



Directives pour la prévention des délits postaux

Groupe «Sécurité postale» de l'UPU

Version 1.1

Berne 2023

Bureau international de l'UPU

Table des matières	Page
1. Introduction	4
2. Vue d'ensemble et objectifs	4
3. Évaluation des risques	6
4. Techniques et principes de l'évaluation des risques	6
5. Bâtiments et installations	7
6. Équipements et technologies	11
7. Courrier	11
8. Finances	12
9. Employés	14
10. Clients	16
11. Autres personnes présentes, voisins et communauté	17
12. Maintien de l'ordre	18
13. Utilisation frauduleuse des postes	18
14. Services de sécurité et d'enquête	19
15. Bilan et conclusions	20
Appendice A	21

1. Introduction

Les communications électroniques et les nouvelles technologies ont profondément transformé la façon dont les services postaux mènent leurs activités. Après avoir opéré historiquement sous la forme de monopoles protégés, les services postaux sont maintenant en concurrence dans un environnement plus exigeant au sein duquel les pressions exercées par les clients et le marché déterminent la mesure dans laquelle les opérateurs désignés atteignent ou non leurs objectifs commerciaux.

Si les opérateurs désignés souhaitent rester des entités commerciales viables, ils doivent faire tout ce qui est en leur pouvoir pour faire en sorte que leurs produits et services de base et exclusifs proposent des éléments dont la valeur est supérieure ou égale aux offres de leurs concurrents. Dans cet environnement, l'une des exigences essentielles est que les services, les produits et les capitaux soient disponibles, en sécurité et protégés, et que les personnes travaillant dans l'environnement postal, de même que les clients, se sentent en sécurité et appréciés à leur juste valeur.

Une chance unique se présente aux opérateurs désignés du monde entier pour appuyer la croissance des activités postales grâce à des initiatives de qualité en faveur de la sécurité, ce qui améliorera encore la qualité des services proposés aux clients.

Compte tenu de la mondialisation du commerce et du commerce électronique, il faut maintenant plus que jamais proposer des services postaux de qualité et sûrs, non seulement dans le domaine de compétence d'un opérateur individuel, mais également au sein du réseau international. Significativement, dans ce contexte, il est essentiel d'avancer dans la compréhension des principes de la prévention des délits et des actes de mal-honnêteté dans l'ensemble de l'environnement postal.

S'il est d'usage que des enquêtes judiciaires soient menées en réaction à des délits, l'objectif étant de déterminer l'identité et les méthodes des auteurs de ces délits, il est tout aussi important de reconnaître la nécessité de mettre en place des stratégies efficaces et proactives de prévention incitant les clients et les employés à faire confiance à la poste. Ces stratégies doivent être poursuivies en adoptant une approche globale dans le cadre de laquelle la prévention des délits, les enquêtes et le renseignement judiciaire jouent individuellement un rôle essentiel dans la conception et la mise en place d'une prévention efficace des délits.

L'objectif du présent document est de présenter à l'ensemble des opérateurs désignés une approche ciblée et progressive des idées et des stratégies de prévention des délits qui puisse servir de liste de contrôle face aux problèmes de sécurité. Dans le même temps, il cherche à présenter des directives générales utiles aux membres de l'UPU dans toute leur diversité, avec des informations et des propositions sérieuses. En dernier lieu, la question de la valeur ultime des stratégies de prévention efficaces et de la nécessité de les mettre en place sera traitée en partant du constat que, si les produits et services ne sont pas protégés, les clients des postes ne peuvent pas y accéder.

Ce document s'adresse évidemment aux professionnels de la sécurité et du maintien de l'ordre des Pays-membres de l'UPU. Il est également conçu de façon à donner des idées et des perspectives aux responsables et aux employés des postes, aux collaborateurs externes qui contribuent à la protection des postes ainsi qu'aux clients. La solidité et la capacité de survie des postes du monde entier dépendent en premier lieu de la sécurité et de la prévention, qui permettent d'assurer la protection de leurs actifs de valeur.

2. Vue d'ensemble et objectifs

Pour que la prévention des délits fonctionne dans une organisation ou une entreprise, il convient d'adopter une approche globale dans laquelle tous les éléments sont interconnectés. Voici certains des principaux aspects sur lesquels doit agir une stratégie efficace de prévention des délits:

- Si elles sont menées de façon réactive et portent leurs fruits, les enquêtes servent un double objectif: elles permettent de traduire les auteurs de délits devant la justice et de déterminer les éventuelles lacunes au niveau de la sécurité qui ont permis la commission du délit.
- Une stratégie efficace de prévention des délits cherche à faire participer et à sensibiliser l'ensemble des employés, à tous les niveaux, aux rôles et responsabilités qui sont les leurs en matière de sûreté et de sécurité, de même qu'aux avantages que revêt pour eux le fait de profiter d'un environnement de travail plus sécurisé.

- Une approche inclusive de la formation et de la sensibilisation des employés permettra de susciter chez eux un sentiment d'acceptation et d'engagement grâce auquel ils pourront se mettre en première ligne de la sécurité et de la prévention.
- La sécurité physique joue un rôle important pour améliorer au sein de l'entreprise la sûreté et la sécurité de ses employés, de ses actifs, de son équipement, de ses clients, etc. Néanmoins, c'est l'efficacité de la gestion au niveau opérationnel qui détermine au bout du compte la réussite de la mise en œuvre.
- Une stratégie efficace de prévention des délits maintient un juste équilibre entre les contrôles minimaux nécessaires, d'une part, et l'acceptation et le soutien maximal des employés, d'autre part.
- Le fait de comprendre les raisons pour lesquelles un délit est commis n'est pas simple, mais peut ouvrir des perspectives pour mettre sur pied une stratégie de prévention des délits.
- L'objectivité, la responsabilité et le professionnalisme du personnel des services de sécurité et d'enquête ont des répercussions positives sur le soutien apporté par les employés, leur acceptation des mesures prises et l'aide qu'ils peuvent apporter.
- La communication dans l'ensemble de l'organisation (d'un bout à l'autre de la hiérarchie), ainsi qu'avec les clients, les collaborateurs et les organisations connexes au sujet des besoins en matière de sécurité et des façons de les satisfaire, est incontournable pour garantir l'efficacité de la stratégie.
- Il est impossible de détecter et de prévenir efficacement un délit dans un milieu cloisonné. Voilà pourquoi il est vital de développer des partenariats (à l'interne et à l'externe) et de faire participer la communauté.
- Pour réussir, la meilleure approche à adopter est l'«approche d'équipe», qui passe par une stratégie de prévention clairement comprise et bien acceptée avec des responsabilités particulières et des objectifs proactifs axés sur la qualité et les projets. Il convient d'adopter une perspective de résolution de problèmes.
- Il est de la responsabilité des professionnels de la sécurité de communiquer efficacement avec les employés et les cadres au sujet des risques et des avantages liés à la sécurité et à la prévention.

Une stratégie judicieuse de prévention des délits n'est pas une approche fondée seulement sur les mesures de sécurité physique. Il s'agit d'un concept dans le cadre duquel les éléments de base sont l'élaboration et la mise en place de stratégies constructives, de contre-mesures et de plans d'action. Il va de soi que les plans de sécurité contiennent tous des failles et qu'il faudra toujours faire face à des attaques criminelles, mais une approche efficace permettra aux spécialistes de la sécurité de tirer les enseignements des nouveaux défis à relever et des procédures d'évaluation continue; ainsi, le contrôle doit être intégré au plan de prévention.

Dans les grandes lignes, la prévention des délits repose sur les principes suivants:

- Évaluation de la valeur et de la vulnérabilité des entités ayant besoin de protection.
- Évaluation des menaces, des risques, des occasions et des influences dans le milieu qui pourraient entraîner ou avoir entraîné une activité délictueuse.
- Conception et mise en application de contre-mesures, de stratégies, de systèmes et/ou de procédures susceptibles de limiter l'envie et la possibilité de commettre des délits.
- Évaluation continue de l'existence de contre-mesures, de stratégies, de systèmes et/ou de procédures ainsi que de leur efficacité lorsqu'ils ont été mis en place.
- Formation des clients, des employés et des autres acteurs des opérateurs désignés afin qu'ils signalent les incidents aux autorités compétentes aux fins de conservation des informations, l'objectif consistant à évaluer la situation de façon plus approfondie et à prendre les mesures nécessaires pour résoudre le problème.
- Sensibilisation et responsabilisation continues de l'ensemble des employés.

L'objectif premier de la prévention des délits est la généralisation de la sensibilisation et de la responsabilisation à tous les niveaux de la hiérarchie et auprès de l'ensemble des employés de l'entreprise. C'est un concept facile à comprendre, mais difficile à mettre en œuvre dans la durée. Il s'agit d'ailleurs du premier défi à relever pour les professionnels de la sécurité.

3. Évaluation des risques

L'argent, les stocks, les propriétés et les bâtiments, l'équipement et, surtout, les employés constituent les actifs d'une entreprise ou d'une société. Il existe également des actifs immatériels comme la confiance des clients, l'image de marque, les informations et données exclusives/de l'entreprise ainsi que la place au sein de la communauté. L'ensemble de ces actifs peuvent être diminués ou perdus en raison des multiples menaces d'activité délictueuse auxquelles est confronté un opérateur. Pour ce qui est des employés et des clients, ils représentent aussi bien l'élément essentiel des opérations commerciales que des sources potentielles de risques et de menaces. Ainsi, ils doivent être soutenus et protégés tout en se voyant interdire la possibilité de mener des activités illégales ou dangereuses: c'est un exercice de recherche d'équilibre parfois périlleux, mais nécessaire, pour les professionnels de la sécurité.

À l'origine de la sensibilisation à la sécurité et de la prévention, on trouve l'évaluation des risques. Cette évaluation doit, cela va de soi, toujours être directement associée à la valeur et à l'exposition des actifs. Dans la mesure où les risques prennent des formes diverses et changent en permanence, il existe différentes techniques et différents principes à envisager pour les évaluer. S'il est certain que tous les risques ne peuvent pas être éliminés, la difficulté pour les spécialistes de la sécurité réside dans le fait qu'ils doivent faire preuve d'une vigilance constante par rapport à l'exposition au risque de l'organisation, mais également qu'ils doivent réévaluer et modifier en permanence la stratégie de sécurité lorsque la situation évolue, ce qui se produit régulièrement.

Le présent document se concentre en grande partie sur le domaine essentiel que constitue l'évaluation des risques, telle qu'elle s'applique de manière ciblée à la protection des différents actifs et services qui fondent un opérateur désigné moderne. En outre, des suggestions d'approches visant à réduire l'exposition et les risques seront proposées, tout en sachant qu'il est impossible d'identifier et d'éliminer l'ensemble des risques, tout comme il est impossible de couvrir l'ensemble des approches qui pourraient permettre de contrôler ou d'éliminer les risques. Comme toujours, l'outil le plus important à la disposition du spécialiste de la sécurité est son discernement professionnel, qui s'appuie sur l'expérience et l'analyse.

Les domaines d'exposition des actifs et d'évaluation des risques ci-après seront évoqués de façon détaillée dans les sections ci-dessous:

- Bâtiments et installations, en mettant l'accent sur la prévention des accès non autorisés et des attaques externes.
- Équipements et prévention des vols et des sabotages.
- Vols de courrier et menaces sur le courrier.
- Actifs financiers et vols et détournements internes/externes.
- Employés et menaces qui pèsent sur eux/qu'ils font peser.
- Protection des clients et contrôles d'accès.
- Autres occupants des installations partagées et contrôles d'accès.
- Utilisation frauduleuse des postes, par exemple envoi de marchandises dangereuses, de pornographie, de drogues et d'autres articles interdits, contrefaçons de timbres/machines à affranchir, fraude ou envois piégés.
- Assistance aux forces de l'ordre et coopération avec leurs agents.
- Services de sécurité en sous-traitance.

4. Techniques et principes de l'évaluation

Un bon point de départ pour l'évaluation des risques est de tenter d'évaluer la valeur des propriétés et des actifs ainsi que des coûts qu'engendrerait leur remplacement ou un fonctionnement en leur absence. En un sens, la sécurité peut être envisagée comme des cercles concentriques, le plus haut niveau de protection devant être accordé aux ressources irremplaçables ainsi qu'aux propriétés et actifs de plus grande valeur, indispensables et dont le remplacement prendrait beaucoup de temps. Pour répondre à la question essentielle de ce qu'il faut protéger et du niveau de protection qu'il faut mettre en place, la première chose à faire est de lancer une enquête et une analyse de l'existant en matière de bâtiments/installations, de personnel, d'équipements, de courrier, de finances et de stock. La Direction doit collaborer à l'obtention et à l'analyse de ces

informations. Cela peut avoir comme avantage secondaire de les aider à comprendre les risques pesant sur les actifs essentiels dont ils ont également la responsabilité ainsi que le préjudice potentiel pour l'organisation si ces actifs étaient perdus ou altérés d'une façon ou d'une autre.

Il convient de souligner que, de la même façon que les personnels chargés de la sécurité ne sont pas les seuls responsables de la sécurité, ils ne peuvent pas non plus être la source unique de données, d'information et d'analyses pertinentes en ce qui a trait aux menaces et aux risques pour la sécurité. Il faut pouvoir compter sur un réseau de contributions de la part des cadres, des employés, des forces de l'ordre et de la communauté afin de réussir l'évaluation des risques. Il est important de mener les recherches nécessaires et de tisser des contacts avec les personnes pertinentes afin de fournir des éléments pour une analyse efficace.

Les forces de l'ordre sont une source d'information inestimable pour l'analyse des délits et l'évaluation des risques. Au niveau local, on peut compter sur elles pour transmettre des informations et des observations sur les menaces et les activités délictueuses dans la communauté au sein de laquelle un établissement opère ou doit être implanté. Là où il existe des statistiques nationales ou locales sur les délits compilées par les forces de l'ordre, celles-ci peuvent représenter un outil essentiel pour évaluer les risques dans différents domaines et différentes communautés. Il convient de tisser et d'entretenir des liens avec les forces de l'ordre, car leurs membres constituent une ressource importante pour l'analyse des délits ainsi que des partenaires précieux pour répondre aux menaces et aux attaques.

Outre les outils des forces de l'ordre permettant d'analyser les communautés, il est important de tenir compte d'autres sources d'information aux fins d'évaluation des risques. Par exemple, les organisations communautaires et de voisinage peuvent être en mesure de fournir des points de vue et des informations uniques. Il est possible d'étudier les données disponibles, par exemple les études et analyses sociologiques ainsi que les études environnementales sur la densité de population et la composition de cette dernière, les services disponibles (police, pompiers, etc.) et d'autres informations et rapports pertinents. Il va de soi que la composition d'une communauté et le brassage relatif de populations urbaines/périphériques/rurales peuvent avoir une influence importante sur la nature des menaces et des risques, donc sur l'approche à adopter sur le plan de la sécurité.

Les enquêtes portant sur la sécurité constituent un outil spécifique essentiel pour les professionnels de la sécurité. Une évaluation des risques efficace doit s'appuyer sur une enquête bien conçue pour permettre d'orienter l'investigation de façon logique. S'il n'existe pas de format d'enquête préétabli (ou seulement sous forme de projet), il serait dans l'intérêt supérieur des responsables de l'analyse des risques de commencer par tracer leur plan d'action. L'enquête devrait être conçue de façon à traiter les objectifs spécifiques de l'évaluation. Pour mettre sur pied un format d'enquête efficace, il est judicieux de recueillir le plus possible de points de vue.

Idéalement, il faudrait recueillir les points de vue des cadres et des employés et réunir les compétences variées de l'équipe chargée de l'enquête. On peut envisager d'utiliser des questionnaires pour approfondir autant que possible différentes informations auprès des cadres, des employés, des clients et de la communauté. Il est important de garder à l'esprit que les éléments et les analyses dont les spécialistes de la sécurité disposent avant l'enquête peuvent leur permettre de définir un format d'enquête réaliste et ciblé susceptible de servir de feuille de route et de liste de vérification de grande valeur afin de garantir la réussite et la pertinence de l'évaluation. Cette approche a également l'avantage de faire mieux accepter les changements à tous ceux qui sont consultés et qui participent et d'accroître leur mobilisation. Si les formats spécifiques des enquêtes portant sur la sécurité seront très variables en fonction de la nature et de la finalité de l'évaluation, il s'agit en premier lieu de disposer d'un plan logique traitant des principaux risques, préoccupations et occasions déterminés par la population cible de l'enquête/les clients et l'équipe chargée de l'examen.

5. Bâtiments et installations

Lorsqu'ils envisagent la sécurité, la plupart des gens réfléchissent à la sécurité physique des bâtiments, des centres et des installations. C'est un bon point de départ pour commencer à penser à la mise en application des directives de sécurité. Néanmoins, comme cela sera précisé dans la suite du présent document, ce n'est que le point de départ, et les questions de sécurité des bâtiments et des installations sont complexes, comme l'est tout ce qui compose une approche globale et exhaustive de la sécurité. En outre, à l'heure d'envisager la

sécurité des bâtiments et des installations, les gens réfléchissent trop souvent à l'après, c'est-à-dire aux évaluations de sécurité menées après la construction. En fait, les directives et les normes de sécurité devraient plutôt être appliquées aux nouvelles installations en amont, ce qui coûterait moins cher pour apporter les modifications nécessaires. Les spécialistes de la sécurité ne doivent pas oublier que la perfection n'existe pas et que l'environnement postal, toujours plus concurrentiel, nécessite d'appliquer des analyses rigoureuses coûts-avantages, même dans le domaine incontournable de la sécurité. En valorisant la sécurité auprès de la haute direction, il convient de faire preuve de modération et il est souvent conseillé d'être en mesure de présenter différents niveaux de protection avec une analyse sérieuse des coûts, des avantages et des risques inhérents aux différentes options.

Les principes de la sensibilisation à la sécurité doivent être appliqués dès les premières étapes de la planification des bâtiments et installations (c'est-à-dire avant même leur construction). Dans la mesure du possible, l'évaluation des risques doit être menée à bien sur le terrain et analysée avant le début de la construction. Comme cela a été indiqué ci-dessus, une bonne sensibilisation à la sécurité dépend de l'efficacité de la communication et de la coopération dans l'ensemble de l'entreprise postale. Par conséquent, il convient de mettre en place un partenariat de qualité entre les agents de sécurité et les responsables chargés de la sélection des sites, des achats immobiliers, de la conception architecturale et de la construction des centres. Si les objectifs et les responsabilités des différents responsables chargés de ces domaines ne coïncident pas toujours, la coopération et le soutien sont globalement bénéfiques aux intérêts commerciaux.

À l'heure d'évaluer les sites de construction envisagés, il est important d'utiliser les techniques adaptées et les principes de l'évaluation des risques abordés dans la section 4 afin de répondre à des questions clés:

- Qu'est-ce qu'il y a actuellement sur place?
- Quelle est la densité de population? Quelle est la composition de la population?
- Quel type d'activité criminelle constate-t-on dans cette zone?
- Quelles sont les autres installations présentes dans la zone? Quels problèmes ont été rencontrés sur ces installations et quel est leur niveau de sécurité?
- À quoi ressemble l'environnement physique? Quels sont les avantages et inconvénients dont il convient de tenir compte pour concevoir et construire des installations?
- Quelles autres menaces pourraient se profiler (p. ex. coupure de courant, incendie, effondrement du bâtiment, dégât des eaux)?

Dans le cadre de l'évaluation architecturale, il convient d'envisager les modifications raisonnables de la conception globale qui pourraient renforcer au mieux la sécurité et garantir la sûreté des employés, de l'infrastructure et des clients. Cette évaluation doit également considérer l'emplacement des caméras et des autres dispositifs de sécurité, les contrôles d'accès, les flux d'entrée et de sortie, les clôtures, la signalétique, les aménagements extérieurs, le stationnement et les autres modifications ou améliorations possibles pour des raisons de sécurité. La disposition intérieure des installations est également importante du point de vue de la sécurité afin de définir les éléments à protéger, de déterminer la valeur du bâtiment, de son contenu et de ses services et d'établir la façon dont les accès seront contrôlés à l'intérieur du centre.



Pour les responsables de la sécurité, l'un des principes de base veut que la sécurité commence sur le périmètre extérieur d'une installation et fonctionne en cercles concentriques, avec différents niveaux d'accès avant d'arriver aux zones les plus sensibles, où sont protégés les actifs ayant le plus de valeur. La première ligne de protection est le périmètre extérieur, où la question fondamentale sur le plan de la sécurité consiste à déterminer qui peut avoir accès au site et comment contrôler cet accès. Les contrôles d'accès à l'entrée des installations ouvertes au grand public ne seront pas les mêmes que ceux mis en place à l'entrée des centres où sont entreposés des actifs et des biens de grande valeur. Il est de la responsabilité des agents de sécurité, en collaboration avec les cadres, de déterminer le niveau adéquat des contrôles d'accès et de surveillance du périmètre. Concernant les clôtures, par exemple, toutes les options devraient être envisagées, y compris une signalétique, des clôtures décoratives (pour délimiter les différentes zones et restreindre l'accès de façon discrète) ou du fil barbelé (accompagné d'une alarme ou d'une clôture électrique), de même que l'option consistant à ajouter aux éléments de sécurité physique des agents de sécurité (armés ou non). Tout dépend de ce qu'il y a à protéger, des personnes devant accéder au site et de la nature des environs. Lorsqu'on se penche sur l'installation de clôtures et le contrôle du périmètre extérieur, il est également utile de tenir compte des environs, notamment des arbres, de la végétation et du terrain.

Après le contrôle du périmètre extérieur et les clôtures, les contrôles d'accès constituent le niveau de sécurité suivant. En fonction de la valeur des actifs et des exigences en matière d'accessibilité, il convient de se pencher sur le niveau approprié des contrôles d'accès à mettre en place. Par exemple, le niveau de contrôle souhaité implique-t-il l'utilisation de tourniquets, de portes, de détecteurs de métaux, de cartes d'identification avec photo, de badges d'identification électroniques avec suivi des déplacements ou d'autres dispositifs adaptés? Outre le contrôle des entrées, il est également important dans certaines situations de contrôler les sorties afin de limiter les possibilités de vols ou d'entrée non autorisée, sans oublier qu'il faut prévoir des sorties de secours clairement indiquées dont les portes doivent être équipées d'un système d'alarme. Il existe également d'autres outils efficaces pour contrôler les accès, des plus simples (p. ex. signalétique donnant des indications ou restreignant l'accès) aux plus complexes (p. ex. systèmes de caméras et d'alarmes ou technologies de reconnaissance faciale). Les agents de sécurité sont également le plus souvent des ressources précieuses pour un contrôle efficace des accès. Il convient néanmoins de garder à l'esprit que, plus le niveau de sécurité est élevé, plus son coût augmente. Quel que soit le système d'accès adopté, il est important de prévoir des procédures efficaces et attentives pour recevoir les personnes en situation de handicap (clients, visiteurs ou autres occupants du bâtiment ou du centre) et permettre la circulation des piétons.

À l'heure de prévoir la sécurité du périmètre et les contrôles d'accès à l'entrée/à la sortie, il faut porter une attention particulière à la gestion de la circulation automobile et du stationnement. Les véhicules représentent une menace potentielle, car ils peuvent être utilisés pour transporter des personnes et des articles non autorisés jusqu'à l'intérieur des installations, ou pour faire sortir des articles, de l'équipement, du courrier ou des biens volés. En outre, les véhicules sont l'un des dispositifs les plus largement utilisés et les plus efficaces pour transporter des bombes terroristes dans les installations ou à proximité (que le conducteur et les passagers soient au courant ou non). Pour certaines personnes, le lien entre les infrastructures postales et le gouvernement peut symboliquement faire des installations une cible attractive, en particulier si les lacunes en matière de sécurité sont particulièrement évidentes. Une des méthodes pouvant être envisagée est le contrôle extérieur (et éventuellement intérieur) des véhicules qui pénètrent dans les installations postales et qui les quittent, encore une fois en fonction du risque et de la sensibilité de chaque installation. Ce point doit être mis en balance avec les problématiques de confidentialité et d'efficacité.

Tout au long de la réflexion visant à déterminer le niveau approprié de contrôle du périmètre extérieur, il est important de garder à l'esprit que le degré de contrôle doit se fonder sur le niveau de risque et les menaces, déterminés grâce à une utilisation rationnelle des techniques et des principes de l'évaluation des risques. Même s'il n'existe pas de solution facile ni de garantie d'efficacité lorsqu'un système est conçu pour cerner les menaces réalistes en matière d'accès non autorisé, de sabotage et de terrorisme, il convient tout de même de procéder à l'évaluation des risques.

Au-delà des préoccupations liées à la protection du périmètre extérieur, il est également important de garder à l'esprit que, comme cela a été mentionné précédemment, il y a d'autres couches de sécurité à l'intérieur même des installations avec différents niveaux de contrôles d'accès adaptés qui peuvent varier d'une zone et d'une pièce à l'autre. Cela peut parfois nécessiter différents niveaux de badges d'accès afin de conserver des protocoles de sécurité adaptés. En outre, il convient d'étudier dans quelle mesure il est nécessaire de mettre en place des «chambres fortes» pour surveiller les espèces, les articles de grande valeur et le courrier. En général, les pièces de ce type doivent se trouver à l'intérieur des installations afin de limiter les possibilités de braquage et elles doivent être équipées de contrôles d'accès, de caméras et de systèmes permettant de rendre chacun strictement responsable de ses actes.

Un autre sujet important dont il faut tenir compte à l'heure d'évaluer la sécurité des bâtiments et des installations est le contrôle des clés. Si les clés ne sont pas contrôlées, cela affaiblit la sécurité globale d'un centre. Il est donc essentiel que des procédures soient mises en place pour attribuer, inventorier et transférer les clés et pour surveiller la réalisation de copies. La responsabilisation de chacun implique aussi de mettre en place des procédures strictes de gestion des clés perdues. On peut envisager, le cas échéant, d'utiliser un système à deux clés dans les espaces particulièrement sensibles, nécessitant la présence de deux membres du personnel responsables pour accéder aux articles de grande valeur. En outre, les combinaisons des serrures ouvrant les chambres fortes et les coffres-forts doivent être contrôlées et modifiées de manière régulière, en particulier lorsque les employés changent de service ou quittent l'entreprise.

Les bâtiments et les installations qui ne sont pas occupés vingt-quatre heures sur vingt-quatre et sept jours sur sept doivent être considérés comme des cibles potentielles de cambriolage. La prévention des cambriolages doit, dans la mesure du possible, être intégrée aux installations. Par exemple, un bon éclairage et une bonne visibilité sur l'ensemble du périmètre ont un effet vraiment dissuasif pour les cambrioleurs. Il convient de faire attention aux buissons et aux aménagements extérieurs aux alentours des bâtiments. Un système d'alarme constitue également un outil efficace et dissuasif, en particulier si les forces de l'ordre ou les agents de sécurité ont la possibilité d'intervenir rapidement. L'installation de caméras peut contribuer à décourager et à identifier les cambrioleurs. Les programmes communautaires de prévention des cambriolages – par exemple la surveillance de quartier, dans le cadre de laquelle les communautés œuvrent collectivement afin de lutter en amont contre les délits – peuvent aussi être considérés comme une ressource potentielle de prévention des cambriolages et des délits.

Enfin, en vertu d'une bonne approche de la sécurité, il est sage de mettre au point et d'actualiser, en collaboration avec les cadres responsables de ces questions, des plans d'urgence permettant de faire face à des menaces comme les catastrophes naturelles ou les incendies/explosions, des procédures d'évacuation, les interventions en cas d'alerte à la bombe et d'incidents violents, etc. La réflexion et la planification en amont peuvent permettre de limiter la panique et la confusion qui pourraient régner si quelque chose se produisait, ce qui renforce globalement la sécurité et la confiance des employés et des clients.

6. Équipements et technologies

Les organisations modernes dépendent davantage d'équipements et de technologies dont le coût est élevé. Les interconnexions entre les équipements, les technologies et les personnes sont essentielles pour permettre une production, des mesures et un contrôle efficaces. Néanmoins, cet accroissement du risque de vol ou de sabotage des équipements représente une menace importante pour les entreprises modernes. Ces dernières décennies, la pression de la concurrence et la nécessité de gagner en efficacité ont poussé les postes du monde entier à dépendre de plus en plus des technologies. Cela a entraîné une augmentation des risques dans les trois principaux domaines suivants:

1. Les équipements ou les technologies sont parfois considérés comme des menaces en raison de facteurs comme les licenciements, des employés mécontents pouvant trouver légitime de saboter les équipements en représailles.
2. L'augmentation du coût et de la valeur des équipements a accru le risque de vol.
3. Les technologies complexes peuvent parfois être utilisées par des personnes malintentionnées pour falsifier des données portant par exemple sur la productivité, ou pour cacher des vols ou des détournements.

Dans tous les domaines de la prévention aux fins de sécurité, les risques décrits ne sont pas seulement du ressort des spécialistes de la sécurité, mais ils relèvent également de toute la Direction, et les actions mises en place devraient l'être en partenariat avec l'ensemble des collègues. Il est recommandé d'adopter une approche coordonnée pour assurer la sécurité des employés en plaçant, en utilisant et en entretenant correctement les équipements. De même, avec l'utilisation des technologies visant à contrôler la productivité et à rendre des comptes en la matière, il est important de travailler avec les cadres pour mettre en place et actualiser des systèmes (p. ex. en comptabilité et vérification) et pour introduire des méthodes de protection contre les vulnérabilités pouvant entraîner des actes de sabotage et de piratage.



Les emplacements destinés à accueillir les équipements sont un point important à prendre en considération dans les enquêtes préalables à la construction et à la rénovation. Les équipements chers et contenant des technologies essentielles doivent être placés dans des zones où ils sont susceptibles d'être protégés et sous une surveillance appropriée. Il convient d'envisager de limiter l'accès à ces équipements aux personnes dûment autorisées qui ont besoin d'y avoir accès. Des outils comme les contrôles d'accès, les alarmes, les caméras, les mots de passe et les technologies de lecture de cartes d'accès sont des exemples de mesures de sécurité pouvant être utilisées. Il est également important de disposer d'un système d'inventaire de qualité et d'identifier les équipements au moyen de numéros de série. Lorsque les employés, les contractants ou les clients sont autorisés à sortir des équipements des installations, un système doit permettre de faire un suivi de ces mouvements et de les contrôler. Enfin, il convient de mettre en place des calendriers pour l'entretien des équipements et de tenir des registres permettant de garantir que ceux-ci ne représentent aucun danger, ce qui permet également d'établir les responsabilités de chacun.

7. Courrier

Le service principal offert par les postes du monde entier consiste à garantir le traitement et le transport du courrier en toute sécurité et de façon rapide et fiable. En raison de la valeur et de l'exposition potentielle des volumes importants de courrier expédiés partout dans le monde, les menaces de vol, de braquage et de destruction sont innombrables. Les risques surviennent depuis différents angles – les menaces, par exemple, peuvent provenir de l'intérieur ou de l'extérieur – et leurs répercussions dépendent du volume de courrier, de sa valeur et de la complexité des flux de courrier (p. ex. itinéraires et réseaux). Les professionnels de la sécurité ont ainsi de multiples défis à relever, ce qui peut être décourageant quand on s'aperçoit que des envois seront probablement perdus dans une opération de cette envergure. En revanche, une telle prise de conscience ne doit pas restreindre les efforts déployés pour relever le défi.

Parmi les complexités inhérentes au courrier, on peut citer le fait que la valeur intrinsèque des envois est très variable. Si tous les envois sont importants, il existe des différences entre le courrier de grande valeur et le courrier qui en a moins, et les voleurs potentiels connaissent cette différence. Il est nécessaire de mettre en place durablement un système permettant de séparer et de protéger le courrier et les expéditions de grande valeur. La plupart des postes classent leur courrier dans différentes catégories: recommandé, avec valeur déclarée, certifié ou autres services de courrier spéciaux. Du point de vue de la sécurité, il est important que ces catégories de courrier reçoivent le niveau de protection adapté. Les procédures d'enregistrement, de numérotation, de réception, de transfert de responsabilité en main propre et de suivi doivent être vérifiées et

faire l'objet d'un contrôle à intervalle régulier. Les mouvements, le stockage et le transport de ces envois méritent une attention adaptée en envisageant la nécessité de prévoir des accompagnateurs et des gardes chargés de leur sécurité. Au sein des installations, des dispositifs de sécurité adaptés (p. ex. cabines sécurisées) devraient être mis en place dans les zones de traitement des envois et faire l'objet d'évaluations régulières; la nécessité de contrôles d'accès, de caméras, d'alarmes, etc., devrait aussi être envisagée.

Pendant le transport, le courrier est particulièrement exposé au risque de vol, de détérioration et de destruction. Le Groupe «Sécurité postale» (GSP) de l'UPU a souvent porté une attention particulière à l'utilisation efficace des conteneurs sécurisés, comme les sacs de courrier, les verrous et les scellés. En outre, les systèmes de suivi du courrier de grande valeur et l'utilisation du transfert de responsabilité en main propre constituent des techniques de prévention importantes à envisager afin de garantir la sécurité.

Les colis représentent souvent une cible particulièrement attrayante pour les voleurs en raison de leur valeur potentielle. Des procédures spéciales peuvent s'imposer pour le traitement et le stockage. En outre, les colis ne constituent pas le même type de menace que le courrier ordinaire, dans la mesure où ils sont plus susceptibles de contenir des marchandises interdites et dangereuses ainsi que des bombes. Cette question sera traitée de façon plus approfondie dans une autre section.

Le courrier quittant les installations pour être livré par les facteurs est encore plus exposé aux risques et représente une menace particulière pour les employés. Le braquage des facteurs et le cambriolage des boîtes aux lettres de collecte ou des boîtes relais constituent un problème majeur à certains endroits. Les employés chargés de la distribution doivent être correctement formés afin de ne pas baisser la garde pour prévenir les braquages et de savoir comment réagir pour leur sécurité et leur protection, tout en sachant comment être des témoins efficaces si une enquête était diligentée. La sécurité des employés est la principale préoccupation. Des procédures distinctes peuvent être nécessaires pour traiter les chèques, les espèces et les autres articles de grande valeur en fonction du risque évalué à certains endroits. Lorsqu'un grand nombre de chèques sont déposés sur une même journée, des dispositifs de sécurité supplémentaires ou la présence des forces de l'ordre pourraient être si possible envisagés. Les boîtes aux lettres de collecte ou les boîtes relais devraient être sécurisées et renforcées autant que nécessaire afin de prévenir les vols, et les clés devraient être suffisamment protégées.

Le courrier qui se trouve temporairement sous la responsabilité de contractants et de compagnies aériennes au moment du transport, donc qui n'est plus entre les mains des services postaux, pose souvent des difficultés particulières pour les agents chargés de la sécurité postale. Il est essentiel de collaborer avec les administrateurs des contrats postaux et les responsables et avec les agents des contractants et des compagnies aériennes afin d'assurer un niveau adéquat de sécurité, de responsabilisation et de contrôle. S'il s'agit d'un domaine sensible, il est important de se concentrer sur ces questions, car les contractants ou les compagnies aériennes ont souvent la main sur l'embauche et le contrôle des antécédents des sous-traitants, sur la viabilité des transports, sur le stockage et sur les systèmes de sécurité. Dans la mesure du possible, il est bon de mener régulièrement des enquêtes portant sur la sécurité, de préférence avec le soutien et la participation des membres du personnel du contractant et de la compagnie aérienne/de la sécurité aéroportuaire afin d'évaluer et d'améliorer la protection du courrier placé sous leur responsabilité. Comme dans tous les domaines de la sécurité, les partenariats et l'esprit d'équipe sont l'objectif à atteindre.

8. Finances

Les espèces et les instruments financiers, particulièrement attrayants pour les cambrioleurs, présentent le risque le plus élevé. En raison de son pouvoir d'attraction et dans la mesure où la perte ou le vol de ce type d'actifs peut avoir un impact important sur la santé financière d'une entreprise, il est très important de mettre en place et d'entretenir un système efficace de protection des recettes. Les risques les plus évidents pour les actifs monétaires sont les vols, par des personnes internes ou externes, ainsi que les braquages. Les postes qui proposent également des services financiers ou d'épargne à leurs clients sont souvent les plus exposées. Il est habituellement possible de prendre des mesures à l'égard des vols perpétrés à l'interne par des employés postaux au moyen de contrôles internes stricts passant par la gestion des liquidités et un système de vérification. En revanche, les vols perpétrés à l'externe et les braquages présentent des difficultés bien distinctes, avec le risque supplémentaire de préjudice potentiel pour les employés et les clients.

Comme pour les autres éléments permettant de mettre en place des mesures de sécurité, les techniques de prévention des braquages doivent reposer sur une évaluation et une analyse des risques approfondies. Il est important de connaître le quartier et les niveaux d'activité délictueuse, la valeur et le flux des actifs monétaires à protéger, et la vulnérabilité des installations et des services au guichet, ainsi que leur attractivité pour les délinquants. Après avoir enquêté sur ces domaines au moyen de techniques adaptées et en appliquant les principes de l'évaluation des risques, les responsables de la sécurité et les cadres seront en mesure de s'attaquer aux vulnérabilités. Il est essentiel de former les employés exposés aux risques dans les zones particulièrement ciblées par les délinquants. Leur sécurité en cas de braquage est la priorité. La formation permettra aussi de mettre en place des procédures pour protéger les actifs et contribuer aux investigations potentielles (ce qui peut avoir un effet dissuasif important pour les délits futurs).

Les transformations physiques comme les alarmes activées depuis le comptoir, l'utilisation d'espèces ou de mandats postaux servant d'appâts, les caméras de surveillance et les écrans de protection pare-balles (en particulier dans les installations à haut risque) garantissent une protection supplémentaire et peuvent contribuer aux investigations menées a posteriori. Lorsqu'ils sont bien formés, les agents de sécurité postés à l'entrée peuvent aussi dissuader des délinquants potentiels. Comme cela a été mentionné précédemment, il convient également d'envisager de manipuler les envois de grande valeur et de stocker les liquidités dans des pièces sécurisées situées au cœur des installations afin d'en limiter l'accès. De plus, les responsables doivent avoir conscience du fait qu'une bonne gestion financière et une bonne protection des recettes impliquent de limiter, dans la mesure du possible, la quantité d'espèces manipulées lors des opérations au comptoir afin de limiter les menaces et les pertes.

En outre, il est également nécessaire de garantir une bonne gestion financière et une bonne protection des recettes pour limiter les détournements, les vols et les pertes par les employés. Pour que les employés aient moins de probabilité de commettre des activités délictueuses, des procédures claires de responsabilisation et de contrôle doivent être mises en place et il faut s'assurer que chacun reçoit la formation adéquate pour connaître ses responsabilités financières. Cela doit être appuyé par un système de vérification composé d'opérations systématiques et d'opérations menées par surprise. L'utilisation des technologies de surveillance (p. ex. caméras et contrôles d'accès) peut également dissuader les personnes tentées de commettre des vols.

L'accumulation, le stockage et le transport des actifs monétaires sont des éléments auxquels il faut apporter une attention particulière. Dans la mesure du possible, il convient de limiter l'accumulation de liquidités. Il est essentiel d'être équipé de coffres-forts et d'équipements de sûreté (accompagnés de bonnes procédures de contrôle). Lorsque de grands volumes d'espèces doivent être transportés, il faut envisager le meilleur mode d'envoi, notamment le type de véhicule utilisé, l'opportunité de faire appel à un service de messagerie externe, l'escorte de sécurité, etc.

Si le stock de timbres n'est pas aussi attractif pour les cambrioleurs, il reste un actif ciblé clairement source de risques pour les services postaux. La disparition de stocks de timbres, à la suite d'un vol ou d'un détournement, a une influence négative sur le résultat financier, tout comme les montants perdus après un vol d'argent. Les mêmes types de systèmes de responsabilisation ainsi que de procédures de stockage et de transport mis en place pour les espèces doivent être appliqués pour les stocks importants de timbres. Il convient également de garder à l'esprit que les employés manipulent parfois les stocks de timbres pour tenter de masquer d'autres détournements d'argent; cette question doit être envisagée dans les procédures de vérification interne. Enfin, une attention doit être portée aux risques associés à l'impression et à la destruction de timbres-poste. Les installations dans lesquelles sont fabriqués les timbres doivent faire l'objet de contrôles stricts avec des enquêtes sur place et des examens réguliers afin de s'assurer de l'efficacité des procédures mises en place contre les vols ou la conversion et de vérifier que chacun soit obligé de répondre de ses actes. Un système efficace de destruction des vieux stocks de timbres doit aussi comprendre des examens réguliers, avec des procédures et des mesures de contrôle claires destinées à prévenir le vol ou la conversion par des employés ou des contractants responsables.

9. Employés

Pour être efficaces, les programmes de prévention aux fins de sécurité doivent être compris par les employés de tous les niveaux de l'organisation, qui doivent y souscrire. Si travailler dans un environnement sûr et sécurisé est le souhait de chacun, il est difficile de déterminer les spécificités d'un programme de sécurité donnant aux employés un certain sens des responsabilités et le sentiment de participer au processus en association avec les valeurs d'un encadrement constructif. Il peut s'avérer compliqué, mais essentiel, de faire participer tout le monde au programme par la mise en place de consultations. Le travail l'équipe est la clé de tout.

En ce qui concerne l'engagement de la Direction, le défi consiste à convaincre les responsables du fait que la sécurité relève du bon sens commercial et qu'il faut prévenir les pertes et garantir la sécurité des employés et des clients pour assurer la solidité des résultats financiers. Pour relever ce défi, il faut d'abord que les spécialistes de la sécurité fassent leur part du travail et qu'ils mettent le doigt sur les menaces spécifiques existant dans l'environnement de travail en appliquant de bonnes techniques d'évaluation des risques. Les responsables de la sécurité doivent se réunir avec la haute Direction pour sensibiliser les dirigeants aux risques existants et potentiels ainsi que pour leur transmettre des suggestions pratiques assorties d'estimations de coûts concernant les mesures à prendre face à ces risques. Les idées, les points de vue et les souhaits des membres de la Direction doivent également être entendus afin qu'ils appuient les initiatives et se mobilisent.

Une fois que la haute Direction adhère aux propositions, il faut appliquer ce même processus de consultation, de sensibilisation et d'échange d'idées avec les cadres intermédiaires et les supérieurs hiérarchiques de premier niveau. On peut se heurter à des difficultés particulières à l'heure de collaborer avec ces catégories de responsables, parce qu'ils disposent souvent de peu de ressources et qu'ils considèrent qu'ils assument déjà de nombreuses responsabilités et qu'ils sont tiraillés de toutes parts. Le fait de se montrer compréhensifs, à l'écoute et ouverts à des compromis raisonnables pour coller au «monde réel» peut largement contribuer à atténuer la résistance et à obtenir l'adhésion des cadres intermédiaires et des supérieurs hiérarchiques de premier niveau. C'est également un domaine dans lequel il est essentiel de pouvoir compter sur le soutien de la haute Direction.

La compréhension, la participation et l'engagement des employés sont également des éléments essentiels d'un programme performant de prévention aux fins de sécurité. De bien des façons, les employés constituent la première ligne de défense. Voilà pourquoi il est important que les employés soient bien sensibilisés à la sécurité et que des procédures soient mises en place pour consigner et notifier les incidents. Les employés devraient être invités à observer et à écouter les failles de sécurité, à intervenir dans ces situations, à les mettre en échec et à les notifier dès leur détection. Une fois ces mesures mises en place, les efforts de prévention seront plus efficaces et porteront mieux leurs fruits. Pour y parvenir, il faut un programme de sensibilisation à la sécurité de qualité constamment soutenu et renforcé en appliquant des approches et des techniques multiples, par exemple:

- proposer des programmes d'initiation à la sécurité aux nouveaux cadres et employés, suivis de séances d'information et de formations à intervalles réguliers afin de renforcer la sensibilisation à la sécurité et la responsabilisation;
- élaborer des programmes permettant de proposer des suggestions d'amélioration dont les coordonnées feraient l'objet d'une grande publicité en prévoyant des récompenses et des reconnaissances et en mettant en valeur par la suite les accomplissements;
- rédiger de la documentation écrite, notamment des instructions ou des conseils, des aide-mémoire sous forme d'affiches, des indications et, bien sûr, des politiques et procédures de sécurité consignées par écrit;
- utiliser des supports audiovisuels (p. ex. séquences multimédias, brochures, affiches et présentations PowerPoint) ainsi qu'une combinaison de supports informationnels lors des réunions et dans les espaces où les employés convergent (cafétérias, salles de pause, etc.), ou lors de réunions informelles visant à traiter des thèmes pour lesquels une sensibilisation est nécessaire;
- intégrer la sécurité aux opérations et aux objectifs hiérarchiques (avec l'accord de la haute Direction) en prévoyant une couverture particulière des résultats en matière de sécurité dans les critères d'examen du mérite et pour l'obtention d'une promotion, afin d'obtenir des primes ou des récompenses sous forme de rémunération incitative, ainsi que lors des réunions du personnel habituelles ou spéciales organisées par les supérieurs hiérarchiques et les cadres;
- intégrer la question de la sécurité aux descriptions de poste et aux avis de recrutement;
- mener des examens de la sécurité et diffuser les résultats, qu'ils soient positifs ou négatifs;
- partager les informations disponibles sur les menaces identifiées, les statistiques relatives aux délits et les tendances propres à certains bureaux ou certaines zones;
- organiser des forums et des manifestations pour la prévention des délits à destination des personnels de tous les niveaux de l'organisation afin d'encourager ces personnels à mieux comprendre ces sujets, à prendre leurs responsabilités et à participer;
- publier des notes pour la prévention des délits;

- comparer les normes de sécurité et adopter les pratiques exemplaires dans l'ensemble du bureau ou de l'organisation;
- maintenir une présence et une disponibilité concrètes en matière de sécurité dans les différents domaines de travail afin d'encourager le contact avec les employés et de les informer du fait que la sécurité est mise en place dans leur intérêt.

Pour que ces initiatives aient plus de chances de succès, il est important de travailler en collaboration et avec le soutien d'autres groupes au sein de l'entreprise, par exemple les services chargés de la formation, des ressources humaines et des relations de travail ainsi que des communications.

Travailler avec des syndicats et des organisations du personnel peut être un défi délicat à relever pour les responsables de la sécurité, mais il est important de se concentrer sur le principe fondamental selon lequel la sécurité est à l'avantage de chaque personne au sein de l'organisation. Lorsque les organisations ne baissent pas la garde face aux délits et à la sécurité dans l'environnement de travail, cela peut améliorer la possibilité d'avoir recours à une approche collective et coordonnée de la prévention des délits. L'appui des organisations et leur capacité à communiquer efficacement avec les employés qu'elles représentent sont une des clés de la réussite des programmes de sécurité. Il convient tout de même de garder à l'esprit que les décisions finales en matière de sécurité relèvent des professionnels de la sécurité désignés et de leurs supérieurs hiérarchiques.

Pour les groupes d'employés, les cadres et les travailleurs, la sécurité est une considération importante. Or on peut tracer un lien direct entre la sûreté et la sécurité, d'une part, et la prévention des délits, d'autre part. L'objectif de la sûreté peut être le moteur des programmes de sécurité. Pour les cadres, le personnel chargé de la sécurité peut être les yeux et les oreilles lui permettant de connaître les violations de la sécurité ainsi que les procédures dangereuses et les mauvaises conditions de sécurité, par exemple des portes de sortie bloquées, des équipements laissés à découvert, des matières dangereuses, etc. Ces questions méritent d'être abordées lors des entretiens. La présence de responsables de la sécurité peut permettre aux employés de se sentir en sécurité et, s'ils sont aimables et prévenants, ils peuvent être perçus de manière positive.

Comme cela a été mis en exergue tout au long de ce document, les collègues sont des alliés et partenaires essentiels dans les programmes de prévention aux fins de sécurité et ils coopèrent pour la plupart à l'instauration d'un environnement de travail sûr, sécurisé et à l'abri de tout délit. Dans le même temps, quelques membres du personnel représentent une menace potentielle pour le bien-être de tous et la viabilité de l'entreprise en se livrant à des activités délictueuses ou dangereuses. Ces activités peuvent comprendre le vol, la violence, le sabotage, voire la participation à des attaques criminelles menées depuis l'extérieur en donnant des informations sur le fonctionnement interne ou en prenant part à la conspiration.

En raison du préjudice que peuvent causer quelques employés, il est malheureusement nécessaire de mettre en place des contrôles de sécurité de différents degrés, en fonction du risque et des menaces. Si l'idée du contrôle a parfois une connotation péjorative, il est important d'agir directement sur ces perceptions auprès des cadres et des employés, tout en adoptant une approche juste et mesurée. Le fait de rencontrer les employés et leurs représentants lorsque des évolutions de la sécurité sont envisagées peut avoir un effet positif et permettre d'améliorer le niveau de compréhension, de soutien et de coopération. De bonnes procédures de contrôle peuvent être considérées comme nécessaires et positives, mais également bénéfiques pour la sûreté des employés et la pérennité de l'organisation.

Pour que les procédures de contrôle de sécurité soient efficaces, tout commence au moment de l'embauche. Le contrôle des antécédents régulièrement actualisés avant l'embauche peut permettre d'exclure les personnes indésirables. Après l'embauche, il est important de commencer par un parcours complet d'initiation et une formation professionnelle efficace abordant l'importance des procédures de sûreté et de sécurité et la nécessité de leur mise en place. La formation à la prévention des délits et les séances d'information portant sur des sujets comme les braquages, les vols, la sensibilisation et la prévention, de même que l'importance de contrôles financiers de qualité, peuvent éviter que des problèmes ne surviennent. La participation continue des employés, par l'intermédiaire de formations de remise à niveau et de séances d'information, de même que l'accessibilité de personnels de sécurité se montrant ouverts et attentifs, peuvent porter leurs fruits et inciter les employés à adhérer aux mesures de prévention et de sécurité.

Grâce à une bonne communication et à la participation des employés, ces derniers peuvent être sensibilisés à l'importance et aux avantages des procédures de contrôle, par exemple les badges d'identification, les contrôles d'accès, les détecteurs de métaux, les restrictions d'accès à certaines zones et la séparation des zones de repas et de pause des installations de travail. Les employés peuvent également être incités à signaler les activités délictueuses et les conditions de travail dangereuses, à interpellier les visiteurs non autorisés et les intrus et à faire part aux autorités compétentes des situations suspectes. Il faut également mettre en place des contrôles d'accès pour les véhicules et des mesures de sécurité dans les zones de stationnement.

Outre les contrôles stricts à l'embauche des employés permanents, il convient aussi de faire attention aux employés vacataires et aux autorisations d'accès aux installations dont ils disposent. Dans le cadre des négociations contractuelles, il faut se pencher sur les procédures de recrutement des contractants et les politiques d'examen des antécédents. Les contrôles d'accès pour les contractants et les autres visiteurs doivent être aussi rigoureux que ceux qui s'appliquent aux employés.

Lorsque des évaluations de la sécurité sont menées dans des installations, les employés et les cadres de tous les niveaux doivent être inclus dans le processus et informés des résultats, qu'ils soient positifs ou négatifs. Pour cela, il est possible de mettre en place des entretiens, des réunions de groupe, des questionnaires, des rapports écrits, des présentations ou des visioconférences. Si la charge logistique peut sembler lourde à porter, les avantages au niveau de la qualité des contributions à l'évaluation et de l'acceptation des résultats seront importants. Les employés peuvent rester anonymes ou il existe la possibilité d'inclure leurs coordonnées au processus d'évaluation.

Il est parfois nécessaire pour les professionnels de la sécurité de prendre part aux interactions avec les employés, par exemple lors des procédures disciplinaires, des renvois d'employés et des poursuites pénales. Certes, il ne s'agit pas d'une tâche habituelle, mais il est essentiel de traiter rapidement, équitablement et efficacement la question des employés posant problème. Pour cela, il faut des notes soignées et exhaustives, des mesures de surveillance et des enregistrements des entretiens, et les preuves doivent être convenablement conservées. Il est également nécessaire d'entretenir de bonnes relations avec la Direction et les autres représentants des forces de l'ordre, tout en traitant la question des employés posant problème avec professionnalisme. Si le fait de renvoyer ou de poursuivre un employé peut donner une impulsion positive à la sensibilisation à la sécurité, voire accroître le soutien des employés à la prévention des délits, la question doit être traitée de façon délicate et dans un respect total des principes juridiques et de l'équité.

10. Clients

Outre les employés, il faut aussi protéger les clients afin qu'ils ne subissent aucun préjudice physique dans les installations postales. La confiance des clients peut être sérieusement écornée par les situations dangereuses, pouvant aussi engager la responsabilité juridique de l'opérateur désigné et entacher gravement sa réputation et son image de marque. En outre, les postes doivent également protéger les clients, dans la mesure où les acteurs malveillants utilisent parfois les produits et services postaux pour mettre en place leurs stratagèmes, comme la fraude postale, les envois piégés et d'autres actions dangereuses, préjudiciables, illégales ou répréhensibles. Les clients doivent également être protégés des actes délictueux commis par les quelques employés postaux violant leur confiance en volant ou détruisant le courrier confié au système postal.

Une bonne communication et la sensibilisation des clients à la question de la sécurité peuvent permettre aux opérateurs désignés de servir et de protéger leurs précieux clients tout en limitant l'exposition et les risques pour les postes. Il est important que les clients aient seulement accès aux zones où se déroulent les échanges commerciaux par la mise en place de contrôles d'accès et d'une bonne signalétique aux fins d'orientation et d'information et en veillant à la disponibilité des employés pour les aider au besoin. Pour bien communiquer avec les clients, il faut mettre en place des programmes de formation et de sensibilisation à leur intention. Les brochures et affiches imprimées, par exemple, peuvent prodiguer aux clients des conseils et des orientations au sujet des services disponibles comme des moyens de se protéger. Il peut être utile à ce sujet de travailler avec le personnel chargé de l'information du grand public et des relations publiques ainsi qu'avec le service à la clientèle. Des forums ouverts au grand public dans le cadre desquels les clients sont invités à partager des informations, des observations et des opinions peuvent également s'avérer utiles. Les enquêtes auprès des clients peuvent aussi permettre de traiter les questions de sécurité ainsi que les besoins, les idées et les attentes en la matière.

Si l'objectif est de faire en sorte que tous les contacts avec les clients soient positifs, cela n'est pas toujours possible; il est donc essentiel de mettre en place un système pour permettre aux clients de faire part de leurs préoccupations, réclamations, soupçons et problèmes. Un système de réclamations client peut également traiter les problèmes de prévention aux fins de sécurité et les activités potentiellement délictueuses ou contraires à l'éthique. Lorsqu'il existe un système de réclamations/d'information à destination de la clientèle, il doit être facile d'utilisation et il convient de le faire connaître. Les personnes à contacter et leurs coordonnées doivent être clairement indiquées et faciles d'accès, en garantissant l'anonymat si nécessaire. Il peut être très utile de mettre en place un programme de récompense/reconnaissance (à l'intention des clients comme des employés) à condition de garantir sa bonne gestion.

Il est judicieux sur le plan commercial de traiter les questions de la sécurité et des activités délictueuses en association avec les clients de façon ouverte et positive. Cela montre que l'opérateur désigné s'inquiète pour le bien-être et la sécurité des clients et les considère comme des partenaires: ce qu'ils voient et entendent peut permettre à l'opérateur de prendre conscience des menaces et des lacunes au niveau de la sécurité ou des procédures et ils peuvent faire connaître leurs soupçons en ce qui concerne des activités délictueuses ou contraires à l'éthique. Ce type de partenariat client/entreprise renforce les liens sur la base de la confiance et du soutien réciproques. Dans le même temps, les postes peuvent informer leurs clients de leurs besoins en matière de sécurité et leur expliquer les éventuelles restrictions en réaction à ces besoins. À tous les niveaux, les cadres peuvent accueillir avec satisfaction ce genre d'approche positive du service à la clientèle et lui apporter leur soutien, de même que constater les avantages que peuvent avoir la prévention des délits et la sécurité pour les activités postales.

11. Autres personnes présentes, voisins et communauté

Dans les situations où d'autres entreprises ou organisations partagent des espaces avec les opérations postales, il est important d'envisager les meilleures solutions de collaboration afin d'assurer la sécurité des employés de ces entreprises et organisations et de limiter les menaces potentielles qu'ils pourraient représenter. Cette dernière question peut être délicate, car les opérateurs désignés n'ont que peu d'autorité sur les employés d'une entreprise partageant les mêmes locaux. Le meilleur point de départ consiste à rencontrer la Direction de l'autre groupe afin d'étudier les besoins de chacun en matière de sûreté et de sécurité. Il est tout aussi important de contrôler l'accès aux opérations et actifs postaux des personnes partageant les locaux que de contrôler l'accès des employés postaux. Dans certains cas, cela peut même être encore plus crucial, car l'opérateur désigné ne peut pas influencer les pratiques d'embauche ou de vérification des antécédents appliquées par d'autres entreprises. Chacun doit respecter les politiques en matière de contrôles d'accès, de badges d'identification et de contrôle du stationnement. Dans la mesure du possible, il vaut mieux traiter ces questions avant de commencer à partager des locaux avec des acteurs extérieurs, par exemple au moment des négociations relatives au bail.

Si on pense souvent au quartier dans lequel se trouve une installation comme source première de menace, la communication et la coopération avec les voisins peut également être bénéfique et permettre d'atteindre les objectifs communs de sûreté, de sécurité et de prévention des délits. Les rencontres avec les dirigeants des communautés peuvent s'avérer profitables et permettre d'instaurer une relation de soutien mutuel et de coopération. Les invitations de type «portes ouvertes» pour visiter les installations peuvent mettre la population dans de bonnes dispositions et encourager la transparence. L'accompagnement ou l'aide destinés à mettre sur pied des programmes de type «surveillance de quartier» ou d'autres activités de coopération peut permettre aux opérateurs désignés d'avoir de bonnes relations de voisinage et de bénéficier de ce que voit et entend la communauté pour contribuer à maintenir un bon niveau de sécurité et de prévention des délits. Plus les opérateurs désignés peuvent contribuer à garantir la sécurité des communautés, moins ils devront faire face à des menaces et plus les opérations et les employés seront en sécurité. Cela peut également permettre aux responsables des postes de se bâtir une bonne réputation commerciale.

Le fait de nouer des partenariats avec d'autres entités commerciales (p. ex. institutions bancaires, établissements chargés de garantir la sécurité, autorités aéroportuaires, forums d'entreprises, services de protection des consommateurs et fournisseurs de services de sécurité) peut être positif et permettre de partager les idées et les préoccupations de chacun ainsi que de s'apporter un soutien mutuel. Au niveau international, la coordination avec d'autres opérateurs désignés au sein de l'UPU et du GSP permettra d'intensifier les efforts déployés pour prévenir les délits partout dans le monde. Les organismes gouvernementaux concernés, les autorités de maintien de l'ordre et les magistrats sont également des alliés et des partenaires incontournables dans la lutte contre la criminalité dans le secteur postal.

12. Maintien de l'ordre

Les forces de l'ordre font partie des alliés les plus importants en matière de prévention et de lutte anticriminalité. Des interactions régulières avec les magistrats et les fonctionnaires de police afin de les sensibiliser aux sujets postaux et aux préoccupations en la matière peuvent avoir d'importants effets bénéfiques. En outre, les agents chargés de la sécurité postale peuvent proposer des formations et des consultations à destination des professionnels du maintien de l'ordre et des magistrats pour les aider à comprendre les questions uniques en lien avec les délits postaux.

Comme cela a été mentionné auparavant dans la section sur les techniques et les principes de l'évaluation des risques, les services de police peuvent être une source précieuse de statistiques et d'analyses de l'activité délictueuse en ce qui a trait aux menaces et aux risques dans certains lieux et vis-à-vis de différents types de délits postaux. Dans les quartiers dans lesquels la police est davantage présente, les policiers ont une connaissance incomparable de la criminalité locale, y compris des problèmes et défis liés à la prévention. En travaillant en coopération et en s'appuyant sur cette ressource, les opérateurs désignés comprendront mieux les problématiques de la sécurité postale et les opportunités qu'elle ouvre.

Il est possible d'améliorer la réponse de la police aux alarmes et aux attaques contre les installations postales en prenant des initiatives en faveur de la liaison et en renforçant la compréhension mutuelle. En outre, les opérateurs désignés peuvent aider les agents chargés d'intervenir en jouant leur rôle au sein du partenariat, à savoir en mettant en place des plans d'urgence face à des incidents comme des actes de violence, des braquages, des explosions, des incendies, des cambriolages et des envois piégés. Les opérateurs désignés peuvent partager avec les forces de l'ordre les informations qui sont en leur possession concernant les délits postaux, par exemple la fraude postale, la présence de drogue dans les envois, le blanchiment d'argent, la pornographie, la contrefaçon de timbres, etc.

Les responsables de la sécurité postale peuvent aussi être des partenaires précieux pour les magistrats et les législateurs et leur transmettre des informations importantes pour contribuer à rédiger des statuts, des lois et des règlements applicables aux activités postales portant sur des délits particuliers. Les professionnels de la sécurité postale peuvent former les magistrats et les aider à préparer un procès ou à faire face à des problématiques complexes dans le domaine postal susceptibles de se poser durant les procès; ils peuvent également témoigner. Les agents de sécurité sont souvent les premières autorités qui font face aux attaques ou incidents de nature délictueuse dans les installations postales et ils jouent un rôle essentiel pour la protection des preuves et des lieux où se sont déroulés les faits. Leurs premières observations et leurs premiers témoignages (le cas échéant) sont précieux pour les magistrats afin d'instruire correctement les affaires.

C'est dans ses relations avec les forces de l'ordre et les magistrats que l'intégrité et le professionnalisme des postes sont les plus incontournables. Les affaires pénales doivent bénéficier du plus haut degré de confidentialité, d'attention aux questions de protection des renseignements personnels et d'équité. Les poursuites pénales dans les affaires postales peuvent avoir des conséquences positives en renforçant les normes de prévention applicables aux employés lorsque les affaires sont menées avec le plus grand professionnalisme et le maximum d'équité.

13. Utilisation frauduleuse des postes

Certes, les agents de sécurité assurent la sécurité des installations et des personnes qui s'y trouvent, mais ils doivent également relever un défi important et parfois plus complexe: prévenir l'utilisation frauduleuse des postes. Ces utilisations frauduleuses peuvent porter préjudice aux clients et aux employés et ébranler la confiance dans le système postal. Un programme de prévention efficace doit aussi agir sur des préoccupations comme les bombes et les marchandises dangereuses expédiées par courrier, l'utilisation du courrier pour l'expédition de drogue, les mécanismes de blanchiment d'argent, la pornographie et les allégations mensongères. En outre, il faut également se pencher sur les risques dans le domaine de la protection des recettes, par exemple la fraude contre les opérateurs désignés, la contrefaçon de timbres, la falsification, le vol et la destruction de chèques ainsi que les fraudes à la machine à affranchir.

Il est possible de renforcer les approches adaptées de la prévention de ces problèmes en sensibilisant les employés et les clients au moyen de formations, de brochures, d'affiches d'information et d'autres ressources multimédias. Ces efforts doivent viser principalement à permettre aux employés et aux clients d'être les yeux et les oreilles de la première ligne de prévention. Une fois sensibilisés, ils peuvent reconnaître les irrégularités

et les allégations mensongères et ils savent comment transmettre leurs observations et leurs préoccupations aux autorités concernées. L'établissement du profil des domaines posant problème peut être un outil précieux pour attirer l'attention sur les secteurs les plus utiles et productifs. Tout en étant en mesure de reconnaître un colis potentiellement piégé ou pouvant contenir de la drogue, les employés et les clients devraient aussi savoir à quel moment il convient de contacter les autorités et les responsables. Un programme de récompenses peut permettre d'améliorer la sensibilisation et la participation des employés et des clients.

Les techniques d'échantillonnage, d'établissement de profils et d'enquête peuvent s'avérer utiles pour reconnaître des timbres falsifiés et contrefaits ainsi qu'une utilisation frauduleuse des machines à affranchir. En ce qui concerne l'utilisation frauduleuse des machines à affranchir et des timbres, une collaboration avec des représentants de l'industrie des machines à affranchir et de l'expédition peut permettre de mieux cerner et éliminer les risques de pertes majeures. Les graves menaces potentielles de ce type sont également des sujets sur lesquels le GSP doit absolument travailler et porter son attention. D'autres fraudes contre les postes (p. ex. fraudes à la sous-traitance, à la facturation et à la passation de marchés) peuvent être limitées par l'application d'un programme de vérifications et de meilleures procédures.

Enfin, le fait d'accorder une attention accrue à l'utilisation frauduleuse des postes en faisant appel à des interventions policières et à des poursuites judiciaires à bon escient a un fort effet dissuasif. Il peut être très efficace de rendre publiques les arrestations, les poursuites judiciaires et les peines encourues en cas d'infraction à l'encontre du courrier et du système postal. Ceux qui seraient tentés de commettre des délits peuvent être dissuadés de violer la législation postale s'ils savent qu'ils ont de grands risques de se faire prendre et d'être sévèrement sanctionnés.

14. Services de sécurité et d'enquête

Il existe différentes façons d'avancer vers la réalisation des objectifs de prévention et de les atteindre afin de garantir la continuité des opérations postales et la sécurité des employés et des clients. Les cadres supérieurs doivent décider, vraisemblablement avec l'appui des spécialistes de la sécurité, si la meilleure stratégie est d'employer le savoir-faire et les ressources humaines internes pour la sécurité, ou de faire appel à des ressources externes et de sous-traiter les services de sécurité. De même, en fonction de la flexibilité de l'environnement postal, des décisions doivent être prises concernant le recours de préférence à des services d'enquête internes et externes ou le recours strict aux forces de l'ordre.

À l'heure d'évaluer les différentes options, il faut examiner les nombreux arguments pour et contre une approche interne ou externe. L'évaluation coûts-avantages est sans aucun doute un élément majeur dont il faut tenir compte pour décider des ressources à employer, sans néanmoins oublier les questions en lien avec le savoir-faire, la motivation, la loyauté, l'efficacité, le contrôle et le niveau d'attention portée aux problématiques postales. Les questions juridiques, réglementaires et de mise en application aussi également être abordées.

Que le choix se porte sur le recours à des ressources internes, à des services externes sous-traités ou à une combinaison des deux pour assurer la sécurité, la Direction doit évaluer avec attention les domaines hautement prioritaires évoqués ci-après et les éventuels passifs que devra assumer l'organisation. Les enquêtes sur les antécédents des agents de sécurité (internes ou sous-traités) doivent être approfondies et actualisées à intervalles raisonnables. Les formations à l'entrée en fonction et les remises à niveau doivent être de qualité et aborder les questions et les problèmes concrets. Les politiques relatives à l'autorité des agents – par exemple concernant l'emploi de la force et le port d'une arme – sont des sujets sensibles qu'il convient de mettre au clair. Les politiques devraient également être fréquemment consolidées au moyen de formations et d'exams. Le code vestimentaire des agents est une question moins essentielle, mais qui a son importance, car elle détermine le regard porté par les agents eux-mêmes, les employés et les clients sur les services de sécurité. Il y a des avantages et des inconvénients à recourir à des uniformes, des badges ou des vêtements plus informels et la décision prise aura une influence importante sur l'autorité et la perception des agents.

Comme cela a déjà été évoqué, le coût n'est pas la seule problématique. La haute Direction et les responsables des programmes de sécurité doivent également évaluer les bénéfices et les risques qui, s'ils ne sont pas pris en considération judicieusement, peuvent coûter plus cher par la suite en raison de la perte de recettes, de ressources, de motivation, de réputation et de soutien des clients/du grand public. Ce qui a le plus de valeur dans un bon programme de sécurité, ce sont les bénéfices liés à une réduction ou une élimination de ce type de passifs à venir. Le coût relativement faible grevant aujourd'hui le résultat financier peut permettre de préserver les recettes à venir et de mettre à l'abri l'organisation et ses employés.

15. Bilan et conclusions

En bref, le présent document vise à donner un aperçu des nombreuses facettes que revêt un programme efficace et exhaustif de prévention des délits. Des directives générales ont été fournies dans les domaines de l'évaluation des risques (y compris des techniques et des principes), la sécurité des bâtiments et des installations, la protection de l'équipement, la technologie, le courrier, les finances, les employés, les clients, etc. Les problèmes généraux que pose l'utilisation frauduleuse des systèmes postaux peuvent mener à des interactions professionnelles avec les forces de l'ordre, les magistrats et les services de sécurité et d'enquête.

L'objectif a été d'aborder la sécurité et la prévention des délits de façon globale en tenant compte de la participation des professionnels de la sécurité, des cadres à tous les niveaux, des employés et de leurs représentants, des clients, des groupes communautaires, des partenaires commerciaux et d'autres acteurs avec lesquels les opérateurs désignés entrent en contact dans l'exercice de leurs fonctions. Comme pour l'ensemble des efforts déployés dans le domaine professionnel, plus les personnes avec qui et pour qui nous travaillons nous apportent leur soutien, plus nous avons de chances de réussir.

Ce document n'apporte pas toutes les réponses à toutes les questions et à tous les problèmes complexes susceptibles de survenir en matière de prévention des délits. Il ne propose pas non plus de stratégie parfaite. Les problèmes et les incidents liés à des délits et à la sécurité feront toujours partie des défis que les spécialistes de la sécurité doivent relever en permanence. Les enseignements en matière de coopération, de participation, de flexibilité, d'évaluation et d'analyse, associés à la créativité fondée sur l'expérience des spécialistes et des responsables de la sécurité offrent les meilleures chances de réussite en gardant une ou deux longueurs d'avance sur les personnes susceptibles de nuire aux installations, aux employés et aux clients.

Ce document propose une liste de vérification globale des questions, des préoccupations et des approches à destination des professionnels de la sécurité. Sur la base de ces directives, de ces idées et de ces approches, les personnes endossant des responsabilités importantes en matière de sécurité peuvent formuler des stratégies pour lutter contre des problèmes particuliers et relever les défis susceptibles de se profiler dans le domaine complexe de la sécurité postale et de la prévention des délits. Les possibilités de stratégies diverses à disposition sont aussi nombreuses que les formes possibles d'attaques de nature délictueuse.

Un exemple de stratégie utile élaborée par les services de sécurité et d'investigation de la poste sud-africaine est présenté dans l'appendice, sous le titre «La résolution de problèmes en tant que stratégie de prévention des délits». Cette approche par étapes comprend des méthodes d'identification du problème, une analyse du programme, l'intervention, l'évaluation et le plan d'action. Ce modèle efficace de résolution de problèmes est fourni à titre d'exemple, car il montre la façon dont les responsables de la sécurité peuvent affronter les préoccupations en matière de sécurité et agir sur les aspects et les défis inhérents à la prévention par une planification approfondie, logique et exhaustive.

Nous tenons à remercier les services de sécurité et d'investigation de la poste sud-africaine de nous avoir transmis ce modèle et de nous avoir fait part de leurs idées et travaux innovants pour l'élaboration des présentes directives. Sans leur formidable travail, ce document n'aurait pas pu exister.

Résolution de problèmes en tant que stratégie de prévention des délits

Les agents des services de sécurité et d'investigation sont confrontés à un nombre extraordinaire de situations complexes. Les vols de courrier, les braquages des bureaux de poste, la fraude contre les banques postales, les violations de courrier, les fraudes à la carte bancaire et les vols de liquidités et de stocks sont quelques-uns des incidents qui se produisent pratiquement tous les jours. Les altérations des envois dans les centres de traitement du courrier et l'exploitation des services postaux pour le trafic de drogue sont des problèmes qui se posent continuellement, en dépit des enquêtes menées a posteriori et de l'incarcération des délinquants.

Traditionnellement, on pensait que la seule façon de limiter ces incidents était de mener des enquêtes et de répondre individuellement à chaque cas. Le nombre de suspects inculpés, suspendus ou renvoyés permettait de mesurer dans quelle mesure les incidents étaient traités avec succès. Lorsqu'il semblait qu'un incident était réglé, les recherches étaient lancées concernant l'incident suivant afin de recommencer à enquêter, à suspendre les délinquants et à les placer en détention. Cette stratégie fondée sur les incidents:

- adopte une approche réactive plutôt que préventive;
- repose sur quelques informations glanées auprès des victimes, des témoins et des suspects;
- nécessite de faire appel au système judiciaire pour traiter efficacement tous les incidents.

Trop souvent, les interventions sont inefficaces, prennent beaucoup de temps et ne permettent d'obtenir que peu de résultats concrets. La fréquence des incidents de ce type montre qu'une approche fondée sur les incidents ne permet pas d'agir sur les facteurs sous-jacents.

La théorie de la résolution des problèmes se fonde sur le postulat selon lequel les facteurs sous-jacents sont la cause du problème. Il peut s'agir notamment des facteurs suivants:

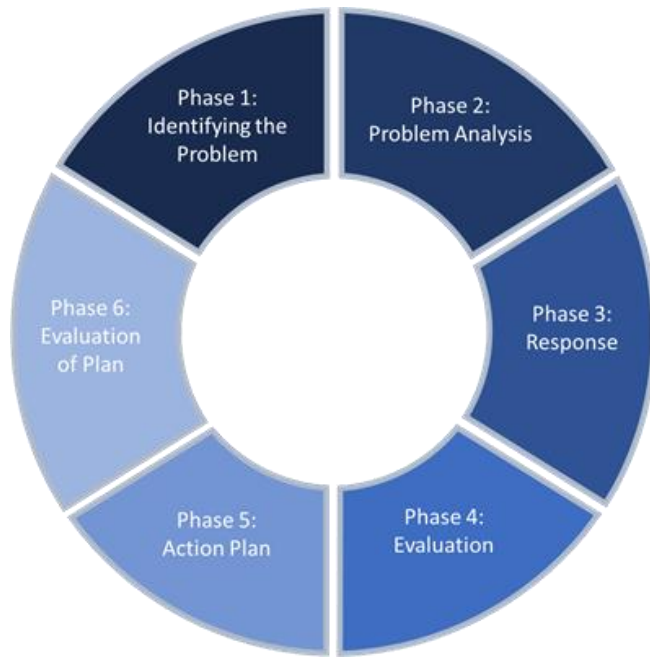
- Environnement physique offrant des occasions de vol ou de braquage.
- Lacunes dans les systèmes permettant la fraude et les vols et les rendant difficiles à détecter.
- Absence d'encadrement ou de supervision efficaces, ce qui peut entraîner des comportements inacceptables susceptibles de provoquer des incidents de nature délictueuse.

Même s'ils découlent de la même cause, ces incidents ne sont que des symptômes: tant que les problèmes sous-jacents ne sont pas résolus, les incidents continueront de se produire.

La résolution de problèmes se concentre sur les causes des incidents, c'est-à-dire sur la façon de les affronter. Cette façon d'aborder les choses permet un équilibre efficace entre les approches réactive et proactive de la sécurité.

En introduisant et en adoptant formellement la résolution de problèmes, le processus de résolution de problèmes devient une activité globalement recevable et reconnue qui fait partie des opérations quotidiennes.

Modèle de résolution de problèmes



Phase 1 – Cerner le problème

Lorsqu'il s'agit d'analyser un problème, par exemple un vol de courrier, un braquage, etc., il convient de mener une analyse détaillée aussi minutieuse que possible. L'installation concernée, le type de propriété, l'heure de l'incident, le mode opératoire, etc., peuvent tous pointer des problèmes différents nécessitant chacun une solution différente.

1. Définir ce qu'est un problème

Un problème est constitué d'un ensemble d'incidents en lien les uns avec les autres et/ou se répétant. Les caractéristiques montrant des occurrences multiples ou un lien entre les incidents sont les suivantes :

- Comportement: l'occurrence d'un comportement habituel est probablement la façon la plus simple de déterminer qu'un certain nombre d'incidents constituent un problème. C'est particulièrement le cas lorsqu'on se concentre sur des problèmes comme les vols de courrier, les braquages de bureaux de poste et les fraudes aux mandats de poste à l'échelle d'une ville ou d'un pays.
- Zone: lorsque différents problèmes de comportement se concentrent sur une zone en particulier, ces problèmes sont cernés en fonction du lieu où ils se produisent, par exemple les altérations et les vols de courrier dans les principales zones de tri du courrier.
- Horaire: les multiples occurrences d'un incident peuvent être définies comme un problème en fonction de leur répétition à une heure, une saison ou un jour de la semaine en particulier. On peut citer comme exemple les altérations des envois en période fiscale, les braquages des bureaux de poste à la fermeture ou les vols de liquidités à la fin du mois.
- Personnes: un problème peut être circonscrit en fonction des délinquants et/ou des victimes, par exemple les syndicats, les caissiers, etc.

2. Cerner les problèmes

Pour cerner les problèmes, il faut :

- réunir les contributions de toutes les personnes occupant des fonctions de service au sein de l'opérateur désigné – agents administratifs, agents de sécurité, caissiers, personnel généraliste, etc.;
- prendre sérieusement en considération les informations remontées par les clients;

- tenir compte des recommandations formulées par les organismes établis – forums de police de proximité, entreprises, pouvoirs publics, syndicats;
- consigner les demandes de renseignements des clients;
- mettre en place des compensations;
- analyser le grand nombre d'incidents consciencieusement consignés par les services de sécurité et d'investigation.

Les médias sont généralement considérés comme les voix de la communauté. Une étude portant sur les articles diffusés dans les médias pourrait laisser entendre qu'une communauté ou un groupe de personnes en particulier a une perception négative d'un problème précis avec l'opérateur désigné ou avec les services qu'il propose (p. ex. corruption).

Différentes autres sources pourraient potentiellement être utilisées pour obtenir des informations aux fins d'identification des problèmes. On peut citer notamment des données issues des appels de service, des réclamations écrites, des appels à l'aide, des statistiques des services de police, etc. Les services de sécurité et d'investigation de chaque région devraient définir leurs sources d'information de proximité plutôt que d'utiliser l'ensemble des informations disponibles.

3. *Hiérarchiser les problèmes*

Le processus d'identification des problèmes mettra inévitablement au jour d'autres problèmes à traiter. Les ressources disponibles étant limitées, il faudra nécessairement hiérarchiser les problèmes cernés. Les problèmes nationaux ou régionaux appellent une analyse intensive, ce qui peut prendre beaucoup de temps. Les agents des services de sécurité et d'investigation peuvent se trouver face à un ensemble de problèmes dont la complexité et l'étendue sont variables. Il leur faudra donc déterminer des critères de sélection, par exemple:

- situation dans laquelle des vies sont en danger;
- intérêt des clients à résoudre le problème;
- probabilité que le problème soit résolu – dans quelle mesure les services de sécurité et d'investigation ont la capacité de résoudre le problème;
- gravité du problème – dans quelle mesure le problème est dangereux, fait scandale, est d'intérêt public;
- conséquences pour la poste – préjudice, dégâts et pertes.

Étape 2 – Analyse du problème

Examiner le problème (cinq questions essentielles)

L'étape suivante consiste à enquêter sur le problème en le décomposant et en définissant l'ensemble des éléments qui le composent.

Pendant l'analyse, il est très important de se poser les cinq questions essentielles, à savoir qui? quoi? quand? où? et pourquoi?

Examiner les renseignements relatifs à la victime, au délinquant et à la situation – À l'heure d'analyser le problème, pensez à réunir suffisamment de renseignements sur la victime, le délinquant et la situation afin de pouvoir élaborer des réponses stratégiques à la prochaine étape. La situation correspond aux circonstances ayant contribué au problème ainsi qu'aux facteurs environnementaux susceptibles d'avoir une influence sur lui (p. ex. conditions d'éclairage, facteurs géographiques et considération météorologiques/climatiques).

Il faut examiner les informations sur la victime, le délinquant et la situation en considérant le problème à travers chacun des facteurs suivants:

- Impact:
 - Dans quelle mesure le problème est-il grave?
 - Qui est touché?
 - Quels autres problèmes subissent les conséquences de la situation?
 - Qui sont les parties intéressées?

- Gravité:
 - Quelles seraient les répercussions si rien n'était fait?
 - Quelle est la perception du grand public? Dans quelle mesure se préoccupe-t-il de la question?
 - Quel est le degré de priorité/le statut de ce cas pour les forces de police?
- Complexité:
 - Dans quelle mesure le problème est-il complexe ou bien enraciné?
 - Existe-t-il des ressources pour le traiter efficacement?
 - Qui est responsable?
- Possibilité de résolution:
 - Dans quelle mesure les personnes, les équipes et/ou la communauté peuvent-elles avoir un impact sur le problème?
 - Si elles ne le peuvent pas, que leur manque-t-il?
 - Quel serait le coût?

Méthodes d'analyse

Voici quelques méthodes que vous pouvez choisir d'utiliser pour analyser le problème:

- Informateurs.
- Analyse de l'incident.
- Observation/surveillance directe.
- Groupes de discussion.
- Entretiens.
- Recherches dans les bibliothèques/sur Internet.
- Rencontres avec d'autres organismes.
- Enquêtes, questionnaires.

Remarque: il ne serait pas surprenant que, pendant l'analyse, le problème doive être redéfini. Il pourrait également apparaître qu'il y a plusieurs problèmes.

Avant d'envisager les réponses stratégiques, définissez clairement le problème. Maintenant que le problème est défini, l'objectif doit être établi, avec l'une des intentions suivantes:

- Résoudre le problème: habituellement, c'est le cas pour les petits problèmes simples dont la résolution nécessite peu de ressources et peu d'argent.
- Atténuer le problème: cela concerne les problèmes persistants et bien enracinés qu'il est impossible d'éliminer totalement.
- Limiter le préjudice ou les répercussions: s'il est difficile de résoudre ou d'éliminer un problème, les équipes de sécurité peuvent être en mesure de limiter ses répercussions pour les victimes, ou pour l'opérateur désigné et/ou sa réputation.
- Redéfinir les responsabilités vis-à-vis du problème: l'équipe doit chercher des moyens de réattribuer les responsabilités mal partagées générant une charge de travail inappropriée pour les services de sécurité et d'investigation. Il convient de reconnaître que les agents de sécurité et d'investigation ne sont pas les seuls responsables de l'ensemble des problèmes en lien avec les délits au sein de l'opérateur désigné (braquages, vols de véhicules, etc.).

Les décisions relatives aux objectifs évoqués ci-dessus seront axées sur les stratégies de l'opérateur désigné dans certains domaines.

Le plus difficile est de concevoir des réponses adaptées à ces problèmes au niveau local. Les problèmes de nature délictueuse n'ont pas une cause unique. En effet, les différents types de délits ne sont pas dus aux mêmes raisons et appellent donc des approches de prévention différentes.

Étape 3 – Réponse

Le choix des réponses (solutions) possibles à apporter n'a qu'une seule limite: l'imagination. La créativité et une approche plus large de la résolution de problèmes sont les clés de la réussite. Les stratégies de résolution de problèmes devraient être orientées sur des problèmes précis. Par exemple, les stratégies mises sur pied contre les vols en général gagneraient en efficacité si elles étaient conçues pour un problème de vol en particulier.

Remarque: la résolution de problèmes doit se fonder sur un engagement à mettre sur pied une réponse précise à un problème particulier dans un endroit donné et des circonstances spécifiques.

À partir de l'analyse du problème, des réponses réactives et proactives seront élaborées par les responsables des services de sécurité et d'investigation et par les parties prenantes concernées, par exemple les syndicats, les forces de police, etc. Nombre de ces parties prenantes ont mis en place des réponses traditionnelles qui continueront probablement d'être reconnues comme des stratégies efficaces pour lutter contre les problèmes.

Étape 4 – Évaluation

L'objectif de la résolution de problèmes est d'agir avec succès sur un problème particulier. Par conséquent, il est essentiel que des méthodes d'évaluation soient mises en place afin de mesurer les conséquences des stratégies de sécurité sur les problèmes identifiés. Aucune organisation ne peut se permettre d'utiliser des ressources précieuses sans indication claire du rapport coût-efficacité. Les avis non étayés selon lesquels l'approche fonctionne ne suffisent plus. À l'inverse:

- il faut pouvoir prouver, ou tout du moins attester, qu'une stratégie particulière est efficace; l'aggravation/atténuation du problème ou le fait qu'il continue de se produire, les économies/pertes financières pour l'opérateur désigné, les dégâts évités et la récupération des actifs et de leur valeur sont quelques-uns des facteurs à prendre en considération à l'heure de déterminer les critères d'évaluation.
- la détermination d'objectifs clairement mesurables établira des normes explicites;
- il faut montrer que le problème a été bien compris.

Étape 5 – Plan d'action

- Équipe: déterminer l'équipe responsable du plan.
- Problème/question: fixer le point de mire du plan.
- Objectif: établir l'objectif du plan (éliminer/réduire...).
- Stratégie: la stratégie doit répondre au critère suivant: que faut-il faire pour atteindre les objectifs de la stratégie?
- Tâche: répertorier les tâches particulières à accomplir:
 - Qui?
 - Où?
 - Dans quel délai?

Remarque: les tâches associées au suivi et à l'évaluation de la stratégie doivent également être réparties.

- Activité: énoncé des résultats par la personne effectuant la tâche.
 - Qui?
 - Où?
 - Quand?
 - Pour quel résultat?

- Stratégie:
 - Résultats (prévus et non prévus).
 - Examen de la meilleure stratégie ou d'autres résultats d'apprentissage.
- Résultats et évaluation du plan d'action: résultats obtenus par le plan et méthodes d'évaluation utilisées pour en déterminer la réussite.
 - Avez-vous réussi?
 - Comment le savez-vous (résultats des évaluations)?
 - Quelles sont les stratégies qui ont fonctionné et celles qui n'ont pas fonctionné?
 - Quels résultats non prévus avez-vous obtenus?

Étape 6 – Évaluation du plan

Il n'est pas nécessaire de procéder à une analyse complexe pour déterminer si les objectifs ont été atteints ou non. Par exemple, si votre objectif était de résoudre ou d'atténuer un problème, ces mesures seront largement quantifiables (p. ex. diminution de 45% des réclamations pour fraude sur les six derniers mois). Les statistiques relatives aux délits et à leur occurrence vous permettront de savoir si vous avez réussi ou non à changer les choses.

Si, à l'inverse, l'objectif était de limiter le préjudice ou les répercussions, la mesure utilisée devra peut-être être davantage qualitative (p. ex. réponses à une enquête auprès des victimes indiquant une plus grande satisfaction à l'égard du service reçu).

La résolution de problèmes implique que chaque agent des services de sécurité et d'investigation cherche des solutions aux problèmes qu'il rencontre chaque jour. Il doit toujours y avoir une justification morale et juridique à l'utilisation des approches et instruments choisis. L'approche ou l'instrument doivent également faire l'objet d'une analyse critique permettant d'évaluer la possibilité de réussir en les employant.

Sans chercher à limiter la réflexion ou la créativité, voici quelques options susceptibles de pouvoir être appliquées pour faire face aux problèmes identifiés:

- Réponse par la mise en œuvre/investigation – Application de stratégies de mise en œuvre/investigation, aléatoires ou dirigées, concernant des problèmes ou questions identifiés.
- Politique/législation/réglementation – Mise en application/adoption de nouvelles politiques, mise en place de nouvelles procédures et adoption de l'utilisation d'une législation publique plus large.
- Médiation/négociation – La négociation, comme moyen de résoudre les conflits, peut être particulièrement utile dans des situations ordinaires pour lesquelles il n'existe peut-être aucune solution acceptable. La négociation fait référence à un processus en vertu duquel des parties en conflit communiquent afin d'atteindre une solution acceptable pour tous.
- Stratégie de communication – Une stratégie de communication peut être utilisée pour limiter les craintes vis-à-vis des délits et la victimisation.
- Permettre aux agents postaux d'être autonomes – Résoudre les incertitudes relatives à la législation, aux politiques ou aux procédures; alerter les victimes potentielles et leur donner des conseils concernant les précautions à prendre pour leur sécurité; sensibiliser les employés postaux aux activités délicieuses potentielles; obtenir l'adhésion en faveur d'une solution/d'un programme, etc. Des moyens de communication comme les courriers électroniques, la radio, la télévision, les brochures et les bulletins d'information peuvent être utilisés dans les campagnes menées contre les délits. Une recherche créative peut ouvrir de nouvelles possibilités, par exemple l'organisation d'ateliers.
- Mobiliser l'ensemble des employés – La mobilisation fait référence aux efforts visant à faire participer l'ensemble des employés postaux et des groupes intéressés, par exemple les syndicats, conjointement ou individuellement, afin de lutter contre les délits en général et de résoudre les problèmes.

- Plans du milieu – Prise en considération des questions concernant le milieu susceptibles de contribuer à un problème/une question, y compris des facteurs comme les routes, les parcs, les parkings, l'emplacement des arbustes, l'éclairage des rues, etc. Ces questions peuvent apporter une réponse immédiate à une préoccupation identifiée.
- Autres organismes/parties prenantes – Mécanismes formels et informels de collaboration avec des organismes, des institutions ou d'autres parties prenantes confrontées à des problèmes semblables ou qui en sont «responsables». Il peut s'agir simplement de transmettre un dossier ou de travailler en partenariat.
- Prévention ciblée des délits – Avec une prévention ciblée des délits, la commission de certains délits devient plus grave et demande plus d'efforts par la réduction des bénéfices pour le délinquant; cela résulte de la gestion, de la conception et de la manipulation de différents facteurs dans l'environnement physique. Pour cela, il faudrait mettre en place des mesures visant à réduire la possibilité de commettre des délits, dans l'espoir que cela décourage les délinquants ou, tout du moins, que cela les fasse changer de cible.
- Durcissement de l'accès à la cible – Par «durcissement de l'accès à la cible», on désigne tout obstacle physique rendant plus difficile pour un délinquant potentiel de commettre un délit. De tels obstacles devraient contribuer à cerner les comportements délictueux et mener à l'arrestation du délinquant. Exemples de dispositifs de durcissement de l'accès à la cible: écrans de protection aux comptoirs des bureaux de poste, mise à l'abri des articles de valeur dans des coffres-forts, barres antieffraction, portes blindées et alarmes de sécurité.
- Contrôles d'accès – Les contrôles d'accès visent à limiter ou à prévenir l'accès à certaines installations (bâtiment ou terrain) ou à certains systèmes (p. ex. systèmes informatiques). La mise en place de contrôles d'accès peut prendre les formes suivantes: construction de clôtures, de murs, de portails et de portails motorisés; utilisation de systèmes d'interphone et de cartes d'accès; recours à des agents de sécurité, des réceptionnistes et des portiers; utilisation de mots de passe et de codes d'identification.

Une stratégie de prévention des délits ne sera fructueuse que si elle est pratique et s'inscrit dans un processus basé sur des projets visant à résoudre les problèmes du milieu.