pictures may differ from the live display. The quality of the pictures should not be compromised to allow more to be squeezed onto the system. There is some scope however for using a sliding scale of image quality based on time since recording. For example, high quality high frame rate video for the first 24 hours with gradually increasing compression or decreasing frame rate after this, but retaining useful images up to at least 20 days. This would be dependent on the nature of the installation and the type of recordings being made.
3.5. To ensure continued quality of recording it is essential that regular maintenance of all aspects of the system be conducted - especially camera focus, cleaning of lenses, housings, etc.
3.6. Adequate perimeter and site lighting (to facilitate natural observation and for personnel safety), supplemented with infra-red or similar lighting as necessary, must also be provided to ensure that a satisfactory CCTV image is given at all times, night and day, that will allow the image on screen to be detected as a person - that is an image that will provide for a minimum of 50 % screen height. This is where it is used as an aide for access control, or for 'incident reconstruction' purposes.
3.7. The system should be capable of being continuously recorded, and if it is monitored 'live' so much the better in order to be able to respond to an incident, or for detecting signs of intrusion. It is also essential to have a response plan in place.
3.8. The cameras in place must be maintained in good working order (rather than out of order/faulty). The times displayed on cameras must be accurate.
3.9. There should be a Service Level Agreement (SLA) in place with the third party maintenance vendor to ensure that faulty cameras are repaired in a timely manner.

4. Storage

4.1. Access to the system and recorded images should be controlled to prevent tampering or unauthorised viewing. Electronic protection methods that require proprietary software or hardware will hinder an investigation if they prevent the pictures from being provided to authorised third parties. Physical methods of access control, e.g. system in a locked room, are just as effective if documented appropriately. This is in order to ensure that the integrity of the stored images is maintained.
4.2. It is important that recordings cover a sufficiently long period to assist in investigations. Retention beyond 20 days may be useful in some circumstances, but should not affect the quality of the more recent recordings.
4.3. It should be possible to protect specific pictures or sequences, identified as relevant to an investigation, to prevent overwriting before an investigator can view or extract them.
4.4. BT's contractual requirements specify images are retained for 45 days (SBCA requirements) or 20 days (BT Security Requirements), and this includes back up images. Images should therefore be retained for a minimum of 20 days.
4.5. Suppliers must extend this period under the following circumstances:-
4.6. Where CCTV video evidence has to be retained for an on-going criminal investigation.
4.7. Where security industry standards, such as NACOSS (National Approval Council for Security Systems), specify a definitive retention period.
4.8. Where specified as a necessary requirement in countries outside the UK to adhere to local country legislation.
4.9. Once the retention period has expired, all CCTV images must be erased (overwriting is acceptable).

4.10. All CCTV video/digital video recorders must be discreetly located to prevent unauthorised access and the possibility of 'casual' viewing of any associated CCTV screens.
4.11. All CCTV digital video recorders must be accessed by authorised personnel only and access to the images must be password protected.
4.12. CCTV recorded images must be backed up, and the storage of those ideally placed in a separate location.

5. Export of Images

5.1. In the event of a security incident it is important that the system has the ability to export copies of the CCTV footage in order to aid the investigation, and any law enforcement agencies. It is unlikely that the investigator will be familiar with the operation of your system. To facilitate replay and export a trained operator and simple user guide should be available locally.
5.2. Export of medium and large volumes of data can take a substantial period of time. The operator should know the retention period of the system and approximate times to export short (e.g. 15 minutes), medium (e.g. 24 hours), and large (up to all of the system) amounts of data.
5.3. If the software needed to replay the pictures is not included at export, viewing by authorised third-parties can be hindered. Export of a system event log or audit trail, and any system settings with the pictures will assist with establishing the integrity of the pictures and system.
5.4. The amount of video that an investigator will need to export will be dependent on the nature of the investigation. For example an office burglary may only require a few stills or a short sequence, however a more serious incident may require anything up to all the video contained on the system to be exported. It is essential that the system is capable of doing this quickly and to an appropriate medium. An ideal solution for medium-to-large downloads, would be for the system to have the facility to export to a ‘plug-and play’ hard drive. Export and recording should be possible at the same time without affecting the performance of the system.
5.5. The system should not apply any compression to the picture when it is exported from the system as this can reduce the usefulness of the content. Also, the picture should not undergo any format conversion that affects the content or picture quality.

6. Playback of Recorded Images

6.1. The replay software or other technology must allow the images to be capable of searching the pictures effectively and see all the information contained in the picture and associated with it. It should be possible to replay exported files immediately e.g. no re-indexing of files or verification checks.

7. Siting of Cameras

7.1. Site plan-
The first task when constructing an operational requirement is to draw a site plan on which to mark the areas of concern. The more detail that can be included in this plan the better as this will aid in the placing of lights and cameras especially with regard to fields of view and potential environmental problems such as low sun or foliage.

7.2. The next step is to define the problems that affect the site. Some of these may be general threats but some may be specific to a given location. Typical threats or risks that might be identified include:

- Crowd control
- Theft
- Unauthorised entry
- Public safety

7.3. These potential problems and/or threats can be marked on the site plan. This can then be used to visualise the scale of the problem and the level of cover required. Some areas such as checkouts and entrances/exits may need cover for different activities i.e. to monitor flow of people and to identify people in the event of a theft or similar.

7.4. External CCTV should be position to cover the perimeter, access (egress/ingress) to the building, and other sensitive areas such as diesel storage, power panels, backup generators, etc.

7.5. Where motion detection is deployed the field of vision of the camera must be correctly set to ensure that the field of vision is not reduced to record nothing.

7.6. Internally, CCTV should be positioned to monitor all egress/ingress points of all BT areas and other sensitive areas such as Data Centre, Comms room, common lobby areas etc. should be covered but should not be positioned where they could capture any BT information from screens.

8. Risk Assessment

8.1. In deploying and using CCTV, suppliers should carry out regular assessments of the security risks that they are seeking to cover using CCTV. These assessments should cover the following:

What is the realistic likelihood of the activity happening?

- Low / medium / high

What would be the consequences if the activity was not monitored and/or recorded?

- Minor / moderate / severe
- For example, will the activity result in financial loss or compromise the safety of your personnel or the public?
- Can you prioritise the activities you wish to monitor?
- Could you use alternative (or more cost-effective) methods to tackle the activity such as better lighting, fences or intruder alarms?
- Is the activity likely to be a short or long term issue?

9. Determine the Most Effective Solution

9.1. Once the problem areas and potential threats have been marked on the plan, then an assessment can be made of the most effective solutions. CCTV is likely to be only one of a range of possible options and should be considered in the context of a wider security/safety audit, alongside other measures such as:

- Lighting
- Physical protection / barriers
- Proximity alarms / intruder detection systems
- Improved site design / threat removal

There are, however, several scenarios where a correctly designed CCTV system may be of benefit. These usually fall into one of three broad categories:

- Safety / security
- Deterrence
- Crime investigation

10. Success Criteria

10.1. In deploying and using CCTV, suppliers should carry out regular assessments of whether CCTV has been successfully deployed. These assessments should cover the following:

After detecting an activity, what is a successful outcome?

- Prevention of theft of damage
- Identification of intruder
- Improvement in traffic flow
- Deterring an activity

The success will be determined by a combination of how effectively the system performs and how well it meets the operational requirements.

How often will you expect a successful outcome?

(i.e. How effectively / reliably will the task have to be done?)

- All of the time
- On most occasions
- Always during the day, but only occasionally after hours

Frequency of risks and incidents not being addressed by CCTV.

Document Control

Third Party Closed Circuit Television (CCTV) Standard- Good practice

Author: BT Security

Issue 1, published 1st August 2016

11. Appendix A

What should be contained in a CCTV policy?

The following list is neither exhaustive nor mandatory but gives good practice indications:-

- Details about the CCTV;
- Objectives of the system;
- Statement of Intent;
- How the CCTV is being used e.g. continuous recording or not, motion sensors, infra-red etc.
- Operation of the system;
- Is it monitored by a Security Guard or does it alarm to an Alarm Management Centre?
- Where the cameras are positioned;
- Where the images are stored;
- Retention period for images;
- Who can access the images;
- Back up;
- Details of maintenance;
- How incidents are managed out of hours;
- Details of the process in place to manage requests for sight of images;
- Details of proactive checks or audits carried out on a regular basis to ensure that procedures are being complied with;
- Roles and responsibilities e.g. the role of the CCTV operator must be defined within a Job Description;
- Clearly defined and specific purposes for the use of information, and details of how these have been communicated to those who operate the system; and
- Stipulations that the use of CCTV must meet local legislation.