CGI

La force de l'engagement[MD]

ÉTUDE TECHNIQUE

La police de demain

Utiliser la technologie pour aider la police à s'adapter à la société changeante

La limitation des ressources force les corps policiers à reconnaître la nécessité de passer d'un modèle de services de police traditionnel à un modèle proactif. Il s'agit donc de modifier les processus et d'adopter une nouvelle technologie afin d'orienter le travail des policiers vers des tâches qui produisent de meilleurs résultats. La présente étude technique examine certaines des nouvelles méthodes utilisées par les corps policiers ainsi que la technologie qui soutient ces processus.

juillet 2014

cgi.com

Table des matières

Le dilemme actuel

Aujourd'hui, les corps policiers se trouvent devant un véritable dilemme. Leur rôle fondamental dans la société est resté le même; ils doivent faire respecter la loi et protéger les citoyens comme ils l'ont toujours fait. Toutefois, leur environnement d'intervention ne ressemble en rien à celui d'il y a 20 ans, voire 10 ans.

Un crime n'est plus nécessairement dirigé de façon locale, mais peut être organisé à des milliers de kilomètres à l'aide de réseaux informatiques situés dans différents territoires.

Les faibles coûts de la technologie et la croissance non réglementée du Web ont créé des avenues lucratives pour les criminels, rendant les citoyens vulnérables à la cybercriminalité et compliquant le travail de la police.

Les attentes des citoyens ont également été stimulées par le mouvement dominant en matière de responsabilisation et la discussion entourant les causes qui retiennent l'attention des médias. Ajoutons le goût indéfectible pour les séries dramatiques dans lesquelles tous les crimes sont résolus. Ce contexte peut exercer une pression sur la police pour engager davantage de poursuites.

Parallèlement, on s'attend de plus en plus à ce que la police élargisse son champ d'intervention; on fait appel aux policiers pour une querelle entre voisins ou un chien nuisible. Les citoyens veulent tout obtenir sur demande, y compris leurs services de police, mais les budgets serrés ne permettent plus de poster un policier à chaque coin de rue, particulièrement en raison du besoin urgent de mettre en place un corps policier virtuel pour lutter contre la cybercriminalité.

La longue tradition de l'attitude du « travail accompli » de la police s'est traduite par sa réaction admirable à ce changement. Les policiers veulent faire tout ce qui est en leur pouvoir pour s'adapter et tirer le maximum des ressources afin de répondre aux besoins. Cependant, le rythme du changement exige une nouvelle approche.

Les corps policiers du monde entier ont réalisé que les ressources ont été exploitées au maximum, et que seul l'abandon du modèle traditionnel de services de police réactifs – résoudre des crimes une fois qu'ils ont été commis – pour mettre l'accent sur un modèle proactif – le programme de prévention – leur permettra de s'attaquer directement à ces nouveaux défis.

DE NOUVELLES PERSPECTIVES

Un modèle proactif requiert un changement de processus et l'adoption d'une nouvelle technologie afin d'orienter le travail des policiers vers des tâches qui produisent de meilleurs résultats. Il peut s'appliquer à cinq secteurs principaux.

- **Une prévention éclairée –** Une approche plus systématique à l'égard de la cueillette et de l'analyse de données révélant les tendances de l'activité criminelle entraînera une utilisation plus efficace des ressources pour cibler le crime et le prévenir.
- **La collaboration entre les organismes –** En travaillant en étroite collaboration avec les autres organismes, la police pourra appréhender les criminels plus rapidement, intervenir de concert lors d'incidents graves et trouver de nouvelles méthodes pour protéger les victimes potentielles.
- **Le passage à la mobilité –** Les corps policiers de demain devront être pleinement informés, même lorsqu'ils travaillent sur le terrain. L'utilisation généralisée des appareils mobiles personnels sécurisés peut répondre à ce besoin. Ces technologies mobiles réduiront également l'obligation pour les policiers de retourner à la station pour rédiger un compte rendu.
- **La surveillance citoyenne –** La police devra mobiliser les citoyens à l'aide des réseaux sociaux et d'autres technologies afin de les inciter à assister la justice. Ils auront la possibilité de recueillir des preuves et de mettre un frein aux activités criminelles.
- **La lutte contre la cybercriminalité –** La police de demain devra être prête à s'attaquer directement à la cybercriminalité en alertant les citoyens de comportements ou de sites à éviter et en suivant de nouveaux comportements et criminels sur le Web.

Cette réalité obligeant les services de police à fonctionner avec un budget réduit ne sera pas de courte durée; elle deviendra la nouvelle norme.

D'après « The police mission in the twenty-first century: rebalancing the role of the first public service »

Reform, avril 2014

Reform (reform.co.uk) est un groupe de réflexion indépendant dont la mission est de trouver une meilleure façon d'offrir des services publics et d'assurer la prospérité économique.

cgi.com

Comme le révèle la présente étude technique, ces nouvelles méthodes de travail et la technologie qui les soutient n'existent pas seulement dans les rêves d'universitaires isolés dans leur tour d'ivoire. Aujourd'hui, elles sont présentées à différents corps policiers, elles contribuent à la gestion réussie des réductions budgétaires et accélèrent la recherche de preuves et la résolution des crimes.

Police de demain

Une prévention éclairée

Le resserrement de l'écart entre les attentes des citoyens et la réalité en matière de prévention du crime est urgent. Pour répondre à ce besoin, la technologie et les méthodes de travail doivent être redirigées vers l'information et les services de police fondés sur le renseignement afin de prévenir la criminalité.

Il est possible d'y parvenir grâce aux actions suivantes :

- l'analyse des données sur l'activité criminelle locale;
- l'exploitation des données massives;
- la surveillance des réseaux sociaux et l'utilisation de ceux-ci pour créer un dialogue;
- les prédictions fondées sur des profils d'activités et de comportements;
- l'automatisation de l'analyse des données numériques sur les cellulaires et autres appareils.

ANALYSE DES DONNÉES LOCALES

Un corps policier équipé d'un système de gestion de l'information efficace pourra non seulement connaître les points chauds de la criminalité dans leur municipalité, mais également les types de crimes commis dans ces secteurs à certains moments de l'année, du mois et même du jour.

Munis de cette information, les corps policiers peuvent déployer uniquement le personnel nécessaire à l'endroit approprié et en temps opportun, maximisant ainsi l'utilisation des ressources. Cette approche pourrait avoir un effet marqué sur la réduction de la criminalité dans un court laps de temps.

EXPLOITATION DES DONNÉES MASSIVES

Les occasions de prévention de la criminalité sont plus nombreuses dans notre société branchée, et la police dispose d'une quantité de flux de données pour prévenir la criminalité. Le recours à l'analyse des données massives donne une portée énorme à la police en faisant ressortir les profils d'activités douteuses.

SURVEILLANCE DES RÉSEAUX SOCIAUX

L'observation des conversations sur les réseaux sociaux permet de déceler les signaux révélateurs parmi tout le bruit, et d'anticiper ainsi les problèmes. La technologie peut contribuer à donner un sens à ce « bruit » social et à orienter la police en direction des risques potentiels.

Les messages sur Twitter peuvent, par exemple, révéler les intentions violentes d'un groupe d'amateurs de football lors d'un match à l'étranger. La police pourrait alors réagir en multipliant sa présence au site du match pour intercepter les agitateurs. Dans certains cas, la police n'aurait qu'à intervenir sur les mêmes médias sociaux pour calmer les esprits en informant immédiatement la communauté virtuelle qu'elle exerce une surveillance.

DÉFINIR LES PROFILS

Une autre approche consiste à prévenir la criminalité au sein des criminels ou des gangs de criminels connus. En ciblant une région ou un groupe de personnes, l'analytique se concentre sur un groupe de données très précises décrivant leurs mouvements. L'activité criminelle antérieure d'un groupe ou d'une personne est analysée afin de prévoir de façon relativement exacte la suite des événements, selon les profils émergents. En fait, les données historiques constituent un système de prévision rapide de l'activité.

Leçons en prévention ciblée

Un corps policier régional du nord de l'Europe a analysé les données sur un groupe de personnes récemment libérées de prison et a noté qu'elles étaient plus susceptibles de récidiver au cours d'une période précise. La police les a surveillées de près pendant cette période à risque et a communiqué avec elles par l'entremise des services sociaux pour les empêcher de récidiver.

AUTOMATISATION DE LA DÉTECTION NUMÉRIQUE

Il est également possible d'améliorer les processus et de réduire les délais d'analyse des données numériques en optant pour l'automatisation. Grâce à l'amélioration des technologies de reconnaissance faciale et au progrès constant de la reconnaissance automatique de la voix, des gains d'efficacité importants peuvent être réalisés pour permettre au personnel de résoudre davantage de crimes. Aujourd'hui, si un corps policier est muni de la technologie d'analyse de données adéquate, les policiers peuvent analyser eux-mêmes les données d'appareils mobiles, comme les téléphones, les tablettes et les portables, afin de trouver des preuves, plutôt que d'attendre pendant deux ou trois mois que cette analyse soit effectuée par des policiers spécialistes.

Si 40 téléphones mobiles sont saisis au cours d'une enquête, il est possible de brancher les téléphones au système d'analyse et de créer une copie de l'ensemble des données des appareils – y compris les noms, numéros de téléphone, adresses électroniques et autres éléments d'information essentielle – à partir des messages texte, des courriels et des applications.

Ces données peuvent être recoupées avec les données géospatiales, donnant ainsi à la police les lieux d'utilisation de ces téléphones. Grâce à cette information, un enquêteur peut conclure que six de ces appareils contiennent de l'information pertinente et lui permettront d'établir sa preuve. Il obtient rapidement les données de base nécessaires pour enquêter sur le crime, et le temps des analystes est mieux utilisé puisqu'ils ne devront analyser en détail que les six téléphones clés.

La technologie permet également l'établissement de liens entre les données, informant les enquêteurs, par exemple, du nombre d'occurrences d'un nom sur certains appareils. Par conséquent, si une personne affirme ne pas connaître l'un des suspects, la preuve est immédiatement fournie par son téléphone.

Cette information peut maintenant être récupérée simplement en appuyant sur un bouton plutôt que d'avoir recours à des feuilles de calcul complexes, et améliore l'efficacité des policiers.

L'analyse des données permet aux corps policiers de :

- détecter les points chauds de la criminalité;
- surveiller les médias sociaux à la recherche de risques potentiels;
- suivre l'activité des criminels connus sur les médias sociaux en y cherchant des indices qui pourraient révéler des crimes antérieurs ou planifiés;
- gagner du temps lors de l'analyse des appareils électroniques des criminels.

Obtenir des alertes rapides

En 2011, le service de police de Philadelphie a été surpris par une série d'événements éclair rassemblant un grand nombre de jeunes, durant lesquels ils commettaient des vols à l'étalage et des agressions.

Le service de police a appris plus tard que les jeunes avaient publié leur plan plusieurs jours avant les incidents, mais le service ne consultait pas régulièrement les sites de médias sociaux. Il a rapidement remédié à la situation. Aujourd'hui, le service de police consulte les publications sur Facebook, Twitter et les autres médias sociaux afin d'anticiper les incidents pouvant représenter un danger.

cgi.com

CGI

Intégration des services d'urgence

Aux Pays-Bas, 24 corps de police régionaux sont en cours de centralisation. Les 24 postes de commandement seront bientôt réduits à 10 emplacements, ce qui entraîne un examen des processus existants.

À l'heure actuelle, lorsqu'un citoyen néerlandais compose le numéro d'urgence, on lui demande : « Cherchez-vous à communiquer avec la police, les pompiers ou l'ambulance? » La plupart du temps, la réponse est assez simple; toutefois, certaines situations exigent la présence de plus d'un service. Parallèlement, les citoyens ne sont pas toujours certains du service requis, mais veulent obtenir de l'aide rapidement.

Ainsi, les postes de commandement envisagent de poser la question « Comment pouvons-nous vous aider? » afin de dépêcher les personnes appropriées pour intervenir. Par conséquent, tous les services concernés ont accès à la même information dès le départ.

Il s'agit d'un simple changement d'approche qui aura d'énormes répercussions sur le recours instantané aux ressources appropriées pour les incidents les plus graves.

Collaboration entre les organismes

L'augmentation de la collaboration entre les organismes est un catalyseur important du passage aux services de police proactifs. Cette pratique permet à la police de résoudre plus efficacement les crimes et, dans de nombreux cas, de prévenir la criminalité.

À l'avenir, la collaboration entre les organismes sera appuyée par la modélisation prédictive, qui permettra à la police de cibler les situations à risque élevé pour lesquelles un examen minutieux est requis. Les situations comportant des risques de violence conjugale ou de violence envers les enfants en sont des exemples.

Leçons tirées d'une tragédie

En 2013, on a procédé à l'examen d'un cas grave au Royaume-Uni, relatif à la gestion du meurtre de Daniel Pelka, un garçon de quatre ans abusé et privé de nourriture par la mère et son conjoint. Dans le cas de Daniel et dans d'autres cas semblables, les différentes entités concernées, comme la police, les services sociaux, les écoles et les services de santé, ne se sont pas réunies pour analyser le dossier, jusqu'à ce qu'un événement se produise et qu'il soit déjà trop tard.

Les cas comme celui de Daniel mettent en lumière les incohérences dans la tenue de dossiers, les données conservées de façon isolée dans les différents systèmes des organismes, l'insuffisance des moyens et le manque de coopération entre les organismes. L'information requise pour prendre des décisions vitales n'était malheureusement pas accessible ou n'avait simplement pas été partagée. En conséquence, le Royaume-Uni a commencé à mettre à l'essai le Multi-Agency Safeguarding Hubs ou « MASH », un système de protection multiorganisme, afin de promouvoir la communication entre les organismes pertinents de sorte que l'information essentielle soit accessible et permette aux professionnels de prendre les décisions pertinentes en temps opportun.

Environ 30 systèmes MASH régionaux sont en fonction au Royaume-Uni et, malgré le travail de prévention efficace, plusieurs équipes responsables de ces systèmes sont submergées par les dossiers en attente de traitement. La recherche de l'information sur les dossiers se fait majoritairement de façon manuelle et le partage des données nécessite beaucoup de temps. Les données sont souvent entreposées et peuvent donc être périmées, sans compter qu'elles sont, la plupart du temps, uniquement consultées pour les cas les plus graves. Ainsi, l'escalade des cas les moins graves n'est pas encore optimale.

La technologie peut améliorer les systèmes MASH et autres systèmes multiorganismes en permettant aux personnes autorisées d'accéder aux données en temps réel, de sorte que les professionnels concernés puissent prendre rapidement les mesures nécessaires.

De cette façon, si les policiers devaient intervenir dans un cas de violence conjugale, ils pourraient avoir accès, à partir de leur appareil mobile sécurisé, à de l'information leur indiquant que les services sociaux assurent déjà la protection des enfants et qu'un des parents possède, par exemple, des antécédents de violence.

À l'heure actuelle, lorsque les policiers se rendent à une adresse, ils ignorent si des enfants y habitent et doivent poser la question sur place. Cette information pourrait leur permettre d'adapter leur méthode d'intervention afin d'assurer la sécurité et la protection de la victime.

Cette information, ainsi que d'autres données comme celles énumérées ci-dessous, pourrait même être fournie au téléphoniste lors de l'appel initial.

- Nombre d'appels reçus dans le passé
- Permis d'armes à feu liés à l'adresse
- Connaissance de la résidence par les autorités locales
- Nom du membre du foyer connu des services de renseignement ou ayant un casier judiciaire
- Enfants domiciliés à cette adresse

Ces données accroissent la possibilité de collaboration entre les organismes et accélèrent les interventions.

CRÉATION DE PARTENARIATS

La collaboration entre les organismes est pertinente puisque la responsabilité de la protection du public n'incombe plus à un seul organisme. Les organisations judiciaires et autres entités, comme les services de santé, d'incendie et d'éducation, veillent aussi à la protection des citoyens. Les organismes bénévoles et juridiques ont tous des rôles à jouer.

L'aisance de la coopération entre les organismes et les personnes issues de différents domaines peut s'accroître au fur et à mesure que la capacité de la technologie à examiner les processus propres à la collaboration entre les organismes se renforce.

Prenons l'exemple de la Police National Database au Royaume-Uni, où l'échange d'information entre les corps policiers régionaux est devenu la norme.

Leçons tirées de la Police National Database

La Police National Database (PND) du Royaume-Uni a été mise en place à la suite du meurtre de deux enfants de dix ans, Holly Wells et Jessica Chapman. L'affaire a mené à la recommandation visant l'échange d'information par les corps policiers locaux.

L'homme finalement reconnu coupable des meurtres avait eu des démêlés avec différents corps policiers locaux, mais avait déménagé régulièrement de sorte qu'un profil complet n'avait jamais pu être établi. Le cas échéant, il aurait très certainement été déclaré dangereux pour les enfants et n'aurait jamais pu obtenir un emploi de concierge dans une école pour filles.

La Police National Database est devenue entièrement opérationnelle en 2011. Elle permet de consulter des dossiers sur les criminels et leurs activités dans une base de données centrale. Elle rassemble l'information de plus de 43 corps policiers distincts ainsi que d'un certain nombre d'autres organismes d'application de la loi du Royaume-Uni. L'objectif de son utilisation est de repérer rapidement et facilement l'information sur les activités antérieures des criminels, quel que soit leur lieu de résidence.

Maintenant, les corps policiers n'ont plus besoin de consacrer du temps ni des ressources aux demandes d'information auprès d'autres organismes. Mais, surtout, ils peuvent procéder à des vérifications précises sur des suspects et trouver de l'information vitale pour prévenir les crimes, comme le terrorisme et la violence envers les enfants, avant qu'ils ne soient commis.

La technologie au service de la collaboration entre les organismes

- Consultation des données de dossiers pertinents par les agents de première ligne à partir de systèmes multiorganismes au moment opportun
- Utilisation de données à jour afin que les policiers puissent prendre des décisions éclairées sur la protection des personnes vulnérables ou la possibilité d'une récidive
- Établissement de contrôles de sécurité de sorte que seules les personnes autorisées puissent consulter les données
- Création de bases de données liées pouvant être répertoriées et consultées par les organismes pertinents, au besoin

Le passage à la mobilité

Malgré les progrès des technologies mobiles, les corps policiers n'exploitent pas pleinement leurs possibilités.

La possibilité pour les policiers de se connecter à un ordinateur central à l'aide d'un appareil mobile personnel pourrait réduire la chaîne de communication. Les policiers n'auraient plus à consacrer de précieuses minutes aux appels à la station pour obtenir de l'information. À l'aide de leurs appareils mobiles sécurisés, ils pourraient transporter l'information avec eux sur la route.

De même, l'enregistrement de la déclaration d'un témoin sur un appareil mobile est loin d'être pratique courante. Les policiers finalisent toujours le processus à leur retour à la station.

ACCÈS À L'INFORMATION

La possibilité pour les policiers d'accéder à l'information requise à distance leur fait gagner un temps précieux. Elle élimine également la nécessité de demander à leurs collègues de chercher l'information requise dans un système central et de la leur transmettre.

L'accès mobile à l'information permet au policier de savoir immédiatement que le suspect qu'il est sur le point d'interpeller est connu de cinq corps policiers en raison de son comportement violent et d'infractions à main armée.

Cette technologie est déjà offerte et est entièrement évolutive. Elle offre l'option de limiter la mise en œuvre initiale à un système peu volumineux et d'y ajouter des applications au fil du temps afin de le perfectionner.

Leçons tirées des services de secours de la ville d'Helsinki

Les services de secours de la ville d'Helsinki, en Finlande, tirent actuellement parti des technologies mobiles pour accomplir leur travail. À l'aide d'un système de localisation automatique de véhicules, le poste de commandement et les équipes de secours sur le terrain peuvent échanger de l'information en temps réel.

Grâce à cette information, les services de secours peuvent s'assurer que les équipes appropriées se rendent le plus rapidement possible aux sites d'incidents. Elle permet également à ces équipes d'être prêtes à intervenir en leur fournissant de l'information à jour sur les risques liés aux édifices, notamment en leur signalant la présence de produits chimiques dangereux.

Une carte détaillée permet au poste de commandement de guider, d'informer et d'assister les équipes sur le terrain. En outre, les équipes ont immédiatement accès aux détails, notamment sur les bornes d'incendie à proximité et les autres services publics pouvant leur être utiles.

Grâce à ce système, les services de secours de la ville d'Helsinki peuvent s'assurer que les équipes sont bien préparées pour intervenir lors d'incidents précis et que l'équipement est rapidement accessible et utilisé de façon efficace.

Avantages de la technologie mobile pour les corps policiers

- Présence accrue des policiers dans les rues pour lutter contre la criminalité
- Réalisation d'économies grâce à la réduction des espaces de bureaux coûteux
- Accélération des procédures administratives permettant d'économiser temps et argent

La surveillance citoyenne

Les citoyens reconnaissent leur part de responsabilité en ce qui a trait à leur propre sécurité. Ils commencent à participer plus activement à la protection de leur collectivité.

Le nombre de personnes qui se mobilisent lorsqu'un enfant est porté disparu prouve que les citoyens possèdent la volonté d'aider les policiers.

En outre, les citoyens sont de plus en plus portés à former des équipes de surveillance de quartier ou des groupes de discussion sur l'application WhatsApp. Tandis que les corps policiers explorent les meilleures façons d'utiliser ces ressources, il ne fait aucun doute que les groupes formés par les citoyens ont une incidence considérable sur les services de police.

Cette motivation grandissante des citoyens à renforcer la sécurité publique peut être exploitée par la police pour accélérer la résolution des crimes et même les prévenir.

Leçons tirées de Burgernet aux Pays-Bas

Aux Pays-Bas, depuis 2010, la police demande l'aide des citoyens pour résoudre les crimes. Pour ce faire, elle leur signale les incidents en leur envoyant une alerte par SMS, par téléphone ou à partir d'un système d'information géographique au sein du système Burgernet (« burger » signifiant « citoyen » en néerlandais). Dès qu'un employé du poste de commandement est averti d'un cambriolage ou de la disparition d'un enfant, il crée une alerte Burgernet.

Les participants à Burgernet reçoivent un message vocal ou un message texte leur donnant une description claire de la personne ou du véhicule afin qu'ils gardent l'œil ouvert.

Si un participant aperçoit la personne ou le véhicule en question, il compose le numéro sans frais de Burgernet et est automatiquement mis en communication avec le poste de commandement. L'employé communique ensuite l'information aux policiers. Lorsque l'incident est clos, tous ceux qui ont participé au processus Burgernet reçoivent un message leur communiquant les résultats.

Grâce aux efforts des participants de Burgernet, des suspects ont été pris en flagrant délit, des personnes disparues ont été retrouvées et la police a reçu des renseignements utiles. Le système a connu un énorme succès; plus de 1 000 appels à l'action sont émis par Burgernet chaque mois, dont 10 % ont conduit à l'arrestation du suspect et 20 % ont conduit indirectement à l'arrestation de criminels.

PARTICIPATION CITOYENNE ACCRUE

L'accroissement de la participation citoyenne contribue à établir la confiance au sein de la collectivité et à la conserver. Les citoyens deviennent des partenaires connus qui servent de « capteurs sociaux » pour la police.

ComProNet, (« Community Protection Network »), un autre projet néerlandais visant à réduire la criminalité liée aux incidents locaux, est également à l'essai en Belgique. L'objectif de ComProNet est de réunir les citoyens, la police, les entreprises, les pompiers et les professionnels de la santé dans un même réseau de sécurité afin qu'ils puissent partager leurs expériences et leur expertise.

À l'aide d'une application pour téléphones intelligents, les propriétaires et gestionnaires de bars et de restaurants peuvent alerter la police d'incidents qui se sont produits ou qui sont sur le point de se produire dans le secteur. Ces signalements sont automatiquement transmis aux policiers les plus près afin qu'ils se présentent rapidement sur place et préviennent l'incident.

Les citoyens peuvent jouer un rôle encore plus important dans le cadre de ce projet. En cas d'accident, l'application permet d'alerter les gens ayant une formation de secouriste et se trouvant dans le secteur pour qu'ils viennent rapidement porter assistance aux victimes. Faire appel aux compétences de citoyens volontaires et responsables procure un soutien supplémentaire aux policiers lorsque leurs ressources ne suffisent pas.

Utilisation de la technologie pour augmenter la participation citoyenne

- Collecte électronique d'information sur les crimes auprès des citoyens
- Analyse automatique des données pour en dégager les tendances
- Participation citoyenne en temps réel pour intercepter les criminels
- Signalement des crimes par voie électronique pour permettre aux citoyens de renforcer leur propre sécurité

CGI

Un crime invisible?

Une jeune fille de 17 ans achète des billets en ligne pour un festival de musique et s'aperçoit qu'elle a utilisé un site Web frauduleux. Elle perd 300 €. Le site frauduleux est situé dans un autre territoire et les recours sont limités, mais le fait reste qu'elle est victime d'un crime.

Si une personne s'était introduite dans son domicile et avait volé 300 € de son sac à main, la police aurait pu voir la scène de crime, relever des empreintes digitales et tenter de retrouver le voleur.

La lutte contre la cybercriminalité

La cybercriminalité est un domaine d'intérêt émergent et à croissance rapide pour les forces de l'ordre. Elle provient de l'omniprésence d'Internet, dont le nombre d'utilisateurs est passé de 16 millions à 1,7 milliard depuis 1995. D'ici à 2015, il y aura plus d'appareils interconnectés que de personnes sur la planète.[1]

Nous vivons maintenant dans deux mondes distincts, physique et virtuel, régis par des règles différentes. Dans le monde virtuel, les criminels peuvent facilement commettre des escroqueries, et les cyberintimidateurs peuvent aisément attaquer les gens sous le couvert de l'anonymat et ainsi causer des dommages équivalents à ceux des agressions physiques. Les réseaux numériques comportent un faible risque et sont très payants pour les criminels, surtout du fait qu'une bonne partie des crimes ne sont pas signalés. On estime à 378 millions le nombre de victimes de cybercriminalité chaque année. En 2013, le coût mondial total de la cybercriminalité était de 113 milliards de dollars américains.[2]

Par conséquent, le travail de la police sur le terrain ne peut plus être axé uniquement sur l'application de la loi. Tandis que les crimes traditionnels constituent une préoccupation constante, la cybercriminalité continuera de lancer de nouveaux défis aux prochaines générations de policiers.

De nombreux corps policiers arrivent difficilement à composer avec la cybercriminalité, encore moins à la définir. Les incidents isolés sont difficiles à détecter et à résoudre, et traduire les criminels en justice peut être problématique, car nombre d'entre eux sont situés dans des pays étrangers. De plus, la croissance rapide et continue de la technologie présente des occasions toujours grandissantes pour la cybercriminalité.

ACCENT SUR LA PRÉVENTION

Dans certains pays, aux Pays-Bas et au Royaume-Uni, par exemple, des unités distinctes de cyberpolice ont été spécialement formées pour détecter et prévenir la cybercriminalité. Ces pays reconnaissent le fait que les services de police du monde virtuel exigent une approche différente.

Pour être efficaces, les activités de la cyberpolice doivent faire appel à la collaboration des fournisseurs de services Internet et des administrateurs de sites Web afin que les gens puissent cibler et signaler la cybercriminalité efficacement.

La prévention est l'une des armes les plus efficaces contre la cybercriminalité. Lorsque les citoyens sont avertis des dernières pratiques frauduleuses, ils peuvent prendre des mesures pour se protéger.

Les données devront jouer un rôle de plus en plus important dans la détection de la cybercriminalité. Par exemple, la police peut se servir de l'analyse prédictive pour relever une activité douteuse et avertir les citoyens de ne pas utiliser certains sites ou de les fermer avant qu'ils ne fassent trop de victimes. Les analyses de données massives fréquentes et automatisées peuvent aider la police à relever les comportements inhabituels et à fermer les sites frauduleux plus rapidement.

Avantages de la technologie pour les corps policiers luttant contre la cybercriminalité

- Définition de profils pour détecter les activités potentiellement frauduleuses
- Suivi de la cybercriminalité dans l'ensemble des territoires
- Sensibilisation des citoyens sur les sites ou les nouveaux procédés malhonnêtes à éviter
- Collaboration avec d'autres organismes pour informer les jeunes sur la cyberintimidation

[1] UK National Security Strategy, « A Strong Britain in an Age of Uncertainty », 2010.

[2] 2013 Norton Report, l'une des plus importantes études menées sur la cybercriminalité chez les consommateurs, selon les expériences de plus de 13 000 adultes dans 24 pays.

Conclusion

Le modèle traditionnel de services de police n'est plus approprié à notre société en constante évolution. L'adoption d'une nouvelle approche est la suite logique de l'amélioration continue des services de police pour répondre aux besoins de la société. La croissance rapide de la même technologie qui est à l'origine des nouveaux défis en matière d'application de la loi crée également de nouvelles occasions d'optimiser les interventions et l'efficacité des corps policiers.

Les activités de transition vers la nouvelle génération de services de police peuvent tirer parti des meilleures pratiques existantes et des techniques novatrices en déploiement abordées dans la présente étude, notamment :

- les services de police fondés sur le renseignement;
- les modèles d'échange de données pour soutenir la collaboration entre les organismes;
- les nouveaux canaux de communications augmentant la participation citoyenne;
- les solutions mobiles favorisant l'efficacité du déploiement des ressources;
- l'analytique prévisionnelle contribuant à la lutte contre la cybercriminalité.

La technologie peut être très efficace pour déployer les ressources de façon adéquate, en temps opportun et à l'endroit approprié. Elle constitue une approche ciblée sur les crimes traditionnels et virtuels.

Nous observons un changement de cap dans la façon dont les organismes, les citoyens et la police collaborent. La technologie appropriée continuera de favoriser l'échange d'information entre toutes les parties.

Lorsque les policiers sont avisés de la présence d'enfants à l'étage d'une maison où ils se présentent pour un cas de violence conjugale, ou qu'un groupe d'amateurs sportifs chahuteurs cherchent les ennuis, ils sont mieux renseignés et ont la possibilité d'adopter une approche proactive. Ainsi, la police peut intervenir avant qu'un crime soit commis et économiser du temps et de l'argent, empêcher la souffrance des citoyens et même sauver des vies.

Un regard neuf sur les méthodes de travail révèlera de nouvelles occasions d'innover en vue d'accroître la collaboration de la police avec d'autres organismes et les citoyens afin de créer une société réellement plus sécuritaire pour l'ensemble de la population.

Nous serions heureux d'aider votre entreprise à s'adapter aux changements s'opérant dans la société. Pour de plus amples renseignements, visitez www.cgi.com/securitepublique ou écrivez à government@cgi.com.

POURQUOI CHOISIR CGI

CGI a acquis une compréhension exhaustive de l'application de la loi et de la protection du public en Europe, en Australie et en Amérique du Nord, fondée sur les liens étroits avec ses clients dans ce domaine. Les organismes d'application de la loi collaborent avec CGI parce que nous comprenons les défis avec lesquels ils doivent composer et avons une vaste expérience de l'intégration de systèmes entre organismes. Nos solutions novatrices aident ces clients à adopter des méthodes de travail modernes et efficaces et transforment leurs activités afin d'accroître la participation des citoyens et ainsi créer une société plus sécuritaire.

cgi.com

À PROPOS DE CGI

Fondée en 1976, CGI est un fournisseur mondial de services en technologies de l'information (TI) et en gestion des processus d'affaires qui offre des services-conseils en management, des services d'intégration de systèmes et de gestion déléguée. Grâce à ses 68 000 membres présents dans 40 pays, CGI a un bilan inégalé de 95 pour cent de projets réalisés selon les échéances et budgets prévus. Nos équipes s'arriment aux stratégies d'affaires des clients afin d'obtenir des résultats probants sur toute la ligne.

cgi.com