Bringing it all together

Norme pour la télévision en circuit fermé des tiers (CCTV) - Bonnes pratiques

Émission 1

Date : 29/07/2016,

Sécurité de BT

Tables des matières

1. Introduction

1.1. Généralités

Ce document expose les directives générales sur les bonnes pratiques concernant l'utilisation de la CCTV par les fournisseurs tiers.

1.2. Contexte

Au cours des dernières années, l'utilisation de la CCTV s'est de plus en plus répandue au Royaume-Uni. À l'origine déployés pour protéger les grands établissements et pour la surveillance des centres urbains, les systèmes de CCTV sont à présent fréquemment installés dans les bureaux, les magasins, les écoles et même dans les véhicules du réseau des transports publics. Le marché est de plus rapidement passé de la technologie d'enregistrement analogique à la technologie d'enregistrement numérique, ce qui a eu un impact significatif sur la conception et la fonctionnalité des systèmes de CCTV.

L'objectif de ce document reste toutefois le même : fournir des directives claires aux utilisateurs non techniciens qui souhaitent acquérir un système de CCTV bien adapté. Cependant, les problèmes de qualité de l'image enregistrée et de l'archivage des données, qui sont des éléments essentiels de tout système de CCTV, sont souvent négligés lors de la rédaction des spécifications.

Les systèmes d'enregistrement CCTV analogiques étaient relativement simples à concevoir car ils étaient reliés essentiellement à l'utilisation de bandes VHS pour capturer les images. Les systèmes d'enregistrement numériques sont, par contre, beaucoup plus complexes à définir. Ils enregistrent sur un disque dur qui ne peut stocker qu'une quantité limitée de vidéo. Lorsque celui-ci est plein, le matériel plus ancien, est remplacé par les nouveaux éléments. Par conséquent, lorsque l'on définit un système, il faut penser à la capacité du disque dur, disposer d'une méthode appropriée pour créer un enregistrement permanent des principaux incidents (par ex. graveur DVD) et utiliser la compression (qui va affecter la qualité de l'image enregistrée). Beaucoup de ces questions sont interconnectées ; c'est pourquoi l'amélioration de la qualité d'une image enregistrée et l'augmentation du taux d'images se font au détriment de la réduction du temps de conservation dans le système. L'un des objectifs clés de ce document est de fournir des conseils quant à ces facteurs complexes.

1.3. Matériel supplémentaire et conseil

UK HMG fournit une fiche de conseil de haut niveau pour la fourniture de CCTV :

Manuel des exigences pour l'opération de CCTV	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378443/28_09_CCTV_OR_Manual2835.pdf

Le Centre pour la protection des infrastructures nationales (CPNI) fournit également des conseils sur la cyberprotection et inclut des sections sur l'utilisation de la CCTV, telles que :

Télévision en circuit fermé (CCTV)	http://www.cpni.gov.uk/advice/Physical-security/CCTV/

Le Commissariat à l'Information (ICO) fournit un code de pratique de CCTV :

Dans l'image : Un code de pratique de protection des données pour les caméras de surveillance et les informations personnelles	https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

L'Institut Britannique de Normalisation (BSI) dispose également d'un code de pratique que l'on peut se procurer :

BS 7958:2009 Code de pratique de gestion et de fonctionnement de la CCTV	http://shop.bsigroup.com/Browse-By-Subject/Security/Electronic-Security-Systems/cctvstandards/

Exigences de sécurité des fournisseurs de BT :

Exigences de sécurité des fournisseurs de BT V1.1	http://www.selling2bt.com/working/BTSupplierSecurityRequirements/index.htm

L'Autorité du secteur de la sécurité (SIA) dispose d'informations sur les exigences de licence pour l'utilisation de la CCTV dans les lieux publics :

Surveillance CCTV des lieux publics	http://www.sia.homeoffice.gov.uk/Pages/licensing-cctv.aspx

2. Objectifs

2.1. Le but de ce document est de fournir des conseils généraux de sécurité afin de vous aider en tant que fournisseur de BT, en vous donnant des directives générales sur les bonnes pratiques de l'utilisation des systèmes de CCTV dans vos installations et en faisant référence à d'autres sources d'informations qui peuvent vous être utiles.

2.2. En tant que fournisseur de BT, vous allez être contractuellement obligé d'assurer que les informations de BT et celles des clients de BT qui vous sont confiées sont correctement protégées pour assurer leur confidentialité et leur sécurité. Vous devez respecter ces exigences et vous référer à votre contrat et aux Exigences de sécurité des fournisseurs de BT (voir Section 1.3 ci-dessus) pour plus de précisions.

2.3. La CCTV doit faire partie d'un système de sécurité et ne devrait pas être utilisée seule. Bien qu'elle permette de réduire la quantité du personnel de sécurité et son redéploiement vers d'autres activités de sécurité, elle ne peut pas le remplacer.

2.4. Sous sa forme la plus simple, le système de CCTV consiste en une caméra de télévision reliée par un lien de transmission, tel qu'un câble, à un écran situé dans une salle de garde ou à un point de contrôle central. Des systèmes plus complexes utilisent plusieurs caméras et écrans ou un seul écran avec un système de commutation pour afficher les images de la caméra l'une après l'autre. Les dispositifs complémentaires tels que les enregistreurs qui commutent automatiquement en réponse à un signal d'alarme peuvent être utilisés.

2.5. L'utilisation de la CCTV peut aider à vérifier si une alerte de sécurité est réelle et est souvent vitale pour les enquêtes postérieures aux incidents, mais seulement si les images sont suffisamment bonnes pour identifier ce qui s'est produit et si elles peuvent être utilisées pour le maintien de l'ordre public ou pour vous assurer et assurer BT ou le tiers que les incidents sont traités de façon appropriée.

2.6. Un éclairage extérieur aide le personnel de sécurité et augmente les capacités du système de CCTV s'il est soigneusement conçu et utilisé. Les systèmes de CCTV efficaces peuvent aider à éviter les incidents ou même à identifier la planification d'activités. La bonne qualité des images peut fournir des preuves cruciales au cours d'une enquête et peut aider au maintien de l'ordre public. Elle peut aussi être utilisée comme alarme si elle est associée à un détecteur de mouvements.

2.7. Si vous avez engagé du personnel qui utilise un équipement de CCTV, il faut vous certifier qu'il est sont dûment licencié par l'Autorité du secteur de la sécurité (SIA) et que ces licences continuent à être valables pendant qu'ils utilisent l'équipement de CCTV pour vous. L'absence de ces licences requises est considérée comme une infraction pénale. Ceci est particulièrement important si l'équipement de CCTV est déployé dans des positions fixes ou qu'il dispose d'une fonction panoramique, d'inclinaison et de zoom et où les opérateurs : surveillent proactivement les activités des membres du public, qu'ils soient dans des lieux publics ou dans une propriété privée ; utilisent des caméras pour se centrer sur des activités de particuliers en contrôlant ou en dirigeant les caméras vers les activités d'une personne ; utilisent des caméras pour rechercher des individus ; utilisent des images de CCTV enregistrées pour identifier des individus ou pour enquêter sur leurs activités.

2.8. L'utilisation et l'objectif du système de CCTV doivent être enregistrés comme partie de votre politique de sécurité, qui doit être documentée et conservée pour prouver sa conformité. L'Annexe A présente la suggestion d'une liste des aspects que cette politique peut couvrir.

3. Qualité des images enregistrées

3.1. Avant d'installer un système de CCTV, il faut que vous ayez une idée claire de ce que vous souhaitez que le système fasse et de la façon dont il doit le faire. Ceci doit comprendre avec précision ce que vous voulez visualiser et à quel endroit, par ex. reconnaître le visage

de quelqu'un qui franchit une porte, lire le numéro d'immatriculation d'un véhicule ou enregistrer un type d'activité particulier, tel que traverser une pièce, changer de l'argent ou une agression.

3.2. La résolution appropriée, le niveau de compression et le nombre d'images par seconde seront déterminés par ce que vous souhaitez visualiser sur les enregistrements. Si vous ne parvenez pas à voir l'enregistrement, c'est qu'il n'est pas adapté. Il ne faut pas s'attendre à ce que l'amélioration des fonctionnalités, telles que les contrôles de zoom fournissent davantage de détail.

3.3. Un bon moyen d'assurer que le système est capable de remplir les exigences est de réaliser un test subjectif. Installez une caméra et trouvez un volontaire qui franchisse la porte ou qui gare une voiture au lieu qui vous intéresse et enregistrez des images. Ceci doit être fait dans les mêmes conditions que celles dans lesquelles on prévoit d'utiliser le système – la performance du système peut être différente lorsqu'il y a plusieurs caméras qui sont enregistrées.

3.4. La qualité des images enregistrées ou imprimées peut être différente de l'affichage en direct. La qualité des images ne doit pas être compromise pour permettre d'en comprimer davantage dans le système. Il y a cependant la possibilité d'utiliser une échelle mobile de la qualité d'image selon le temps écoulé depuis l'enregistrement. Par exemple, une vidéo de haute qualité à haute cadence pour les premières 24 heures, avec une compression qui augmente progressivement ou une cadence décroissante par la suite, mais qui conserve les images utiles pendant au moins 20 jours. Ceci va dépendre de la nature de l'installation et du type d'enregistrements à effectuer.

3.5. Pour assurer une qualité continue de l'enregistrement, il est essentiel de réaliser une maintenance régulière de tous les aspects du système - en particulier la mise au point de la caméra, le nettoyage des lentilles, les boîtiers, etc.

3.6. Un périmètre adéquat et l'éclairage du lieu (pour faciliter l'observation naturelle et pour la sécurité personnelle) complété par un éclairage infrarouge ou similaire, selon le cas, doivent également être assurés pour permettre de capter une image de CCTV satisfaisante à tout moment, de nuit comme de jour, qui permette de détecter l'image d'une personne sur l'écran - c'est-à-dire qui occupe au minimum 50 % de la hauteur de l'écran. C'est pour cela que ce système est utilisé comme une aide pour le contrôle de l'accès ou à des fins de reconstitution d'incident.

3.7. Le système doit pouvoir être enregistré en permanence et s'il est contrôlé « en direct », il sera d'autant plus facile de répondre en cas d'incident ou de détecter des signes d'intrusion. La mise en place d'un plan de réponse est également essentielle.

3.8. Les caméras en place doivent être conservées en bon état de marche (et non pas hors service et/ou défectueuses). Les heures affichées sur les caméras doivent être exactes.

3.9. Un contrat de niveau de service (SLA) doit être mis en place avec le responsable de la maintenance du tiers pour assurer la réparation des caméras défectueuses en temps voulu.

4. Stockage

4.1. L'accès au système et les images enregistrées doivent être contrôlés pour éviter leur falsification ou leur visualisation non autorisée. Les méthodes de protection électronique qui requièrent un logiciel ou du matériel propriétaire peuvent entraver une enquête si elles empêchent que les images soient fournies à des tiers autorisés. Les méthodes physiques de contrôle de l'accès, par ex. le système placé dans une salle verrouillée sont tout aussi efficaces si elles sont correctement documentées. Ceci afin d'assurer le maintien de l'intégrité des images stockées.

4.2. Il est important que les enregistrements couvrent une période suffisamment longue pour aider aux enquêtes. Leur conservation au-delà de 20 jours peut être utile dans certains cas, mais ne doit pas affecter la qualité des enregistrements plus récents.

4.3. Il doit être possible de protéger des images ou des séquences spécifiques, identifiées comme importantes pour une enquête, pour éviter leur remplacement avant qu'un enquêteur puisse les visionner ou les extraire.
4.4. Les exigences contractuelles de BT déterminent la conservation des images durant 45 jours (exigences SBCA) ou 20 jours (Exigences de sécurité de BT), y compris les images de sauvegarde. Les images doivent donc être conservées au minimum 20 jours.
4.5. Les fournisseurs doivent prolonger cette période dans les cas suivants :
4.6. s'il faut conserver la preuve fournie par la vidéo de CCTV en vue d'une enquête criminelle ;
4.7. si les normes du secteur de la sécurité, tels que NACOSS (Organisme d'Approbation nationale des systèmes de sécurité), stipulent une période de conservation définitive ;
4.8. si cela est déterminé comme exigence nécessaire dans des pays extérieurs au R.U. pour se conformer à la législation locale du pays.
4.9. Une fois expirée la période de conservation, toutes les images de CCTV doivent être effacées (le remplacement est également acceptable).
4.10. Toutes les vidéos de CCTV/enregistreurs vidéo numériques doivent être situées dans des endroits discrets pour éviter tout accès non autorisé et la possibilité d'une visualisation « accidentelle » des écrans de CCTV associés.
4.11. Seul le personnel autorisé doit avoir accès aux enregistreurs de CCTV vidéo numériques et l'accès aux images doit être protégé par un mot de passe.
4.12. Les images de CCTV enregistrées doivent être sauvegardées et leur stockage doit idéalement être situé dans un lieu séparé.

5. Exportation d'images

5.1. En cas d'incident de sécurité, il est important que le système soit capable d'exporter des copies des images de CCTV afin d'apporter de l'aide à l'enquête et à toute autorité policière. Il est peu probable que l'enquêteur soit familiarisé au fonctionnement de votre système. Pour faciliter la rediffusion et l'exportation, un opérateur formé et un manuel de l'utilisateur simple doivent être disponibles sur place.
5.2. L'exportation de volumes moyens et de grands volumes de données peut prendre assez longtemps. L'opérateur doit connaître la période de conservation du système et le temps approximatif de l'exportation de petites (par ex. 15 minutes), moyennes (par ex. 24 heures) et grandes (jusqu'à la possibilité maximale du système) quantités de données.
5.3. Si le logiciel nécessaire à la rediffusion des images n'est pas inclus lors de l'exportation, la visualisation par des tiers peut être empêchée. L'exportation d'un registre des évènements du système ou d'une piste d'audit et de toutes les configurations du système avec les images aidera à établir l'intégrité des images et du système.
5.4. La quantité de vidéo dont un enquêteur aura besoin d'exporter dépendra de la nature de l'enquête. Par exemple, le cambriolage d'un bureau peut n'exiger que quelques photographies ou une courte séquence, tandis qu'un incident plus grave peut impliquer d'exporter tout ce que la vidéo contenait dans le système. Il est essentiel que le système soit capable de faire cela rapidement et vers un moyen approprié. La solution idéale pour de moyens à grands déchargements est que le système ait la capacité d'exporter vers un disque dur « plug-and-play ». Il faut pouvoir réaliser l'exportation et l'enregistrement simultanément sans que cela affecte la performance du système.
5.5. Le système ne doit pas appliquer de compression à l'image quand elle est exportée du système car cela peut réduire l'utilité du contenu. L'image ne doit pas non plus être soumise à une conversion de format qui affecte le contenu ou la qualité de l'image.

6. Revisualisation des images enregistrées

6.1. Le logiciel de revisualisation ou une autre technologie doit permettre aux images de pouvoir rechercher effectivement les prises de vue et de voir toutes les informations contenues dans la prise de vue et celles qui lui sont associées. Il doit être possible de revisualiser immédiatement les fichiers exportés, par ex. sans re-indexation des fichiers ou contrôles de vérification.

7. Localisation des caméras

7.1. Plan du site - La première tâche à effectuer quand on détermine des exigences d'opération, est de dessiner un plan du site sur lequel on indique les zones critiques. Plus on pourra inclure de détails sur ce plan, mieux cela aidera à placer les éclairages et les caméras, en particulier en ce qui concerne les champs de vision et les problèmes environnementaux éventuels, tels que soleil bas ou feuillage.

7.2. L'étape suivante est de définir les problèmes qui affectent le site. Certains d'entre eux peuvent être des menaces générales, tandis que d'autres peuvent être spécifiques à un lieu précis. Les menaces ou les risques courants qui peuvent être identifiés sont les suivants :

- contrôle de foule
- vol
- entrée non autorisée
- sécurité publique

7.3. Ces problèmes et/ou menaces potentielles peuvent être indiqués sur le plan du site. Ceci peut être utilisé pour visualiser l'échelle du problème et le niveau de couverture requis. Certaines zones telles que les caisses et les entrées/sorties peuvent nécessiter de couvrir différentes activités, c.-à.-d. de contrôler le flux des personnes et d'identifier les personnes en cas de vol ou d'acte similaire.

7.4. La CCTV extérieure doit être placée de façon à couvrir le périmètre, l'accès (évacuation/introduction) au local et les autres zones sensibles, telles que l'entrepôt de carburants, les tableaux électriques, les générateurs auxiliaires, etc.

7.5. Si le détecteur de mouvements est activé, le champ de vision de la caméra doit être placé correctement pour assurer qu'il n'est pas réduit et qu'il n'entrave pas l'enregistrement.

7.6. À l'intérieur, la CCTV doit être placée de façon à contrôler tous les points d'évacuation/introduction de toutes les zones de BT et les autres zones sensibles, telles que les centres de données, la salle de communication, les espaces communs, etc. doivent également être couvertes. Il faut cependant veiller à ne pas la placer à des endroits où elle peut capturer des informations de BT à partir des écrans.

8. Évaluation des risques

8.1. Lorsqu'ils déploient et utilisent la CCTV, les fournisseurs doivent effectuer des évaluations régulières des risques de sécurité qu'ils essaient de couvrir en utilisant la CCTV. Ces évaluations doivent recouvrir ce qui suit :

Quelle est la probabilité réelle de la survenue d'une activité ?

- faible/moyenne/haute

Quelles seraient les conséquences si l'activité n'était pas contrôlée et/ou enregistrée ?

- mineure/modérée/sévère

- Par exemple, l'activité résulterait-elle en une perte financière ou compromettrait-elle la sécurité de votre personnel ou du public ?
- Pouvez-vous prioriser les activités que vous souhaitez surveiller ?
- Pourriez-vous utiliser des méthodes alternatives (ou plus économiques) pour aborder l'activité, telles que meilleur éclairage, barrières ou alarmes d'intrusion ?
- L'activité est-elle susceptible d'être un problème à court ou à long terme ?

9. Détermination de la solution la plus efficace

9.1. Prés avoir indiqué les zones problématiques et les menaces potentielles sur le plan, une évaluation peut être effectuée pour déterminer les solutions les plus efficaces. La CCTV est susceptible d'être l'une des solutions possibles et doit être considérée dans le contexte d'une sécurité élargie/audit de sécurité, parallèlement à d'autres mesures telles que :

- Éclairage
- Protection physique/barrières
- Alarmes de proximité/systèmes de détection d'intrusion
- Amélioration du design du site/élimination des menaces

Il existe toutefois plusieurs scénarios où un système de CCTV correctement conçu peut représenter un avantage. Ces scénarios se rangent souvent dans l'une de ces trois catégories :

- Sécurité
- Dissuasion
- Investigation criminelle

10. Critères de succès

10.1. Lorsqu'ils déploient et utilisent la CCTV, les fournisseurs doivent réaliser des évaluations régulières afin d'évaluer si la CCTV a été déployée avec succès. Ces évaluations doivent recouvrir ce qui suit :

Quel a été le résultat positif de la détection d'une activité ?

- Prévention d'un vol ou de détérioration
- Identification d'un intrus
- Amélioration du flux du trafic
- Dissuasion d'une activité

Le succès sera déterminé par une combinaison de l'efficacité avec laquelle le système fonctionne et de la mesure dans laquelle il a répondu aux exigences opérationnelles.

Avec quelle fréquence espérez-vous des résultats satisfaisants ?

(c.-à.-d. avec quelle efficacité/fiabilité la tâche doit-elle être réalisée ?)

- En permanence
- Dans la plupart des cas
- Au long de toute la journée, et seulement occasionnellement en dehors des heures de travail

Fréquence des risques et des incidents non résolus par CCTV.

Contrôle du document

Norme pour la télévision en circuit fermé des tiers (CCTV) - Bonnes pratiques

Auteur : Sécurité de BT

Émission 1, publiée le 1er août 2016

11. Annexe A

Quel doit être le contenu de la politique de CCTV ?

La liste suivante n'est ni exhaustive, ni obligatoire, mais donne des indications quant aux bonnes pratiques :

- Détails sur la CCTV ;
- Objectifs du système ;
- Déclaration d'intention ;
- Comment la CCTV est-elle utilisée, par ex. enregistrement continu ou non, capteurs de mouvements, infrarouges, etc.
- Fonctionnement du système ;
- Est-elle surveillée par un gardien ou déclenche-t-elle une alarme dans le centre de gestion des alarmes ?
- Emplacement des caméras ;
- Lieu de stockage des images ;
- Durée de conservation des images ;
- Qui peut accéder à ces images ;
- Sauvegarde ;
- Détails de maintenance ;
- Comment les incidents peuvent-ils être traités en dehors des heures de travail ;
- Détails du processus en place pour traiter les demandes de visualisation d'images ;
- Détails des contrôles proactifs ou des audits effectués régulièrement pour assurer que les procédures sont respectées avec ;
- Les fonctions et les responsabilités, par ex. la fonction de l'opérateur de la CCTV doit être définie dans une Description du travail ;
- Définition claire et objectifs spécifiques de l'utilisation des informations et détails de la façon dont ils ont été communiqués à ceux qui opèrent le système ;
- Stipulations que l'utilisation de la CCTV doit respecter la législation locale.