

CONSEILS ET IDÉES POUR MIEUX PROTÉGER SON
ENTREPRISE

“MIEUX VAUT PRÉVENIR QUE GUÉRIR !”



Avec la collaboration de :



FEB
Fédération des
Entreprises de
Belgique

FEB ASBL

Rue Ravenstein 4
1000 Bruxelles
T + 32 2 515 08 11
F + 32 2 515 09 99
info@vbo-feb.be
www.feb.be

Editeur responsable

Olivier Joris
rue du Wolvenberg 17
1180 Bruxelles

Responsable des publications

Stefan Maes

Rédaction

La Police judiciaire fédérale
Christine Darville-Finet (Fédération des Entreprises de Belgique)
Gilbert Geudens (Commission Sécurité des entreprises de la FEB)

Conception et pre-press

Vanessa Solymosi, www.landmarks.be

Impression

Geers Offset

Dépôt légal : D/0140/2010/10

Deze brochure is ook verkrijgbaar in het Nederlands. Une version imprimée de cette brochure peut être commandée auprès de Paola Bulot, Service Mailing et Secrétariat: pb@vbo-feb.be fax 02-515 09 55

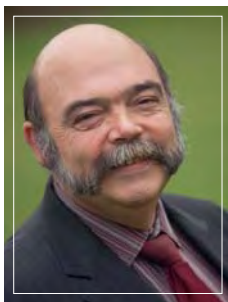
Le contenu de cette brochure est disponible sur le site www.feb.be
(publications > brochures gratuites)

CONSEILS ET IDÉES POUR MIEUX PROTÉGER SON ENTREPRISE

“MIEUX VAUT PRÉVENIR QUE GUÉRIR !”



Christine Darville-Finet,
Responsable du Département
juridique de la FEB



Gilbert Geudens
Président de la commission
Sécurité des entreprises de la FEB



Paul Van Thielen
Directeur général de la Police
judiciaire fédérale

La criminalité est un phénomène auquel n'échappent pas les entreprises belges. Il est d'une certaine façon compréhensible que toutes les entreprises ne prêtent pas un intérêt suffisant à ce problème, voire ne lui accordent pas même l'attention indispensable. En effet, l'adoption de mesures de protection ne contribue pas directement à la réalisation des objectifs commerciaux. Il convient cependant de ne pas perdre de vue que négliger les risques criminels peut entraîner de sérieux dommages pour l'entreprise.

C'est dans ce contexte que la Fédération des Entreprises de Belgique (FEB) – en collaboration avec la Police judiciaire fédérale – a rédigé une brochure afin de vous sensibiliser aux mesures de prévention. L'objectif n'est pas d'être exhaustif et d'analyser tous les phénomènes criminels en détail mais bien d'attirer votre attention sur certains modes opératoires des auteurs et la prise de mesures de prévention pour les contrer.

Toutes les parties d'une entreprise ne présentent pas le même degré de vulnérabilité, mais il va de soi que les lieux où l'on manipule de l'argent, où l'on stocke des marchandises de valeur et où l'on con-

serve des informations sensibles méritent une attention particulière !

Il vaut toujours mieux prévenir que guérir. Dans les statistiques policières, nous constatons que les mesures de protection prises par certains secteurs portent leurs fruits. Les cambriolages dans les commerces et entreprises sont en diminution pour la quatrième année consécutive. Le nombre de tentatives est en augmentation, ce qui démontre que le criminel a plus de difficultés à pénétrer dans les bâtiments.

Les vols avec violence et principalement les vols à main armée – qui ont des conséquences très traumatisantes pour les victimes – présentent une légère augmentation. Les vols à main armée montrent un déplacement des cibles classiques bien protégées (telles que les banques, les bureaux de poste, les transports de fonds) vers des secteurs plus vulnérables et moins protégés (petits commerces, stations essence, secteur horeca, librairies, nightshops, pharmacies, etc.).

Concernant les chiffres repris dans la brochure, il faut tenir compte d'un « chiffre noir » possible des incidents qui ne sont pas enregistrés au sein des services de police et dès lors non compris dans ces statisti-

ques. Nous souhaitons ici attirer votre attention sur le fait que toutes les déclarations sont importantes. Ce n'est que si la Police dispose de toutes les pièces du puzzle qu'elle peut cerner les groupes d'auteurs et intervenir à leur égard. C'est pourquoi nous voulons vous stimuler à porter plainte systématiquement. Pour certains délits, vous pouvez même le faire via Internet.

La création de la Plate-forme de concertation permanente sur la sécurité des entreprises (en exécution du Plan fédéral de sécurité et de politique pénitentiaire¹) a pour objectif de rapprocher le secteur privé et les pouvoirs publics. Outre le groupe de direction fédéral (qui exerce plutôt une fonction de coordination), quatre groupes de travail ont été mis sur pied pour élaborer des initiatives portant sur certaines thématiques spécifiques (criminalité informatique, protection du potentiel scientifique et économique, terrorisme, image criminelle et criminalité organisée). L'importance de cette collaboration entre le public et le privé comme l'un des nombreux outils de la politique intégrée

de protection a également été soulignée dans la note-cadre de politique de sécurité intégrée et intégrale des 30-31 mars 2004².

Il y a lieu de voir aussi les autres réalisations comme la brochure « Terrorisme et extrémisme – Les mesures de protection que les entreprises peuvent prendre »³ et la création du « early warning system »⁴.

La présente brochure d'information est l'un des résultats concrets des activités organisées au sein de ces groupes de travail.

Elle ne nourrit aucunement le dessein de s'ériger en ouvrage de synthèse sur le thème de la protection des entreprises. Parallèlement à une sensibilisation générale aux problèmes spécifiques de protection, la brochure contient une série de conseils et d'idées pratiques (principalement de nature organisationnelle) susceptibles de contribuer à une protection accrue de votre entreprise. Les petits détails font parfois toute la différence ! ●

¹ Ministère de la Justice, 31 mai 2000 – projet 25: <http://www.lachambre.be/FLBW/pdf/50/0716/50K0716003.pdf>.

² <http://www.info-zone.be/wet/plp35/kanoplp35.pdf>.

³ www.feb.be > Publications > Brochures gratuites

⁴ Voyez le chapitre 'Early warning system' p. 42.

Introduction	2
I. Phénomènes et risques criminels	6
Alerte à la bombe et/ou envoi suspect	6
Cadre	6
Mesures préventives générales	7
Comment réagir en cas d'incident ?	7
Vol sans effraction	9
Cadre	9
Mesures préventives	10
Comment réagir en cas d'incident ?	11
Vol au bélier	12
Cadre	12
Mesures préventives	13
Comment réagir en cas d'incident ?	14
Cambriolage	14
Cadre	14
Mesures préventives	16
Comment réagir en cas d'incident ?	17
Extorsion	17
Cadre	17
Mesures préventives	18
Comment réagir en cas d'incident ?	18
Fraude	19
Cadre	19
Mesures préventives	20
Comment réagir en cas d'incident ?	20
Abus d'informations	21
Cadre	21
Mesures préventives	21
Comment réagir en cas d'incident ?	23
Rip deal	23
Cadre	23
Mesures préventives	25
Comment réagir en cas d'incident ?	26
Prise d'otage	26
Cadre	26
Mesures préventives	27
Comment réagir en cas d'incident ?	28

Vol à main armée	29
Cadre	29
Mesures préventives	30
Comment réagir en cas d'incident ?	34
Car-jacking	36
Cadre	36
Mesures préventives	36
Comment réagir en cas d'incident ?	37
Vol dans véhicules	37
Cadre	37
Mesures préventives	38
Comment réagir en cas d'incident ?	39
Vandalisme	40
Cadre	40
Mesures préventives	40
Comment réagir en cas d'incident ?	41
2. Early warning system : un partenariat public - privé contre le terrorisme	42
Un mot d'explication sur le « early warning system »	42
Pour qui et par qui ?	43
Quelles informations ne sont pas échangées ?	43
Comment ?	43
Coopération public-privé	44
Fonctionnement du carré de l'information	44
Exemples d'application du carré de l'information et/ou du point de contact	45
3. Conseils en technoprévention	48
Qu'est-ce que la technoprévention ?	48
Qu'est-ce qu'un conseiller en technoprévention ?	49
Quel est le rôle du conseiller en technoprévention ?	49
Comment entrer en contact avec le conseiller en technoprévention le plus proche ?	50
Caméras de surveillance	50
Autres mesures de sécurisation	51
4. Liens et sites web utiles	52
Police on web	52
eCops	53
Checkdoc	53
DOC STOP	54
5. Annexe	56



1 Phénomènes et risques criminels

ALERTE À LA BOMBE ET/OU ENVOI SUSPECT

Cadre

Alerte à la bombe

Il ressort d'informations policières que cette problématique (ainsi que divers phénomènes connexes tels que les lettres contenant de la poudre suspecte et/ou les colis piégés) est très fréquente. C'est pourquoi, il est important que vous puissiez veiller, en adoptant quelques mesures simples, à ce qu'un maximum d'informations soient mises à la disposition de l'entreprise et des autorités, afin de permet-

tre une évaluation éventuelle des risques et que les mesures nécessaires puissent générer un effet maximal.

Envoi suspect

A quoi peut-on reconnaître un envoi suspect ? Malheureusement, cette question ne relève pas d'une science exacte : un courrier ou un colis devra être considéré comme suspect en fonction d'un certain nombre d'éléments, par exemple :

- Une forme bizarre et/ou un poids inhabituel ;
- La manipulation du colis procure une autre sensation que lorsqu'il s'agit de papier ;

- Une quantité inhabituelle de papier collant a été utilisée ;
- Le pays/la localité d'origine de l'expéditeur du colis ne correspond pas au cachet postal ;
- L'envoi est adressé à une personne qui a quitté l'entreprise ; la fonction est incorrecte ; le colis est adressé uniquement au titulaire d'une fonction ou à une personne totalement inconnue ;
- Une odeur suspecte ;
- La présence d'une ou de plusieurs taches suspectes ou de décolorations ;
- La présence de poudre ;
- L'envoi ne mentionne pas d'expéditeur ;
- La lettre est inattendue et/ou émane d'un expéditeur inhabituel ou totalement inconnu ;
- L'adresse de l'expéditeur est illisible ou incontrôlable ;
- L'enveloppe porte la mention « Personnel » ou « Confidentiel » ;
- L'adresse est écrite à la main ou mal dactylographiée ; elle comporte d'importantes fautes d'orthographe.

Mesures préventives générales

En cas d'alerte à la bombe, de lettre contenant de la poudre, de lettre ou de colis piégé(e) et de véhicules suspects, les mesures préventives générales suivantes peuvent être prises :

- Organisez à l'attention de votre personnel un briefing général traitant de ce phénomène ;
- Désignez des membres du personnel qui pourront, le cas échéant, assister les services de police dans l'hypothèse d'un sweeping (contrôle approfondi des bâtiments) ;
- Prévoyez un plan au sol par étage, un responsable par département ou par étage pour une évacuation éventuelle, ainsi qu'une voie d'évacuation distincte (top-down) ;
- Mettez un aide-mémoire (document standardisé) à la disposition du personnel et définissez un canal de communication explicite (à qui l'information doit-elle être transmise ASAP (As Soon As Possible) au sein de la société).

Comment réagir en cas d'incident ?

Alerte à la bombe

- Parcourez le document standard précité ;
- Informez immédiatement le responsable de la sécurité ;
- En concertation avec la police locale, décidez (au niveau de la direction) s'il y a lieu ou non d'évacuer le bâtiment ;

Mettez un aide-mémoire à la disposition du personnel et définissez un canal de communication explicite.

- En cas d'alerte à la bombe par téléphone : voyez la checklist en annexe.

Lettre contenant de la poudre

Dans ce cadre, il est bien entendu préférable que le courrier soit systématiquement traité dans un local fermé par un membre du personnel bénéficiant d'une expérience. ►►

- ▶▶ • Ne secouez pas la lettre et évitez toute autre manipulation ; n'ouvrez pas l'envoi et évitez tout contact inutile avec ce dernier ;
- Isolez le colis, au minimum dans un sachet en plastique (idéalement dans deux sachets en plastique fermés hermétiquement), afin d'éviter la « dispersion » de son contenu ; à défaut de sachet en plastique ou de tout autre contenant, veillez à ce que personne d'autre ne puisse manipuler le colis ;
- Évacuez le local et fermez-le pour éviter que d'autres personnes y pénètrent ;
- Évitez de ventiler le local et arrêtez l'air conditionné ;
- Si de la poudre a été répandue, ne la nettoyez pas, mais couvrez-la d'un vêtement, de papier, etc., afin d'éviter qu'elle se répande davantage ;

En cas d'envoi suspect, n'ouvrez pas l'envoi et évitez tout contact inutile avec ce dernier.

- Les personnes qui ont touché le produit doivent laver minutieusement à l'eau et au savon les parties du corps qui ont été en contact direct avec le produit ;
- Avertissez votre responsable de la sécurité, qui établira une liste de toutes les personnes susceptibles d'être entrées en contact avec l'envoi – liste à remettre aux autorités – et qui avertira la police locale.



Lettre piégée ou colis piégé

- Ne touchez pas le colis, ne le déplacez pas et essayez de mémoriser un maximum de détails ;
- Quittez calmement le local (évités les vibrations et emmenez les collègues éventuellement présents) ;
- Fermez le local (veillez à ce que d'autres collègues ne puissent plus y pénétrer) ;
- N'utilisez plus vos GSM et vos radios portables ;
- Un périmètre de sécurité doit être installé aux alentours du local, afin d'organiser une « surveillance » à distance ;
- Avertissez immédiatement le responsable de la sécurité, qui préviendra la police locale ;

Véhicule suspect

Il convient d'adopter les mêmes réflexes que ceux à mettre en œuvre pour une lettre ou un colis piégé(e). Il est toutefois recommandé de respecter un périmètre de 200 mètres.

Bien entendu, la police locale sera votre interlocuteur privilégié en cas d'incident de



ce genre. Si nécessaire, celle-ci avertira à son tour la Police fédérale et/ou d'autres instances par les canaux appropriés.

Il n'est pas superflu d'établir un contact préalable entre le responsable de la sécurité ou l'entrepreneur et un représentant de la police locale, afin de pouvoir collaborer le plus rapidement possible en cas d'incident, dans l'intérêt des deux parties.

VOL SANS EFFRACTION

Cadre

Beaucoup d'entreprises sont confrontées au phénomène des vols. Il n'est dès lors pas surprenant que les sociétés prennent des mesures de protection et de prévention contre le vol.

Lors d'un vol, il est généralement question de détournement d'argent ou de marchandises conservé(es) dans un bâtiment. Néanmoins, il arrive également que des

biens soient dérobés dans un véhicule de votre société. De surcroît, vous devez tenir compte de la potentialité du vol de ce véhicule lui-même.

Dans de nombreux cas, le vol est perpétré par des auteurs extérieurs. Parallèlement, il apparaît également qu'un certain pourcentage d'entreprises sont victimes de vols commis par les membres de leur propre personnel.

Le risque de vol résulte bien entendu de la nature des articles que vous possédez et de la présence (éventuelle) d'argent liquide. Les facteurs suivants qui favorisent le vol :

- La présence d'auteurs potentiels (lieux de rassemblement traditionnels où traînent des jeunes ou des drogués,...) ;
- L'absence « d'observateurs sociaux » (passants ou résidents du quartier qui gardent un œil sur les lieux de façon informelle et souvent inconsciente, ou de gardiens et d'agents de police assurant une surveillance formelle) ;
- Un environnement défavorable (présence d'obstacles qui limitent la visibilité) ;



- ▶▶ • Accès trop facile(s) aux bâtiments de l'entreprise et présence éventuelle d'itinéraires de fuite (plus il y a d'entrées et de sorties, plus un bâtiment est attractif pour les voleurs).

Mesures préventives

De nombreuses mesures existent vous permettant de réduire le risque de vol ou de minimiser les conséquences d'un vol éventuel. Ces mesures peuvent varier considérablement d'une entreprise à l'autre. Le principe repose sur trois aspects : les mesures organisationnelles, les mesures mécaniques et les mesures électroniques. Vous trouverez plus de détails à ce sujet le chapitre « Conseils en technoprévention », p. 48.

- Limitez l'ampleur du butin potentiel en déposant votre argent à la banque suivant des horaires irréguliers, en ne stockant pas vos matières premières longtemps avant que vous en ayez besoin et en livrant aussi vite que possible vos produits aux clients ;

De nombreuses mesures existent pour réduire le risque de vol.

- Réduisez autant que possible la circulation d'argent liquide en privilégiant les paiements électroniques ;
- Limitez l'accès aux endroits « sensibles » ;
- Contrôlez l'accès à vos espaces professionnels. Fermez-les si le public n'a pas le droit d'y pénétrer ;
- Rangez les marchandises intéressantes ou de valeur hors de portée des voleurs potentiels ;

- Marquez et faites enregistrer vos appareils et votre stock ; photographiez les objets de valeur⁵ ;
- Déterminez en concertation avec les membres de votre personnel dans quelle mesure ils peuvent utiliser les articles et appareils de bureau pour leur usage privé ;
- Ne laissez pas les véhicules de votre entreprise sans surveillance sur la voie publique ;
- Veillez à ce que vos chauffeurs de camion déchargent leurs marchandises immédiatement après leur arrivée chez le client. Ils ne doivent pas commencer par se restaurer ou passer la nuit à l'hôtel. Tenez-en compte lors du calcul de leur programme de livraison ;
- Mettez en place un système efficace de gestion des clés :
 - Faites preuve de discipline quant à l'identité des personnes habilitées à déterminer les clés de chaque local.
 - Utilisez des clés qu'on ne peut reproduire.
 - N'abandonnez jamais une clé sur une vitrine, un coffre ou une porte.
 - Remplacez la serrure lorsqu'une clé a été perdue ou dérobée.
 - Changez régulièrement les combinaisons chiffrées du coffre. Faites-le en tout cas lorsque vous venez de licencier un collaborateur.
- Connaissez vos clients. Observez les gens et nouez directement le contact lorsqu'une personne arrive. Apprenez à votre personnel à agir également de la sorte ;
- Soyez attentif aux signaux tels que : déambulation dans les locaux, comportement de non-achat, questions hors de propos, véhicules suspects, personnes prêtant une attention particulière à la sécurité, change monétaire suspect ;

- Faites appel à une entreprise de gardiennage agréée ou à un service interne de gardiennage (Loi du 10 avril 1990 réglementant la sécurité privée et particulière⁶) ;
- Envisagez d'équiper vos véhicules utilitaires d'un dispositif de localisation (systèmes après-vol ou « after theft ») grâce auquel la police pourra suivre la trace des véhicules volés ;
- Spécifiquement pour le vol à l'étalage, vous trouverez plus d'information auprès de l'ASBL Prévention et Sécurité (Rue Marianne 34, 1180 Bruxelles, 02/345.99.23) ;
- Organisez régulièrement des **contrôles de sortie** de vos collaborateurs. La **CCT 89** règle les modalités des contrôles de sortie des travailleurs et précise ce qu'il y a lieu d'entendre par contrôles de sortie : les contrôles de travailleurs qui ont lieu lorsque ceux-ci quittent l'entreprise ou le lieu de travail et qui visent uniquement à prévenir ou à constater le vol de biens dans l'entreprise ou sur le lieu de travail. Pour des informations détaillées, vous pouvez consulter la brochure de la FEB « Sécurisez votre entreprise : contrôles de sortie »⁷.



contenant de bons conseils⁸ : moyens pour protéger vos locaux professionnels, sécurité des indépendants, prévenir le vol sur chantier, évitez le vol de véhicules, etc.

Beaucoup d'entreprises investissent principalement dans des mesures de protection techniques. C'est la raison pour laquelle nous précisons dans le chapitre 3 (p. 50) quelques informations relatives à **l'installation de caméras** dans le cadre de la prévention contre le vol.

D'autres mesures organisationnelles sont également importantes et ne doivent pas être perdues de vue.

Comment réagir en cas d'incident ?

Bien entendu, la police locale sera votre interlocuteur privilégié en cas d'incident de ce genre. Si nécessaire, celle-ci avertira à son tour la Police fédérale et/ou d'autres instances par les canaux appropriés. Le vol à l'étalage peut être dénoncé par le guichet virtuel de la police locale via www.police-on-web.be. Vous trouverez plus d'informations à ce sujet au chapitre 4 de cette brochure. ►►

Le service prévention du SPF Intérieur a réalisé différentes brochures de prévention

⁵ Formulaire d'enregistrement dans la brochure « Save your numbers » disponible sur www.besafe.be.

⁶ Plus d'informations disponibles sur www.vigliis.be.

⁷ www.vbo-feb.be.

⁸ Ces brochures sont consultables et peuvent être commandées sur www.besafe.be, rubrique publications.

► VOL AU BÉLIER

Cadre

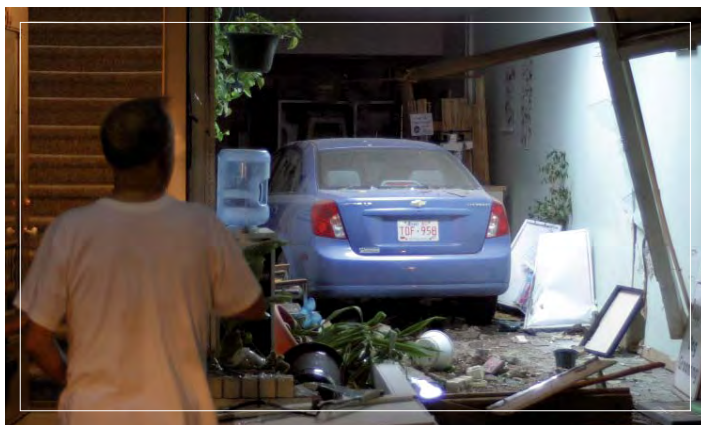
Le vol au bélier est défini par le Collège des Procureurs généraux comme étant: « le fait de commettre un vol ou la tentative de vol au moyen d'effraction sur un étalage, porte ou portail d'accès d'une entreprise indépendante ou d'un commerce indépendant en se servant d'un véhicule, d'un objet (poussé ou non par un véhicule), ou d'une quelconque arme de choc dans le but d'enlever **rapidement** le butin présent ».

En d'autres termes, les faits de vol avec escalade ou fausses clés ne relèvent, dès lors, pas de la définition des vols au bélier.

Dans le cadre des vols au bélier, l'effraction est avant tout commise sur les vitrines d'entreprises où des biens sont vendus,

mais aussi sur une porte ou un portail d'accès. Dans certains cas, les voleurs pénètrent par une porte de chargement sectionnelle, qui est plus facile à enfoncer et/ou qui réduit le risque de blessures.

En raison de l'importante force nécessaire à l'enfoncement, un véhicule constitue l'outil traditionnellement utilisé pour commettre un vol au bélier. Dans certains cas, les auteurs utilisent un objet (utilisation d'un râtelier à vélos, d'une poutre en bois, d'une poubelle comme bélier..) pour contourner les mesures technopréventives. Les auteurs adaptent le modus operandi à la situation. Il s'avère, en effet, que des marteaux (sur lesquels des têtes de forets ont été soudées ou non), des blocs de béton et des plaques d'égout sont des béliers efficaces. De tels objets peuvent en outre souvent être trouvés à proximité de l'entreprise et permettent d'éviter que la voiture avec laquelle les auteurs prennent la fuite porte des traces de l'effraction.



Un grand nombre de ces entreprises appliquent des mesures de protection technopréventive, telles qu'un système d'alarme avec transmission à la centrale d'une entreprise de gardiennage. Les auteurs espèrent toutefois réussir leur coup avant que la police n'arrive sur les lieux.

En raison de la sécurisation des entreprises, le modus operandi est souvent une combinaison de plusieurs méthodes de cambriolage. Les cambrioleurs coupent, par exemple, des fils et des cadenas à l'aide d'une pince coupante afin d'arracher ou de relever le volet éventuel et d'enfoncer la vitrine ou la porte d'entrée avec un véhicule en marche arrière. Les systèmes d'alarme sont souvent sabotés en tournant les caméras vers le haut ou en les recouvrant, ou en débranchant la sirène d'alarme grâce à des matériaux d'isolation. Les biens volés sont souvent jetés sur une bâche à l'intérieur du magasin, puis placés dans le coffre de l'auto. Le véhicule de fuite est souvent volé dans les environs immédiats. L'intrusion dans le magasin, le vol du butin et la fuite sont exécutés très rapidement, souvent en quelques minutes.

La plupart du temps, les auteurs effectuent une reconnaissance plusieurs jours avant de commettre le vol au bélier.

Ces dernières années, le nombre de vols au bélier a clairement suivi une tendance à la baisse. Grâce aux mesures de sécurité qui ont été prises (placement de piliers en béton, bacs à fleurs devant la vitrine...), ce modus operandi est de moins en moins attrayant pour les voleurs.

Mesures préventives

- Limitez autant que possible la quantité et/ou la valeur des biens exposés dans le magasin ; si possible, utilisez des objets factices ;

Grâce aux mesures de sécurité qui ont été prises, le vol au bélier est de moins en moins attrayant pour les voleurs.

- Si le magasin est équipé d'une ou de plusieurs caméras de surveillance :
 - Dissimulez au moins une caméra, mais veillez également à ce qu'une caméra soit clairement visible ;
 - Faites en sorte que l'appareillage soit de bonne qualité ;
 - Vérifiez que les images enregistrées sont claires et utilisables (évitiez le contre-jour) ;
 - Lisez également au chapitre 3 (p. 50) de la présente brochure les modalités relatives à la surveillance par caméras ;
- Faites attention aux personnes et aux véhicules suspects. Très souvent, les auteurs effectuent une reconnaissance quelques heures ou quelques jours avant le vol. Ils examinent l'endroit où sont placées les caméras, mais aussi l'importance du butin éventuel et la solidité des portes d'entrée. Notez les numéros d'immatriculation des véhicules suspects et transmettez-les immédiatement, ainsi qu'une description détaillée de la per- ►►

- ▶ sonne, à la police locale en vue d'une interception et d'un contrôle éventuels ;
- L'existence d'un contrôle social (passants ou habitants du quartier qui gardent un œil sur les lieux de manière informelle et souvent inconsciente) ;



- Veillez à ce qu'il n'y ait pas dans les environs du magasin des objets pouvant être facilement utilisés par les auteurs pour commettre un vol au bélier (conteneurs de déchets, râteliers à vélos...) ;
- Si possible, veillez à ce que les auteurs ne puissent pas passer trop facilement dans le magasin (par exemple, en plaçant des obstacles). La rapidité d'exécution constitue, en effet, leur atout majeur ;
- Laissez peu d'argent dans la caisse et laissez-la ouverte si possible. Vous évitez ainsi que les cambrioleurs l'emportent ou l'endommagent.

Comment réagir en cas d'incident ?

Bien entendu, la Police locale sera votre interlocuteur privilégié en cas d'incident. Elle informera à son tour la Police fédérale et/ou d'autres instances par les canaux appropriés.

Dans l'attente des constatations et du prélèvement éventuel de traces par le laboratoire judiciaire, vous devez laisser autant que possible le « lieu du délit » dans l'état dans lequel il se trouve (ne pas ranger, toucher le moins possible, protéger les traces si nécessaires).

CAMBRIOLAGE

Cadre

Chaque année, un grand nombre d'entreprises sont victimes de cambriolages. Généralement, le butin empoché est considérable. À cela s'ajoutent les dommages causés par l'effraction. Il n'est dès lors pas étonnant que la plupart des entreprises prennent des mesures de sécurité pour réduire le risque de cambriolage.

Certains secteurs sont plus touchés que d'autres : le degré de risque des établissements de l'horeca et des grands magasins est plus élevé que celui d'autres entreprises. La plupart des biens volés dans les magasins et les entreprises sont les suivants : argent, tabac, coffre-fort ou contenu du coffre-fort, ordinateurs, produits alimentaires et alcool, moyens de communication, vêtements...

Une effraction ne débouche pas toujours sur un vol. Il se peut que le cambrioleur pénètre dans votre entreprise pour y dormir au chaud, pour y commettre des dégradations, pour y mettre le feu ou pour commettre une attaque (ultérieure).

Quelles que soient les mesures de prévention que vous prenez, un cambrioleur peut toujours tenter de les contourner, à condition qu'il en ait le temps. C'est pourquoi une bonne protection contre le cambriolage repose sur deux principes : vous devez détecter le plus vite possible le cambrioleur et vous devez faire en sorte qu'il ait besoin de beaucoup de temps pour parvenir à ses fins.

Si vous appliquez correctement ces deux principes, vous pouvez donner l'alarme à un stade précoce du cambriolage, ce qui vous permet de gagner du temps pour

mener les actions nécessaires et faire arrêter le cambrioleur.

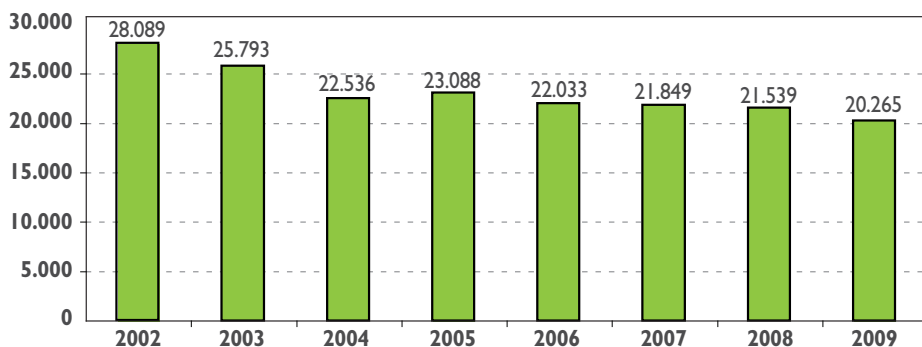
Détecter le plus vite possible le cambrioleur et faire en sorte qu'il ait besoin de beaucoup de temps pour parvenir à ses fins.

Les chiffres concernant les cambriolages dans les commerces et les entreprises suivent une courbe descendante depuis plusieurs années.

• **Quand sont commis les cambriolages dans les entreprises et les commerces ?**

La plupart des cambriolages sont commis en hiver. Le mercredi et le vendredi sont les jours « les plus prisés ». Les auteurs agissent généralement durant la nuit, entre minuit et six heures du matin. ►►

Cambriolages dans les entreprises et commerces (Source : Banque de données nationale générale)



► • **Que cherchent les auteurs ?**

L'argent étant le bien le plus convoité, il occupe la première place du classement des biens volés. Les produits alimentaires, les coffres-forts, les moyens de communication et les multimédias complètent le top 5 et représentent 80% des biens volés dans les entreprises et les commerces.

Toutes les parties d'une entreprise ne présentent pas un niveau égal de vulnérabilité. Il va de soi que les endroits où l'on travaille avec de l'argent, où l'on stocke des objets de valeur ou dans lesquels on conserve des informations sensibles doivent faire l'objet d'une attention particulière !

Les endroits où l'on travaille avec de l'argent ou dans lesquels on conserve des informations sensibles doivent faire l'objet d'une attention particulière !

Mesures préventives

La prévention des cambriolages repose sur les éléments suivants :

- Augmenter le risque de se faire prendre ;
- Compliciter l'accès aux bâtiments ;
- Limiter le butin, les possibilités de revente de ce dernier et les dommages pouvant être causés ;
- Faire une déclaration minutieuse en cas de vol.

Parmi les mesures visant à lutter contre les cambriolages, il faut avant tout songer aux **mesures organisationnelles** telles que:

- Soyez toujours conscient du risque de cambriolage et veillez à ce que vos collaborateurs le soient également ;
- Veillez à ce que les fenêtres et les portes soient correctement fermées. Fermez également les portes intermédiaires. Ne laissez pas les clés des portes (intermédiaires) à portée de main. Veillez à ce qu'il n'y ait pas plus de clés en circulation que ce qui est strictement nécessaire ;
- Marquez et enregistrez vos biens et appareils ; photographiez les objets de valeur⁹ ;
- Copiez quotidiennement vos données informatiques et conservez-les dans un coffre-fort à un autre endroit. Si vos ordinateurs sont volés ou détruits, vous ne perdrez ainsi pas plus d'une journée de travail. N'emportez pas la copie de vos données à votre domicile ;
- Organisez une ronde de contrôle avant la fermeture de l'entreprise afin que personne n'y soit enfermé ;
- Veillez à ce que l'alarme fasse l'objet d'un suivi approprié. Une protection efficace contre les cambriolages n'est en effet utile que si vous menez l'action appropriée lorsqu'un cambrioleur est signalé.

Lorsque la sécurisation a correctement été assurée, des mesures techniques (architectoniques et électroniques) peuvent donner des résultats :

- Faites en sorte de pouvoir faire la distinction entre un intrus et un passant dès l'entrée du domaine de votre entreprise (contrôle d'accès) ;
- Veillez à ce que votre domaine soit éclairé et installez des systèmes de détection électronique ;



- Faites attention à la protection de la façade et du toit : fenêtres, portes, tabatières et dômes vitrés anti-effraction, bonnes charnières et serrures, alarme électronique, volets ;
- Placez des bacs à plantations et/ou des poteaux à des endroits stratégiques de sorte que l'entrée du magasin ne puisse pas être détruite à l'aide d'une voiture ;
- Assurez la sécurité interne en fermant les portes et en prévoyant éventuellement une alarme électronique.
- Compartimentage : placez les objets les plus chers dans l'espace pouvant être le mieux fermé. Placez l'argent, les papiers de valeur et les documents confidentiels dans un coffre-fort ;
- Vigilance sociale.

L'intervention d'une entreprise de gardiennage constitue une autre méthode de sécurisation. Vous pouvez ainsi convenir avec les autres entrepreneurs se trouvant sur le terrain industriel de recourir à une entreprise de gardiennage pour assurer une surveillance permanente⁹.

Comment réagir en cas d'incident ?

Bien entendu, la police locale sera votre interlocuteur privilégié en cas d'incident. Elle informera à son tour la Police fédérale et/ou d'autres instances par les canaux appropriés. Il est dès lors recommandé de toujours faire une déclaration à la Police locale en cas de cambriolage.

Dans l'attente des constatations et du prélèvement éventuel de traces par le laboratoire judiciaire, vous devez laisser autant que possible le « lieu du délit » dans l'état dans lequel il se trouve (ne pas ranger, toucher le moins possible, protéger les traces si nécessaires).

EXTORSION

Cadre

Par extorsion, on entend le fait de contraindre, par la menace, une personne à céder quelque chose.

Il doit y avoir un lien de causalité entre le recours à la violence ou la menace et la ►►

⁹ Formulaire d'enregistrement disponible dans le dépliant « Save your numbers » sur le site <http://www.besafe.be/>.

¹⁰ Pour de plus amples informations, voir les sites web <http://www.vigliis.be> et <http://www.apeg-bvbo.be>.

- remise du bien extorqué. L'extorsion peut se manifester sous plusieurs formes :
 - Racket ;
 - Extorsion commerciale ;
 - Chantage.

Le racket est une forme particulière d'extorsion dans le cadre de laquelle les auteurs d'une bande contraignent par la menace un ou plusieurs indépendants à leur payer régulièrement de l'argent. En échange, le commerçant bénéficie d'une « protection » ou peut poursuivre ses activités commerciales sans « désagréments ».

L'extorsion commerciale se distingue des autres formes d'extorsion par le fait qu'une entreprise est extorquée sous la menace de la contamination ou du sabotage de ses produits.

Le chantage peut être décrit comme le fait de se faire remettre une signature, de l'argent ou des valeurs sous la menace de divulgations compromettantes pouvant porter préjudice à la réputation d'une personne ou d'une entreprise.

Les extorqueurs peuvent rencontrer la victime personnellement ou la contacter par téléphone, par courrier ou par d'autres biais. Il arrive que les extorqueurs prennent contact avec une tierce partie, telle que la presse, la police, un service public, un cen-

tre de distribution... pour faire part de leurs exigences.

Pour le monde des entreprises, cette forme de criminalité, ainsi que la criminalité informatique, est perçue comme une réelle menace.

Mesures préventives

Il n'y a guère de mesures préventives contre l'extorsion. Une entreprise peut toutefois se préparer à la réaction qu'il convient d'adopter si elle est victime d'extorsion. Cela permet d'agir de manière flexible et en connaissance de cause. Il est recommandé de disposer d'un plan de gestion de crise dans lequel figurent, entre autres, l'analyse des incidents possibles, le flux d'information interne, les procédures d'avertissement, de décision et les premières réactions.

Comment réagir en cas d'incident ?

Pour la gestion de la crise, la protection de l'intégrité physique de la personne menacée est la première priorité de toutes les personnes concernées.

Pour éviter d'endommager ou d'effacer des traces, il est recommandé de manipuler le



moins possible la lettre de menace lorsqu'on la reçoit, d'en faire une photographie numérique et de la placer immédiatement dans une enveloppe en papier. On peut ensuite utiliser une copie de la lettre (photo numérique).

En cas d'extorsion par téléphone : voir la liste de vérification (et les questions qu'elle comporte) en annexe de la présente brochure.

En cas d'extorsion, une plainte doit être introduite auprès de la police judiciaire fédérale de l'arrondissement¹¹, qui mènera une enquête en toute discrétion afin de ne pas porter préjudice aux intérêts commerciaux de l'entreprise.

FRAUDE

Cadre

Le mot « fraude » est un terme générique. Il ne fait l'objet d'aucune définition unifiée, ni d'aucune subdivision claire. On peut distinguer trois types de fraude :

- Fraude interne : le fraudeur est un employé de l'entreprise ;
- Fraude externe : le fraudeur est extérieur à l'entreprise ;
- Fraude d'entreprise : l'entreprise est elle-même fraudeuse.

Il est presque impossible de dresser l'image exacte de la fraude car le « chiffre noir »

est élevé. Par voie de conséquence, nous savons que les entreprises sous-estiment ce problème.

Toutefois, des signes indiquent régulièrement qu'un acte de fraude a été commis au sein d'une entreprise : une déclaration anormale, un schéma de congés anormal (le fait de ne pas prendre de congés ou de n'en prendre guère), un schéma de travail anormal (arriver le premier sur le lieu de travail et le quitter en dernier), l'absence de plusieurs offres lors d'achats importants, de nombreuses factures manuscrites, de nombreuses corrections sur des tickets de caisse, le recours fréquent à des notes de crédit, la vente régulière de biens endommagés, le fait de retirer ou de livrer des marchandises à des moments inhabituels, le fait qu'un candidat présente un C.V. trop attrayant ou ne dispose que de copies de ses diplômes.

Les dommages causés par la fraude aux entreprises sont considérables. La plupart d'entre eux résultent de la fraude à la déclaration des frais, du détournement de moyens financiers et du vol de biens. Les facteurs suivants sont à l'origine de la fraude ou la favorisent :

- Confiance excessive de la part de l'employeur ;
- Faible contrôle interne ;
- Contournement du contrôle interne ;
- Absence de règles d'éthique ;
- Absence de procédures ou application incorrecte des procédures ;
- Influence exercée par d'autres collègues ; ►►

¹¹ Les adresses peuvent être consultées sur le site web suivant : <http://www.info-zone.be>.

- ▶ • Enquête insuffisante sur les antécédents de l'employé lors de son entrée en service ;
- Lacunes dans le système d'automatisation.

Souvent l'affaire est résolue en interne, dans de nombreux cas avec l'aide de détectives privés.

Mesures préventives

La prévention de la fraude comporte trois étapes.

La **première étape** de la prévention de la fraude est la « **conscience du management** ». Cette forme de criminalité pose problème à un grand nombre de dirigeants d'entreprise, car il s'agit souvent de leurs propres membres du personnel. Des mesures anti-fraude peuvent avoir un effet négatif sur l'ambiance de travail et créer un climat de méfiance sur le lieu de travail.

En évoquant le risque de fraude avec le personnel, on indique clairement les normes spécifiques à l'entreprise, qu'il convient de respecter.

Les meilleures entreprises sont toutefois en proie à la fraude. C'est pourquoi la **deuxième étape** de la prévention de la fraude consiste à **permettre** que l'on **débatten** de ce problème au sein de l'entreprise. En évoquant le risque de fraude avec le personnel, on indique clairement les normes spécifiques à l'entreprise, qu'il convient de respecter (ligne de conduite par rapport

aux déclarations, aux cadeaux d'affaires, à l'outillage et l'équipement de l'entreprise, aux air-miles...). Il faut jouer carte sur table concernant la réalisation de contrôles périodiques et les raisons de ces contrôles.

En ce qui concerne la **troisième étape**, la pratique nous révèle que près de la moitié des cas de fraude ont pu être évités grâce à un **contrôle interne** efficace. Il n'y a toutefois pas de règle générale pour les actions préventives visant à lutter contre la fraude, car chaque cas de fraude est différent (voir ci-dessus la définition). Généralement, la fraude ne revêt en effet ni un caractère répétitif ni un caractère récurrent. Vous trouverez, ci-après, quelques conseils :

- Confiez l'exécution des tâches et le contrôle de celles-ci à différents membres du personnel ;
- Contrôlez les achats, la gestion du stock et les ventes. Comparez les chiffres et vérifiez les différences ;
- Vérifiez que les clients et les fournisseurs sont fiables. Veillez à la sécurisation des fichiers informatiques. Tenez compte du fait que le gestionnaire de votre système dispose d'un accès illimité à tous vos fichiers ;
- Vérifiez les références d'un nouveau collaborateur ;
- Limitez les compétences des stagiaires et des travailleurs intérimaires et veillez à ce qu'ils soient bien encadrés.

Comment réagir en cas d'incident ?

Si un problème de fraude se pose au sein de l'entreprise, il convient de tenir compte

de la loi organisant la profession de détective privé. Seuls des détectives privés autorisés peuvent procéder à des recherches¹². En raison de sa finalité, de sa rapidité et de ses moyens, la lutte contre la fraude par le secteur privé peut différer de celle menée par le secteur public.

Ici aussi, la Police locale est le point de contact officiel pour tout signalement de fraude.

ABUS D'INFORMATIONS

Cadre

Les informations sont inhérentes aux entreprises : informations stratégiques, informations concernant les processus de production, administration de l'entreprise...

Les informations existent sous trois formes dans l'entreprise : sur un support papier; dans des fichiers informatiques ou mémorisées par les collaborateurs.

Les fichiers informatiques jouent un rôle de plus en plus central dans le stockage et le traitement des informations. Ce rôle prépondérant de l'informatique rend votre entreprise plus vulnérable, car les informations peuvent être volées, manipulées et bloquées par voie électronique, souvent sans que l'entrepreneur s'en rende lui-même compte. Le dommage est souvent irréparable.



Les informations sur support papier et mémorisées par les collaborateurs sont également vulnérables. Les documents papier peuvent être dérobés et falsifiés. Les collaborateurs peuvent, quant à eux, se montrer indiscrets ou être contraints de révéler certaines informations.

Mesures préventives

La sécurisation des informations repose sur trois principes : les informations confidentielles doivent le rester; les informations fia- ►►

¹² Loi du 19 juillet 1991 organisant la profession de détective privé, www.vigilis.be.

- ▶▶ les doivent rester fiables et les informations disponibles doivent le rester.

Vous pouvez prendre les mesures suivantes :

- Indiquez clairement la différence entre les informations confidentielles et non confidentielles. Veillez à ce que les membres de votre personnel aient connaissance du caractère confidentiel de certaines informations. Faites en sorte que les informations confidentielles ne soient connues que des personnes devant les utiliser dans le cadre de leur travail. Ne laissez aucun document confidentiel sur les bureaux, à proximité de la déchiqueteuse ou de la photocopieuse ;
- Protégez votre système contre l'intrusion par le biais d'Internet ou du réseau WIFI, entre autres en utilisant un pare-feu. Faites en sorte que les transmissions entrantes soient analysées par un antivirus. Lorsque vous lisez des disquettes, CD-ROMS ou clés USB n'appartenant pas à votre entreprise, vérifiez au préalable s'ils ne comportent pas de virus ;
- Protégez vos ordinateurs contre l'accès non autorisé. Réglez le contrôle d'accès à (des parties de) votre réseau informatique à l'aide de mots de passe efficaces ou de systèmes plus performants tels que Digipass ou la carte d'identité électronique. Déterminez clairement les personnes compétentes pour voir, ajouter et/ou modifier des données. Veillez à changer régulièrement les mots de passe ;
- Faites chaque jour un back-up de vos fichiers informatiques, tant des logiciels que des données des utilisateurs (banques de données) ;
- Sensibilisez les nouveaux collaborateurs, les travailleurs intérimaires et les stagiaires à une utilisation minutieuse des programmes et fichiers informatiques ;
- N'utilisez pas de logiciels obtenus illégalement ;
- Si nécessaire, cryptez vos données confidentielles sur des clés USB ;
- Concluez par écrit un accord de confidentialité avec les membres de votre personnel. Rappelez cet accord au membre



du personnel dont le contrat de travail se termine.

Comment réagir en cas d'incident ?

On constate une tendance à régler ces infractions en interne. Il est toutefois recommandé de **toujours** faire une déclaration à la Police locale en raison du caractère pénal de l'infraction.

Le cas échéant, veillez à ce que le système informatique reste autant que possible dans son état initial. N'y faites pas vous-même des recherches.

RIP DEAL

Cadre

Depuis quelques années, un phénomène délictuel identifié sous le vocable anglophone de « rip deal » – qui dérive des mots anglais (to rip : arracher – deal affaire) – est observé et suivi en Belgique. Il est apparu au début des années nonante, touchant d'abord les pays du sud de l'Europe et le Royaume-Uni. En Belgique, le « rip deal » n'existe pas comme tel dans le Code pénal mais les faits peuvent être qualifiés ou regroupés sous les qualifications suivantes : escroquerie, faux-monnaillage, vol simple, vol avec violence, association de malfaiteurs, organisation criminelle, blanchiment d'argent.

Si on analyse la manière de procéder des auteurs, il est évident qu'il s'agit d'une escroquerie relevant de la matière économique et financière.

Celle-ci pourrait se définir comme suit : Escroquerie au change ou vol à dimension internationale, commise sous le couvert d'une transaction mobilière ou immobilière, portant sur une somme d'argent ou une valeur, avec ou sans violence, et commise par un groupe criminel structuré.

Le « rip deal » est une escroquerie relevant de la matière économique et financière.

Les **caractéristiques** du « rip deal » sont les suivantes :

- Le mode opératoire consiste pour les auteurs à relever, dans la presse ou sur Internet, une annonce portant généralement sur la vente d'un bien immobilier. Cette annonce peut également concerner la vente de voitures, bijoux, bateaux, chevaux,... dans le but d'accrocher l'intérêt du vendeur potentiel par la crédibilité affichée.
- Les auteurs agissent par phases dont la finalité est de gagner la confiance des victimes en :
 - Se présentant comme faux experts, juristes et notaires, faux cheiks arabes, etc. ;
 - Proposant, par une offre juteuse et alléchante, d'opérer toute la transaction espèces, ou en sous-évaluant le bien, afin de permettre une opération de change en espèces, favorable au vendeur en ce qui concerne le pourcentage pratiqué lié au change, et au pré-



- ▶▶ texte, pour les auteurs, de leur garantir une fiscalité locale avantageuse sur l'acquisition opérée ;
- En orientant la discussion rapidement vers une question d'opération de change ou de transaction en espèces ;
- En réalisant une première transaction avec un bénéficiaire destiné à appâter la victime et à l'amener à une seconde transaction qui aboutira au « rip deal » proprement dit et, par la même occasion, au vol d'un montant important en espèces (plusieurs milliers d'euros) ;
- S'entourant d'artifices (rendez-vous dans des hôtels de luxe, tenue très élégante, véhicules haut de gamme), le but étant de faire croire à de fausses sociétés ;
- Utilisant des identités différentes à chaque phase de l'opération ;
- Fixant des rendez-vous aux victimes généralement dans un pays autre que celui des victimes ;
- Incitant les victimes à leur présenter d'autres victimes potentielles en leur faisant croire qu'elles pourraient récupérer leur préjudice.

- Echange de devises

La victime se retrouve en fait, en contrepartie des sommes engagées, avec des fac-similés de billets portant généralement, sous la bague en papier qui enserre la liasse, des inscriptions fac-similé comme Walt Disney – ristorante italiano ou d'un parc d'attractions. Il ne s'agit cependant pas de faux billets.

Les échanges s'effectuent en :

- Euros contre des fac-similés de billets de 1.000 francs suisses ;
- Euros contre des fac-similés de billets de 200 euros ;
- Euros contre de faux euros ;
- Dollars \$ et canadiens contre de faux euros ;
- Euros contre de faux contrats de prêts ou d'investissements.



- L'usage de la violence n'est pas systématique mais peut survenir dès lors que la transaction ou l'échange dure trop longtemps. Il s'agit, la plupart du temps, de l'arrachage de la valise contenant l'argent apporté par la victime.
- Les préjudiciés sont principalement des ressortissants des pays suivants : Italie / Suisse / Allemagne / Luxembourg / Belgique / Espagne / France / Royaume-Uni. Les victimes sont issues de toutes les couches sociales et sont choisies en fonction de leur situation financière. Le but est de limiter l'action tant policière que judiciaire.

Remarque : Il est utile de préciser qu'il ne s'agit pas d'inverser les culpabilités et d'accabler les victimes qui n'osent ou

n'ont pas déposé plainte par crainte d'un contrôle fiscal. Certaines ont d'ailleurs engagé et perdu, de bonne foi, des sommes parfaitement légales et déclarées. La tactique est en réalité une manoeuvre des auteurs qui réfutent leur responsabilité en la rejetant sur des victimes crédules et appâtées par un gain non déclaré.

fuser régulièrement cette information dans les médias (radio, télévision), presse spécialisée (Test Achats, banques, ...), Internet...

Il est également nécessaire de sensibiliser des professions réglementées (agences immobilières, études notariales,...) qui sont susceptibles d'être mises en contact avec les auteurs, en leur demandant :

Le montant du préjudice d'un « rip deal » peut parfois être estimé à plusieurs centaines de milliers d'euros.

- Le montant du préjudice peut être estimé à plusieurs centaines de milliers d'euros. Il ne s'agit que d'une estimation partielle si l'on se réfère aux différentes qualifications et aux faits qui ne sont pas dénoncés.

Mesures préventives

Permettre au public d'acquérir une meilleure connaissance du phénomène incitera toute victime potentielle à faire preuve de la plus grande méfiance.

La prévention en la matière peut s'effectuer en deux phases :

- **La conscientisation par l'information**
Le grand public ne peut être conscientisé aux risques encourus, surtout en matière d'escroquerie (au vu des divers modes opératoires) que s'il est correctement informé. Si on souhaite obtenir un impact préventif, il paraît donc opportun de dif-

- De communiquer aux services de police, dans les délais les plus brefs, toute information utile dont ils auraient connaissance.
- D'informer leur clientèle et de les inciter à déposer plainte ou à communiquer tout renseignement utile en cas de contact.
- En dénonçant à la CTIF (Cellule de Traitement des Informations Finan- ►►



- cières¹³), par une déclaration de soupçons, les transactions suspectes pouvant être liées à du blanchiment.

- **Le partenariat**

Il est évident que les mesures préconisées ci-avant ne peuvent être réalisées que dans le cadre d'un partenariat en matière d'échange d'informations entre les services de police spécialisés et les partenaires externes concernés (agents immobiliers, notaires, ...).

Comment réagir en cas d'incident ?

- Se méfier de toute proposition d'achat via Internet suivie de la réception d'e-mails provenant de prétendus agents immobiliers établis à l'étranger et agissant pour des investisseurs étrangers.
 - Porter attention au fait que les acheteurs/auteurs ne discutent pas le prix de vente.
 - Ne pas accepter une proposition d'échange ou de transaction en espèces qui présente des conditions trop avantageuses.
 - Refuser tout rendez-vous dans un pays étranger, que ce soit pour discuter d'une transaction ou pour la réaliser.
 - Ne pas offrir de résistance en cas d'usage de violence.
 - En cas de soupçons ou de doutes, informer les services de police.
- En cas de rip deal accompli, déposer plainte auprès des services de police du pays où les faits se sont déroulés de même que dans le pays d'origine de la victime.

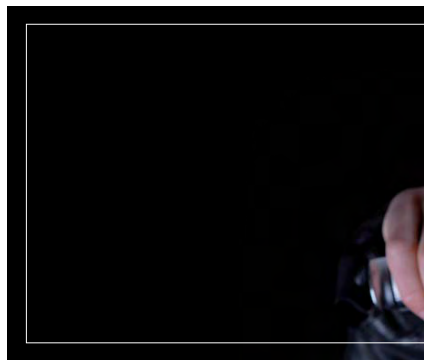
PRISE D'OTAGE

Cadre

Constituent une prise d'otages, « l'arrestation, la détention ou l'enlèvement de personnes pour répondre de l'exécution d'un ordre ou d'une condition ».

L'enlèvement (kidnapping) d'une personne fortunée en vue du paiement d'une rançon constitue une forme spécifique de prise d'otage.

Les auteurs d'une attaque à main armée qui sont surpris par l'arrivée de la police et qui prennent des personnes en otage pour assurer leur fuite est un exemple de prise d'otage non préparée.



Le « tiger kidnapping » est une forme particulière de prise d'otage : il s'agit de l'arrestation, la détention ou l'enlèvement, d'une ou plusieurs personne(s) afin de forcer un employé/mandataire, un proche ou une autre personne à remettre immédiatement aux auteurs toute valeur, somme d'argent considérable ou toute autre forme de rançon appartenant à une institution ou une entreprise. Ce genre d'infractions graves touche surtout le secteur bancaire.

Mesures préventives

- Veillez à sensibiliser les cadres de votre entreprise.
- Une entreprise peut se préparer à la réaction qu'il convient d'adopter en cas de prise d'otage d'un ou de plusieurs membres du personnel. Veillez, entre autres, à rédiger et à tenir à jour une fiche confidentielle comportant des données telles que l'état de santé, les médicaments nécessaires, l'implication dans certaines situations conflictuelles, la composition de famille et les coordonnées des cadres de votre entreprise.



- Il est recommandé de disposer d'un **plan de gestion de crise** dans lequel figurent, entre autres, l'analyse des incidents possibles, le flux d'information interne, les procédures d'avertissement, de décision et les premières réactions.

Les victimes potentielles d'une prise d'otage peuvent prendre un certain nombre de mesures préventives dans leur habitation, sur le lieu de travail, etc.

- Les victimes potentielles d'une prise d'otage peuvent prendre un certain nombre de mesures préventives dans leur habitation, sur le lieu de travail et lors des déplacements entre le domicile et le lieu de travail. Dans le cadre de missions à l'étranger, il est recommandé de procéder à une évaluation correcte de la situation locale :
 - Image de la criminalité locale ;
 - Événements importants pouvant avoir un impact sur l'ordre et la sécurité publics (élections, conflits sociaux, attentats, ...) ;
 - Connaissance des zones à risque éventuelles ;
 - Niveau de la menace liée au terrorisme ;
 - Qualité et fiabilité des services de police locaux ;
 - Climat politique et répercussions possibles sur l'entreprise.

Cela vous permettra de préparer un plan : briefing des cadres, indication de lieux sûrs, ►►

¹³ www.CTIF-CFI.be.

- élaboration d'un réseau local de contacts (consulat, certaines ONG, ...) auxquels on peut s'adresser en cas de menace/besoin.

Il est important de signaler le plus rapidement et minutieusement possible les événements inhabituels ou les agissements suspects.

- On peut envisager de s'assurer contre le risque d'enlèvement.
En ce qui concerne le « tiger kidnapping », les conseils suivants sont d'application :
- Modifiez certaines habitudes (votre itinéraire, l'heure de vos déplacements, le magasin où vous faites vos courses, le parking où vous garez votre véhicule) ;
- Soyez vigilant par rapport aux événements inhabituels. Avertissez immédiatement l'entreprise de téléphonie lorsque votre ligne est en dérangement. Il est également très important que vous signaliez le plus rapidement et minutieusement possible les événements inhabituels ou les agissements suspects, de sorte que la police puisse effectuer des patrouilles proactives et ciblées ;
- Au volant de votre voiture : regardez un peu plus votre rétroviseur afin de remarquer si une personne vous suit sur une distance étrangement longue. Ne prenez jamais un inconnu dans votre voiture. Veillez à savoir où se trouve le bureau de police ou un autre lieu sûr le long de votre itinéraire ;
- Soyez un peu plus attentif aux véhicules à proximité de votre habitation. Si vous habitez, par exemple, à la campagne et que vous remarquez deux jours d'affilée un véhicule inconnu, prenez note du numéro d'immatricu-

lation et avertissez la police, ainsi que le réseau d'information de quartier s'il y en a un ;

- Demandez au conseiller en prévention de la Police locale de venir chez vous afin de voir comment vous pouvez améliorer la sécurisation de votre domicile (par exemple, ne pas laisser une clé sous un pot de fleurs, éclairer l'allée et l'entrée, installer une alarme ou un bouton d'alarme) ;
- Ne laissez pas traîner votre agenda. Discutez-en toutefois avec vos proches collaborateurs afin que quelqu'un connaisse précisément vos projets et rendez-vous ;
- Installez un bouton d'alarme et limitez le nombre de personnes ayant accès au coffre-fort.

Comment réagir en cas d'incident ?

Pour la gestion de la crise, la protection de l'intégrité physique de la (des) personne(s) prise(s) en otage est la première priorité. Il importe de rassembler des informations sur les personnes prises en otages et les auteurs de la prise d'otage.

Lors d'un enlèvement, il convient de prendre immédiatement contact avec la police par le biais du numéro d'urgence 101 ou 112. L'enquête sera menée en toute discrétion afin de ne pas porter préjudice aux intérêts commerciaux de l'entreprise. Il est recommandé de rester discret si la prise d'otage n'a pas encore été rendue publique.

Toutes les traces liées à la prise d'otages et aux auteurs doivent être protégées afin que la police puisse effectuer les constatations nécessaires.

L'entourage (la famille ou un responsable de l'entreprise) peut entreprendre les démarches suivantes :

- Prendre note de manière chronologique de l'ensemble des faits tels qu'ils se sont déroulés ;
- Convenir d'un nom de code pour être reconnu lors des appels suivants ;
- Demander une preuve qu'ils « détiennent » la personne « x » ;
- Tenter d'établir une bonne entente ;
- Toujours insister sur le fait que l'on n'est pas le décideur (si l'entreprise est concernée) ;
- Ne pas traiter soi-même les lettres ou les autres messages concernant les exigences et les placer immédiatement dans une enveloppe.

Quelques conseils pour les victimes :

- Vos chances d'être libéré(e) sont fortement influencées par votre attitude : bonne condition physique, autodiscipline, patience, confiance en soi ;
- Plus le temps s'écoule, plus vos chances d'être libéré(e) augmentent ;

- Tentez de mémoriser un maximum de choses. Occupez votre esprit ;
- Sachez que l'on fera tout ce qui est possible pour vous aider mais que cela prend du temps.

VOL À MAIN ARMÉE

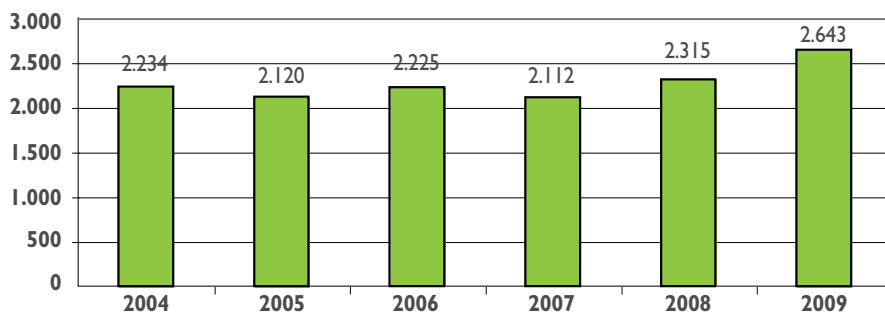
Cadre

S'ils sont moins fréquents que les vols simples et les cambriolages, les braquages (ou vols à main armée) ont un impact et des conséquences traumatisantes nettement plus importants. Un grand nombre d'entreprises prennent des mesures afin de se protéger contre ce problème.

Les vols avec violence, en particulier les vols à main armée (qui sont très traumatisants pour les victimes), sont en légère hausse. En ce qui concerne les vols à main armée, on observe un glissement de cible : alors qu'ils ►►

Vols à main armée (excepté sur la voie publique et car- et homejacking)

Source : Banque de données DJB/VMA



- visaient des cibles classiques mais à présent bien sécurisées (telles que des banques, des bureaux de poste, des transports de fonds), ces vols visent désormais des secteurs moins sécurisés et plus vulnérables (petits magasins, stations-service, secteur horeca, librairies, magasins de nuit, pharmacies, ...).

- Les braqueurs plus expérimentés préparent convenablement leur braquage, travaillent en groupe de manière organisée et ont déjà déterminé l'itinéraire qu'ils emprunteront pour leur fuite. Ils jettent leur dévolu sur des cibles détenant une grande quantité d'argent telles que des banques, des grands magasins, des bureaux de poste, des transports de fonds et des bijouteries ;
- Les braqueurs se font parfois passer pour des clients. Au moment opportun, ils menacent le personnel et le contraignent à ouvrir la caisse.



© Police Fédérale / Service communication

Un braquage présente les caractéristiques suivantes :

- Il ne dure généralement guère plus de quelques minutes ;
- Dans certains cas, les auteurs ne sont pas masqués ;
- La plupart des braqueurs cherchent de l'argent. Ils visent les tiroirs-caisses. Les valeurs et les biens sont moins intéressants ;
- Les jeunes braqueurs inexpérimentés choisissent les cibles les plus faciles telles qu'un snack-bar ou un magasin dans leur propre ville ou quartier. Ils sont vite en proie à la panique lorsqu'un événement imprévu survient au cours du braquage, ce qui augmente le risque de violence ;

Mesures préventives

Il importe de prendre des mesures afin de réduire le risque de braquage. Lorsque vous engagez du personnel, vous êtes tenu, en vertu de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail et de l'arrêté royal relatif à la prévention de la charge psychosociale occasionnée par le travail dont la violence, le harcèlement moral ou sexuel au travail, de prendre des mesures afin de protéger votre personnel contre les actes de violence et d'agression sur le lieu de travail, y compris donc contre les braquages. Il s'agit de mesures tant matérielles qu'organisationnelles.

Organisation de l'entreprise

- Culture et structure de l'organisation axée sur la prévention ;
- Aide et implication visibles de la direction de l'entreprise en vue de permettre une culture d'entreprise axée sur la résolution de problèmes ;

- Structure de prévention comportant un conseiller en prévention et une (des) personne(s) de confiance ;
- Améliorer les relations interpersonnelles, favoriser la coopération (le travail de groupe, l'aide sociale et l'appréciation sont les meilleurs remèdes à la violence, au harcèlement moral et sexuel sur le lieu de travail) ;
- Travailler en duo pour les fonctions « dangereuses » ou pour les travailleurs qui se sentent menacés ;
- Permettre au travailleur de donner son avis, de proposer des solutions ;
- Intégrer des indicateurs mesurables (prendre le pouls) et réaliser des évaluations et des mesures d'effet ;
- Prêter attention au problème de la violence, du harcèlement moral et sexuel sur le lieu de travail lors de l'accueil de nouveaux collaborateurs ou de travailleurs intérimaires ;
- Attribuer un parrain ou une marraine aux nouveaux collaborateurs ou travailleurs intérimaires ;
- Visite régulière du chef, du conseiller en prévention dans tous les espaces de travail et bureaux, ... ;
- Éviter de garder de grandes quantités d'argent dans les caisses (pas uniquement dans les magasins) et manipuler l'argent à l'abri des regards dans un local protégé ;
- Toujours transmettre à un collègue son programme de travail (heures de rendez-vous, adresses, numéros de téléphone, ...) pour les collaborateurs qui sont en service extérieur ;
- Réaliser une analyse des risques après les faits et prendre les mesures supplémen-

taires ou appropriées sur la base de cette analyse (voir l'organisation de l'entreprise et l'aménagement des lieux de travail) ;

- Coopérer avec les autorités locales et les entreprises voisines dans les zones géographiques qui sont souvent la cible ou sont susceptibles d'être la cible d'un acte d'agression et de violence externe.

Aménagement des lieux de travail

- Prévoir des toilettes et des vestiaires séparés pour les hommes et les femmes ;
- Ne pas laisser traîner des objets tranchants (coupe-papier, ciseaux, cutter, ...) et fixer les objets pouvant servir de projectile ;
- Limiter la quantité de meubles dans les locaux ;
- Adapter ou (ré)aménager les lieux de travail s'il s'avère qu'ils ne sont pas adaptés pour pouvoir faire face à une agression (externe). Il peut s'agir de modifications d'ordre électronique ou autre visant à réduire au minimum les risques de violence ;

Afin de mieux prévenir le vol à main armée, il est conseillé, pour les fonctions dangereuses, de travailler en duo.

- Prévoir des espaces de réception, des guichets, des locaux pour les services clientèle à des endroits bien visibles pour les autres travailleurs et le public (il est, dès lors, recommandé de ne pas placer un trop grand nombre d'affiches sur les ►►

- ▶▶ fenêtres afin que l'on puisse voir ce qui se passe à l'intérieur ;
- Prévoir un contrôle d'accès (sas d'accès, système de bouton-poussoir, ...) ;
- Disposer le mobilier de sorte qu'il n'entrave pas la liberté de mouvement du travailleur et que ce dernier soit plus près de la sortie que le client ;
- Utiliser des tables plus larges et plus hautes (bureaux, présentoirs) que la moyenne afin d'éviter autant que possible les contacts physiques ;

Des formations ciblées peuvent faire partie de la politique de prévention.

- Prévoir des systèmes de vidéosurveillance et de surveillance radio ;
- Installer un bouton d'alarme et d'avertissement, prévoir un numéro d'urgence préprogrammé (surveillance interne, police, ...) ;
- Installer un éclairage suffisant autour du bâtiment et au niveau des entrées ;
- Veiller à ce que les salles d'attente soient calmes et accueillantes : sièges confortables, pas d'éclairage trop fort ou aveuglant, espace suffisant entre les différents sièges et la table, mobilier fixé au sol, journaux pour passer le temps, pas d'objets pouvant être jetés ou pouvant servir d'arme.

Information et formation des travailleurs

- Informer les travailleurs concernant les risques, les différents instruments mis à

leur disposition, les mesures de prévention et procédures (par le biais du conseiller en prévention, de publications internes, d'un dépliant ciblé, de l'intranet, ...) ;

- Mener une campagne de sensibilisation annuelle (vidéo, témoignages, affiches, formations, ...) ;
- Placer des affiches sur des panneaux d'information ;
- Prêter attention au problème de la violence et de l'agression lors de l'accueil de nouveaux collaborateurs ou travailleurs intérimaires ;
- Les travailleurs doivent souvent recourir à des compétences qu'ils n'ont pas apprises au cours de leur formation. Des formations ciblées peuvent dès lors faire partie de la politique de prévention (par exemple formation en communication, cours de résistance en vue de la gestion de clients difficiles ou formation en affirmation de soi de manière générale).

© Police Fédérale / Service communication



Les mesures préventives suivantes peuvent être prises :

- Faites surtout attention aux moments et points à risque :
 - L'ouverture et la fermeture de l'entreprise ;
 - La caisse ;
 - L'endroit où se trouvent l'argent, les valeurs ou les objets de valeur (tel qu'un coffre-fort) ;
 - Le transport interne de valeurs, le comptage des recettes et le contrôle de la caisse ;
 - Le transport externe de valeurs ou le gérant qui emporte l'argent à son domicile.
- Prévoyez un **aménagement aisé à surveiller** au sein et aux alentours de votre entreprise :
 - Prévoyez des points stratégiques permettant de voir l'entrée et l'ensemble des locaux ;
 - Prévoyez un bon éclairage sur le lieu de travail et au niveau des entrées (sans partie ombragée) ;



- N'obstruez pas la vue en plaçant des panneaux ;
- Fermez toujours les portes des locaux se trouvant à l'arrière du bâtiment ;
- Demandez un avis complémentaire sur la sécurité interne à un conseiller en technoprévention.
- Placez des pictogrammes indiquant clairement à tout le monde (donc y compris aux braqueurs potentiels) que votre entreprise est bien sécurisée.
- **Ouvrez et fermez** l'entreprise avec prudence :
 - Méfiez-vous des personnes, des situations ou des véhicules suspects ;
 - Si possible, veillez à ce que votre entreprise soit toujours ouverte et fermée par deux personnes ;
 - Vérifiez que personne n'est resté dans l'établissement et/ou si certaines entrées n'ont pas été préparées pour l'intrusion ;
 - Fermez toujours votre entreprise de manière ponctuelle ;
 - Soyez attentif aux traces d'effraction ;
 - Méfiez-vous toujours (de manière saine) des nouveaux membres du personnel, fournisseurs ou transporteurs ;
 - Laissez toujours le tiroir-caisse vide ouvert lors de la fermeture de votre entreprise ;
 - Contrôlez les toilettes avant la fermeture (ronde avant la fermeture).
- Gérez l'argent de manière réfléchie :
 - Ne gardez pas dans la caisse plus d'argent que nécessaire pour rendre la monnaie ; ►►

- ▶ - Évitez de laisser la caisse ouverte lorsque cela n'est pas nécessaire ;
 - Favorisez l'utilisation de moyens de paiement électroniques ;
 - Installez un coffre-fort muni d'une serrure à ouverture temporisée et affichez-le clairement ;
 - Ne comptez pas l'argent à la vue des clients ;
 - La gestion et le transport de l'argent constituent un secret commercial ;
 - Placez un écran au-dessus du tiroir-caisse afin d'empêcher que l'on puise dans la caisse ;
 - Évitez les grandes quantités d'argent dans votre caisse et placez de préférence les recettes importantes dans un coffre-fort ou « dissimulez-les » à un autre endroit sûr ;
 - Placez des inscriptions mentionnant clairement que la caisse comporte uniquement de la petite monnaie et que les billets d'une grande valeur ne sont pas acceptés.
- Évitez les habitudes lors du transport de valeurs. Allez de préférence à la banque

pendant la journée. Si vous utilisez un coffre de nuit, assurez-vous qu'il n'a pas été manipulé. Si la clé n'entre pas facilement dans la serrure, interrompez immédiatement le versement. Idéalement, les transports importants devraient être effectués par deux personnes.

- Élaborez un bon plan de gestion des clés. Limitez le nombre de clés en circulation. Eu égard au risque de braquage, conservez les clés du coffre à un endroit fixe, mais ne les laissez jamais sur le coffre.
- Sensibilisez votre personnel à tous les aspects liés à la sécurité.

Comment réagir en cas d'incident ?

Si un braquage survient, appliquez les principes suivants :

- **Rester calme** : essayez de rester calme. Ne faites pas de mouvements brusques. Essayez d'éviter que l'auteur ait peur qu'une personne puisse entrer.



- **Accepter la situation** : suivez les ordres et évitez la provocation. Partez du principe que l'arme est vraie ! Collaborez avec le braqueur et ne protestez pas. Confirmez par votre attitude que le braqueur détient le pouvoir et le contrôle.
- **Céder l'argent** : en cas de braquage, ne songez pas (plus) à vos biens mais pensez à votre propre sécurité physique, à celle de votre personnel et de vos clients. Informez, dès lors, au préalable votre personnel sur la manière d'agir dans une telle situation. Portez à la connaissance de l'auteur la procédure concernant le coffre-fort (le cas échéant, la serrure à ouverture temporisée).
- **Observer** : tentez de vous souvenir du signalement du (des) braqueur(s), ainsi que de la direction dans laquelle il(s) a (ont) fui et le moyen de transport utilisé. N'entrez en aucun cas leur fuite et ne tentez pas non plus de les suivre. Envisagez l'installation d'un système d'alarme silencieux afin de prévenir la police.

Au cours d'un braquage, il faut toujours tenter de garder le **contrôle de soi** et de penser de **manière positive** : « Je dois rester calme, il ne vient pas pour moi. Je vais m'en sortir vivant ! »

En vue d'une éventuelle identification et arrestation des auteurs, vous trouverez, ci-après, quelques éléments et conseils pouvant faciliter le travail de la police :

- Donner les détails physiques des auteurs (taille et corpulence, langue et élocution, chaussures ou vêtements) ;
- Donner les caractéristiques du véhicule ayant servi à la fuite, éventuellement le numéro d'immatriculation et la direction dans laquelle les auteurs se sont enfuis ;
- Préciser les objets ayant été touchés par l'auteur ;

Si un braquage survient, essayez de rester calme. Ne faites pas de mouvements brusques.

- Rassembler les témoins ;
- Fermer directement l'entreprise et n'effacer aucune trace ;
- Procéder au signalement de l'auteur et noter immédiatement et **individuellement** les détails de l'événement ;
- Dresser l'inventaire des pertes et du butin.

Une telle expérience peut être traumatisante, voire déboucher sur une incapacité de travail. Voici dès lors quelques conseils à prendre en considération lorsque l'on est victime de tels faits :

- Prenez le temps de parler de l'événement ;
- Écoutez les sentiments d'anxiété des autres personnes et ne faites pas de reproches ;
- Demandez à la police de bénéficier d'une aide aux victimes (renvoi vers l'accueil spécialisé des victimes).



►► CAR-JACKING

Cadre

Un car-jacking est un vol (ou une tentative de vol) d'un véhicule au cours duquel les auteurs ont recours à la violence ou à la menace vis-à-vis du conducteur ou du (des) passager(s). Il se peut toutefois aussi qu'ils aient recours à la violence (ou à la menace) au moment où ils sont pris en flagrant délit, et ce, afin de conserver le véhicule volé ou d'assurer leur impunité.

Les car-jackings représentent (seulement) 3,5% du nombre total de vols de véhicules (chiffres de la police pour 2009). S'il est commis dans l'ensemble du pays, ce type de vol est principalement observé dans les arrondissements de Bruxelles (Bruxelles, Asse...), Liège, Charleroi, Anvers et Mons.

Les car-jackings représentent (seulement) 3,5% du nombre total de vols de véhicules (chiffres 2009).

Environ la moitié des véhicules volés selon ce modus operandi sont retrouvés.

Ce sont principalement les véhicules récents qui sont volés. Plus de la moitié des véhicules faisant l'objet d'un car-jacking ont moins de deux ans. Les voitures de direction (modèles plus chers ; ces véhicules étant souvent pris en leasing, le senti-



ment de propriété est moindre) sont assurément les cibles privilégiées des auteurs de car-jackings.

Mesures préventives

Les victimes potentielles peuvent prendre un certain nombre de mesures préventives afin de mieux se protéger. Ces mesures peuvent être de nature générale (fermeture des portes lorsque tout le monde se trouve dans le véhicule, séparer les clés de la voiture et celles du domicile, conserver au domicile une copie de tous les documents de bord), mais aussi de nature plus spécifique :

- Évitez les risques lorsque vous entrez dans votre véhicule ou en sortez (garez toujours votre voiture à un endroit bien éclairé et non isolé ; faites attention aux personnes venant apparemment vous poser des questions lorsque vous entrez dans votre véhicule ou en sortez, ...) ;
- Évitez les risques sur la route (fermez les fenêtres et les portes, surtout dans les



grandes villes ; soyez vigilants lorsque vous devez vous arrêter; vérifiez régulièrement si vous n'êtes pas suivi, anticipez afin de ne pas être immobilisé, ...)

- Évitez les risques lors d'une collision (gardez à l'esprit qu'une collision peut avoir été causée volontairement afin que vous quittiez votre véhicule ; soyez toujours vigilant et fermez toutes les portières si vous remarquez quelque chose de suspect ; communiquez dans un premier temps à travers la fenêtre à moitié ouverte, ...)
- Évitez les risques en cas de barrage (si d'autres usagers de la route barrent la chaussée, tentez de garder une certaine marge de manœuvre afin de pouvoir éventuellement partir avec votre véhicule, ...)
- On peut également recommander des mesures axées sur le véhicule telles que des mesures relatives à la structure, l'électromécanique et l'électronique dans le cadre desquelles on peut envisager tous les systèmes d'alarme possibles. On observe

une nouvelle évolution à cet égard, à savoir le recours à des systèmes « after theft » (après-vol) qui permettent de localiser le véhicule par GPS.

Comment réagir en cas d'incident ?

Si vous êtes victime d'un car-jacking, ne commettez pas d'imprudences : restez calme, n'opposez pas de résistance, évitez le contact physique, éloignez-vous de l'auteur (des auteurs) si vous en avez la possibilité et avertissez immédiatement les services de police.

VOL DANS VÉHICULES

Cadre

Le vol de ou dans votre voiture peut poser une multitude de problèmes. Les dépenses imprévues, les tracasseries administratives, la perte de temps et un sentiment désagréable ne sont que quelques-unes des conséquences découlant d'un tel vol. Tout le monde s'accorde à dire que, dans ce domaine, il vaut mieux prévenir que guérir; mais les gens ignorent souvent les mesures simples qu'ils peuvent prendre. Et il ne s'agit pas seulement d'alarmes onéreuses.

Chaque année, environ 70.000 faits de vol dans des véhicules sont commis, soit 190 par jour. La plupart des vols surviennent dans les grandes villes, qui offrent un plus grand anonymat et comptent une multitude de véhicules. Voici le top 10 des biens les plus volés : sac et porte-monnaie ►►

- ▶▶ (+20 %), GPS, argent, cartes bancaires, autoradio, CD, permis de conduire, GSM, documents de bord, ordinateur portable et vêtements.

Nous souhaitons particulièrement attirer votre attention sur les documents de bord (et en particulier le certificat d'immatriculation), qui sont la véritable carte d'identité du véhicule. Le certificat d'immatriculation est capital et constitue le fil rouge du trafic de véhicules. Ce document permet de réintégrer un véhicule volé dans le circuit légal (grâce à une immatriculation à l'étranger).

Quand vous quittez le véhicule, emportez toujours les documents de bord, car ils valent de l'argent pour les criminels.

Mesures préventives¹⁴

- Garez de préférence votre voiture dans un garage ou dans un autre endroit sûr. Choisissez en tout cas un emplacement de parking non isolé et bien éclairé ;
 - **Fermez toujours soigneusement votre voiture** : n'oubliez pas de fermer les portières, les fenêtres, le toit ouvrant et le coffre de votre véhicule. C'est important car si vous laissez votre voiture ouverte et qu'un vol y est commis sans effraction, l'assurance considérera que ce n'est pas un vol. Vous risquez en outre une amende importante ;
 - Quand vous quittez le véhicule, **emportez toujours les documents de bord**, car ils
- valent de l'argent pour les criminels. Prenez systématiquement cette mesure de précaution en cas d'absence prolongée¹⁵ ;
 - **Enlevez toujours de la voiture votre GPS et son support. Essayez également la marque laissée par la ventouse du GPS** sur votre pare-brise. À la vue du GPS et/ou du support et/ou de l'empreinte laissée par la ventouse du GPS, les voleurs font intrusion dans votre véhicule pour s'approprier le GPS ;
 - **Désactivez toujours la fonction bluetooth et wifi** (de votre GPS, ordinateur portable, GSM, ...) afin que les voleurs potentiels ne puissent pas capter le signal et savoir que des objets de valeur se trouvent dans le véhicule ;
 - S'il n'y a aucun objet de valeur dans votre véhicule, montrez-le : ouvrez la boîte à gants et/ou la plage arrière ;
 - Les objets qui restent (exceptionnellement) dans le véhicule sont placés de préférence dans le coffre (fermé). **Mettez l'objet dans votre coffre sur le lieu de départ** et non sur le lieu de destination, de sorte qu'un voleur potentiel ne voit pas cette opération ;
 - Dressez l'inventaire des numéros de série,



de la marque et du modèle de l'ensemble de vos objets de valeur (vous trouverez des exemples sur le site www.besafe.be). Faites de même pour votre GPS, ordinateur portable, numéro IMEI du GSM, ... Les numéros de série et IMEI sont des numéros uniques permettant à la police de restituer plus rapidement au propriétaire légitime les objets volés retrouvés ;

- **Utilisez le code PIN sur votre GPS.** Cette option est souvent prévue mais n'est pas installée de manière standard. Installez-la. En cas de vol, votre GPS ne peut plus être utilisé sans le code PIN adéquat.

Points concernant spécifiquement le certificat d'immatriculation

Pour chaque voiture de leasing/de location, il y a deux certificats d'immatriculation:

1. Le certificat original (est généralement conservé au siège principal de l'entreprise) ou un duplicata (en cas de perte ou de vol de l'original)
2. La copie du certificat (dès lors qu'il accompagne généralement le véhicule, ce certificat est détenu par le locataire

– voir photo) ; il s'agit d'un document authentique sur lequel figurent les données suivantes :

- a. Véhicule destiné à être loué ;
- b. Copie établie pour être utilisée par le locataire du véhicule ;
- c. Copie non valable lors de la vente du véhicule !

Nous conseillons vivement aux sociétés de leasing ou de location de véhicules d'utiliser la copie. Celle-ci peut être demandée gratuitement à la Direction de l'immatriculation des véhicules (DIV) lors de l'immatriculation.

Comment réagir en cas d'incident ?

Si vous êtes victime d'un vol en dépit de toutes les précautions prises, rendez-vous le plus rapidement possible à un service de police, si possible avec la fiche d'identification¹⁴ de votre véhicule.

En cas de vol des documents de bord, il est encore plus recommandé de faire une ►►



¹⁴ La brochure « Évitez les vols dans votre voiture » du SPF Intérieur peut être consultée sur le site www.besafe.be.

¹⁵ Sur le site www.besafe.be, vous pouvez commander gratuitement un porte-documents et les brochures de prévention.

¹⁶ Vous trouverez un exemple sur le site www.besafe.be.

- déclaration à la police locale. Sans déclaration, vous ne pouvez en effet pas demander à la Direction de l'immatriculation des véhicules (DIV) le duplicata d'un certificat d'immatriculation.

En cas de vol des documents de bord, il est recommandé de faire une déclaration à la police locale.

La demande d'un duplicata du certificat d'immatriculation volé constitue une raison supplémentaire de faire une déclaration. Elle empêche en effet une personne d'immatriculer un véhicule à l'étranger à l'aide du certificat d'immatriculation volé. Votre document ne peut ainsi faire l'objet d'aucun abus.

VANDALISME

Cadre

Le vandalisme est l'une des formes de criminalité les plus fréquentes. Le problème trouve généralement son origine en dehors de l'entreprise. La plupart des entreprises s'attendent à ce que le nombre d'actes de vandalisme reste relativement stable à l'avenir.

Le vandalisme est une infraction propre aux jeunes. Il s'agit souvent de garçons (dans une moindre mesure de filles) âgés de 8 à 16 ans. Ils se rendent délibérément coupables de destructions ou de dégradations, sans rien en tirer sur le plan matériel. Leur unique but est l'acte de destruction ou de

dégradation. Ils explorent ainsi leurs propres limites et tentent de braver le monde des adultes. Le fait de commettre des actes de vandalisme leur permet d'être mieux considérés par leur groupe d'amis.

Les établissements d'enseignement et les organisations de jeunesse prennent un grand nombre de mesures afin de lutter contre le vandalisme. Le fait d'infliger des peines alternatives permet également d'étouffer dans l'œuf bon nombre de problèmes.

Si vous souhaitez prendre des mesures en tant qu'entrepreneur, il importe de garder à l'esprit deux caractéristiques. Le vandalisme est un acte impulsif : l'occasion fait le larron. Il constitue, en outre, un acte social. Il est presque toujours commis en groupe. Bien que le niveau de victimisation potentielle liée au vandalisme soit élevé, les entreprises ne prennent guère de mesures spécifiques pour se protéger contre cette forme de criminalité. Une surveillance interne (et dans une moindre mesure une surveillance externe) concourt indirectement à la diminution du risque. Ces mesures de sécurisation sont souvent prises par les entreprises de plus grande taille, qui sont déjà en proie à des faits de sabotage, de vandalisme ou de vol.

Mesures préventives

Vous pouvez prévenir un grand nombre de problèmes de vandalisme en renforçant le **contrôle informel** dans les environs immédiats de votre entreprise. Plusieurs possibilités sont envisageables :

- Organiser des actions de nettoyage

en collaboration avec le service de nettoyage dans votre commune et les habitants (jeunes et moins jeunes) de votre quartier ;

- Collaborer à l'organisation de festivités dans votre quartier afin de renforcer l'implication des habitants dans votre environnement ;
- Associer les jeunes à l'aménagement de votre environnement en leur permettant, par exemple, d'effectuer des travaux de peinture sur les volets ou les palissades qui sont constamment souillés.

Vous pouvez également renforcer le contrôle formel, avec l'aide notamment d'une entreprise de gardiennage.

Il vous est également possible de prévenir des problèmes en procédant à des **adaptations de l'environnement physique** de votre entreprise. Vous pouvez prendre les mesures suivantes à cette fin :

- Veillez à un bon entretien et réparez rapidement ce qui a été détruit ;
- Renforcez les objets vulnérables, par exemple en utilisant du verre et du plastique incassables. Songez toutefois au fait que les objets renforcés constituent un plus grand défi pour les vandales. Les objets renforcés étant en outre souvent plus chers, les dommages causés par les actes de vandalisme sont plus importants ;
- Protégez les objets vulnérables, par exemple à l'aide de plantations, de volets ou de grillages ;
- Embellissez les objets vulnérables, par exemple en utilisant différentes couleurs



ou en donnant une structure en relief aux murs et aux portes lisses ;

- Enlevez les objets vulnérables.

Enfin, vous pouvez lutter contre le vandalisme en **aménageant les abords** de votre entreprise. Il est ainsi recommandé de faire en sorte que l'on ait une vue suffisante sur l'espace entourant l'entreprise. Vous éviterez ainsi l'apparition de lieux de rassemblement où des jeunes viennent traîner.

Comment réagir en cas d'incident ?

Bien entendu, il convient également **dans tous les cas** de faire une déclaration à la police locale, qui constitue votre interlocuteur par excellence dans le cadre de tels incidents.

Les actes de vandalisme, les dégradations et les graffitis peuvent aussi être déclarés via le guichet virtuel de la police sur le site web **www.police-on-web.be**. Vous trouverez de plus amples renseignements à cet égard au point 4 de la présente brochure. ●



2

Early warning system : un partenariat public - privé contre le terrorisme

UN MOT D'EXPLICATION SUR LE « EARLY WARNING SYSTEM »

Dans le cadre de la lutte anti-terroriste, la collaboration entre différents services et autorités compétentes est permanente. Cette approche intégrée et intégrale a été étendue au secteur privé au sein de la Plate-forme de concertation permanente sur la sécurité des entreprises.

Depuis mars 2009, un réseau d'information pour les entreprises a été formellement démarré. Les entreprises et les services publics échangeront des informations selon une pro-

cédure établie de sorte que les firmes concernées soient informées à temps d'une menace éventuelle et qu'elles puissent ainsi prendre les mesures préventives appropriées.

Les services publics fédéraux Justice et Intérieur ont mis sur pied le réseau d'échange d'informations, en étroite collaboration avec la Fédération des Entreprises de Belgique. Un protocole d'accord a été signé le 6 mars 2009 par le ministre de la Justice Stefaan De Clerck, le ministre de l'Intérieur Guido De Padt et l'administrateur délégué de la Fédération des Entreprises de Belgique, Mr Rudi Thomaes.

Le « early warning system » a pour objectif de permettre à l'ensemble des intervenants de disposer d'un maximum d'informations au moment opportun. Le principe suivi est la création d'un « carré de l'information » qui nécessite que chaque secteur possède un flux d'informations structuré où l'information circule de l'entité locale vers le partenaire fédéral et vice versa.

Ce système d'information rapide pourrait être à présent utilisé pour différents types d'événements : des dégâts occasionnés à l'encontre d'entreprises et de produits fortement critiqués par certains milieux, des lettres anonymes adressées à une entreprise lançant par exemple des appels à la bombe ou toute autre menace, un rassemblement sensible de manifestants devant une entreprise, le comportement suspect d'une personne photographiant une firme dont le pays est impliqué dans une crise au niveau international, une manifestation sensible nécessitant une information précise des entreprises...

Un domaine aussi sensible que le terrorisme demande une coordination étroite des autorités. Celles-ci effectuent une évaluation quotidienne de la menace afin de prendre, à titre de précaution, les mesures de sécurité les plus appropriées. L'entrée en vigueur du « carré de l'information » démontre l'action préventive importante menée tant par le secteur privé que par les autorités publiques.

Du côté des entreprises, la FEB joue un rôle crucial dans la diffusion ciblée de l'information.

Du côté du secteur public, les partenaires les plus importants sont :

- La Direction Générale du Centre de Crise (SPF Intérieur)
- La Sûreté de l'Etat (SPF Justice)
- La Police fédérale
- L'Organe de Coordination et d'Analyse de la Menace (OCAM)
- Le Parquet fédéral

Le réseau est alimenté d'initiative tant par les partenaires publics que privés : de l'information dépersonnalisée est échangée sur les agissements suspects ou incidents constatés par les entreprises ou sur les menaces potentielles qui sont analysées par les autorités.

QUELLES INFORMATIONS NE SONT PAS ÉCHANGÉES ?

Le réseau d'information n'est pas utilisé pour communiquer systématiquement tous les incidents et menaces envers l'ordre public et la sécurité.

Ce réseau n'a pas l'intention de se substituer à la communication traditionnelle entre la police locale et les entreprises.

POUR QUI ET PAR QUI ?

Il s'agit d'un flux d'information entre le secteur public et le secteur privé.

COMMENT ?

Via un point de contact central, les responsables nationaux des entreprises entretiennent ►►

FEB ALERT CONTACT POINT

E-mail : FEBalert@belgacom.be

Téléphone : 0800/91.777

Si ce numéro n'est pas joignable, veuillez essayer les possibilités suivantes :

Ligne d'urgence : 02/202.18.00

Lignes non-PABX : 02/202.61.24 et 02/202.61.25

Fax : 02/202.63.29

- des contacts avec les services nationaux chargés de la lutte contre le terrorisme. Le système a connu une période de test positive et fera régulièrement l'objet d'une évaluation afin de le peaufiner et de l'adapter si nécessaire.

COOPÉRATION PUBLIC-PRIVÉ

Le protocole d'accord entre les partenaires publics et privés fut opérationnel dès le 6 mars 2009, après avoir été signé par les ministres de la Justice et de l'Intérieur

La coopération public-privé est une initiative de la Plate-forme de concertation permanente sur la sécurité des entreprises.

et l'administrateur délégué de la Fédération des Entreprises de Belgique.

Cette forme de coopération public-privé est une initiative de la Plate-forme de

concertation permanente sur la sécurité des entreprises, qui depuis de nombreuses années est dirigée par le service de politique criminelle du SPF Justice.

Si vous souhaitez obtenir des informations complémentaires par le biais de la Commission « Sécurité des entreprises » au sein de la FEB, il vous est loisible de prendre contact avec Mme Christine Darville, coordinatrice de cette commission ou Mr Gilbert Geudens, président de la commission.

FONCTIONNEMENT DU CARRÉ DE L'INFORMATION

Le carré de l'information a pour objectif d'échanger des informations pertinentes entre le secteur public et le secteur privé dans le cadre d'une (éventuelle) menace terroriste. Le carré de l'information complète les canaux politiques existants. Les notifications de situations suspectes ou de menaces envers une entreprise doivent donc toujours se faire via la police locale.

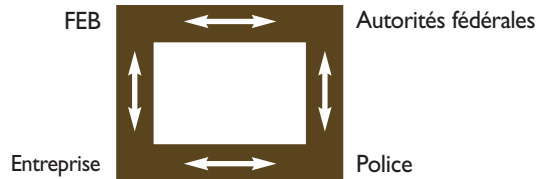


Cette dernière transmettra à son tour les informations aux autorités fédérales, où une analyse en profondeur des informations sera entre autres effectuée.

L'entreprise peut à présent également transmettre ces informations à un point de contact national organisé par le monde des entreprises. Ce point de contact transmettra également les informations aux autorités fédérales. Un système d'alerte précoce (« Early warning system ») est ainsi lancé

pour des informations pertinentes potentielles venant des entreprises.

Inversement, les autorités (en plus de la transmission d'informations vers et via la police locale) peuvent informer via le point de contact national un ou plusieurs secteurs d'une situation spécifique ou d'une menace afin que la vigilance soit augmentée ou que des mesures de sécurité complémentaires soient prises.



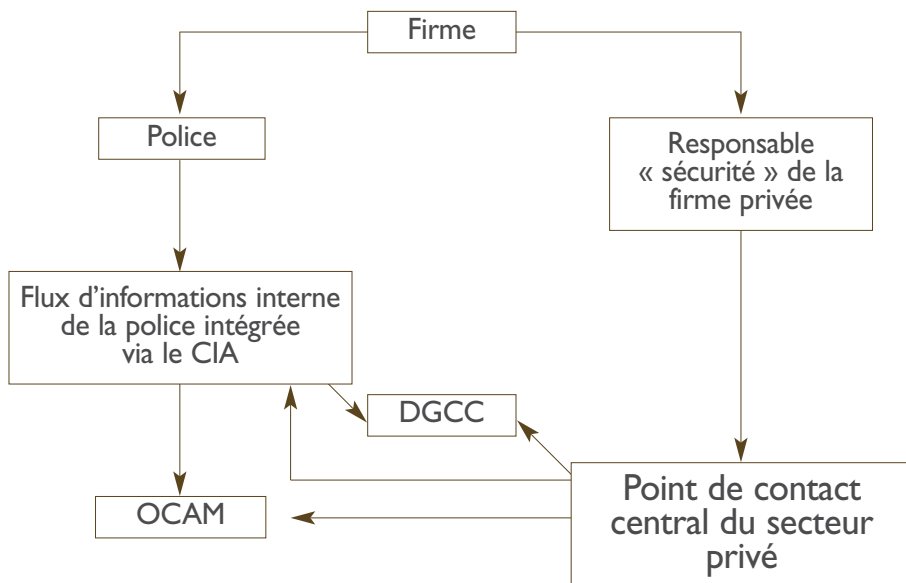
EXEMPLES D'APPLICATION DU CARRÉ DE L'INFORMATION ET/OU DU POINT DE CONTACT

- Mouvements suspects aux alentours d'une entreprise ;
- Messages anonymes adressés à une entreprise ;
- Attroupement "sensible" aux portes de l'entreprise ;
- Feedback aux entreprises concernant des agissements (présumés) suspects ;
- Transmission de données spécifiques d'entreprises ou de secteurs aux autorités (ex: coordonnées des responsables de la sécurité).



EXEMPLE I :

▶▶ ALERTE À LA BOMBE – INCIDENTS – AGISSEMENTS SUPECTS /
SECTEUR PRIVÉ VERSUS SECTEUR PUBLIC



Légende:

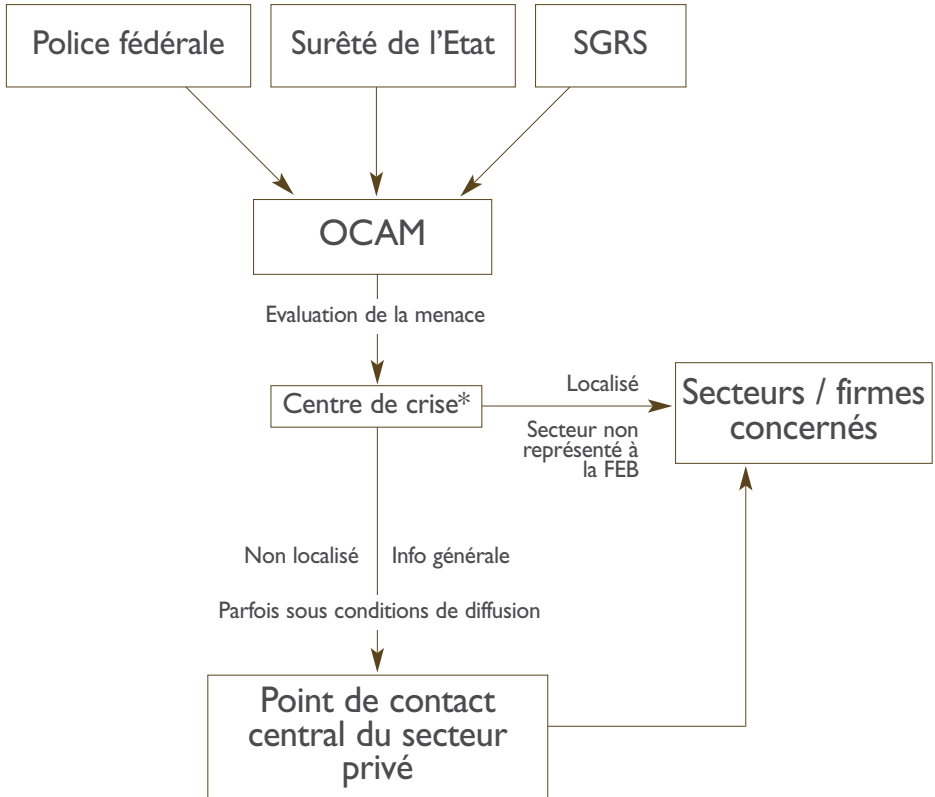
CIA : Carrefour d'information d'arrondissement de la Police fédérale

DGCC : Direction générale du Centre de Crise

OCAM : Organe de Coordination et d'Analyse de la Menace

EXEMPLE 2 :

MENACES – RECOMMANDATIONS – SECTEUR PUBLIC VERSUS SECTEUR PRIVÉ



*Transmission également vers la Police fédérale via les canaux prévus.

Dans le cas où le secteur privé apprend de sa société mère à l'étranger que les mesures de protection doivent être augmentées, un cross-check du secteur privé vers le secteur public peut avoir lieu via le point de contact central. ●

Légende:

OCAM : Organe de Coordination et d'Analyse de la Menace

SGRS : Services généraux du Renseignement et de la Sécurité militaire



© Police Fédérale / Service communication

3 Conseils en technoprévention¹⁷

QU'EST-CE QUE LA TECHNOPRÉVENTION ?

La technoprévention vise à prévenir les cambriolages, les vols à la tire et les attaques. Cette discipline englobe trois types de mesures de sécurisation qui sont toujours traitées dans l'ordre suivant :

- a. Mesures organisationnelles,
- b. Mesures mécaniques,
- c. Mesures électroniques.

Ces mesures permettent de réduire considérablement les risques d'être victime d'un cambriolage, d'un vol ou d'une attaque.

a. Mesures organisationnelles :

La sécurité commence par la prise de

bonnes habitudes. Ces mesures peuvent être appliquées par tout le monde, elles ne coûtent pas cher et sont tellement simples qu'elles sont souvent négligées. Or, elles constituent la première étape essentielle du plan de sécurisation. Exemples : bonne gestion des clés, enregistrement des objets de valeur, portes et fenêtres fermées à clé même pour une brève absence, ...

b. Mesures mécaniques :

Vous pouvez renforcer les portes et fenêtres de votre commerce pour rendre la tâche difficile aux cambrioleurs potentiels¹⁸. Exemples : vitrage de sécurité, volets anti-effraction, systèmes de sécurisation pour les portes, fenêtres, volets, portes de garage, coupoles, fenêtres de toit, soupiraux

et clôtures, comme des serrures de sécurité, des systèmes de sécurisation des serrures, verrous de sécurité et entrebâilleurs, coffres-forts, ...

c. Mesures électroniques :

L'installation d'un système de sécurité électronique doit s'effectuer en combinaison avec des mesures organisationnelles et techniques préalables. Les mesures électroniques sont donc un complément aux mesures organisationnelles et techniques. Exemples : systèmes d'alarme, caméras de surveillance¹⁹ (voir infra, le point « Caméras de surveillance »), systèmes de suivi, ...

Savez-vous que vous pouvez bénéficier d'un soutien du gouvernement lorsque vous réalisez des investissements en sécurité dans votre commerce ? Pour plus d'infos sur la déduction fiscale majorée dont vous pouvez bénéficier, adressez-vous au conseiller en technoprévention de votre zone de police²⁰.

QU'EST-CE QU'UN CONSEILLER EN TECHNOPRÉVENTION ?

Le conseiller en technoprévention est actif au sein de la commune ou de la police. Il est agréé par le Service public fédéral Intérieur et formé pour délivrer des con-

seils neutres et gratuits en matière de technoprévention.

QUEL EST LE RÔLE DU CONSEILLER EN TECHNOPRÉVENTION ?

Les principales missions du conseiller en technoprévention (CTP) consistent à :

- a. Fournir gratuitement des avis objectifs et complets en termes de sécurisation contre le cambriolage;
- b. Fournir des conseils préventifs aux candidats constructeurs ou aux personnes qui rénovent une habitation, parfois sur la base des plans réalisés par l'architecte (sur demande);
- c. Conseiller les indépendants, commerçants, titulaires de professions libérales, ... en matière de sécurisation contre le cambriolage/les attaques/les vols à l'étalage;
- d. Donner des explications/conférences sur la prévention de la criminalité à différents groupes cibles (à la demande de groupements de citoyens, d'associations de quartier, d'associations de commerçants, d'unions professionnelles, ...);
- e. Apporter des informations pertinentes et actuelles relatives au matériel de technoprévention et aux différentes techniques de sécurisation et de prévention.



¹⁷ Source : www.besafe.be.

¹⁸ Plus d'infos sur : www.veiligewoning.be.

¹⁹ Loi du 21 mars 2007 – www.privacycommission.be.

²⁰ Ou sur le site www.besafe.be (rubrique Indépendants).



COMMENT ENTRER EN CONTACT AVEC LE CONSEILLER EN TECHNO-PRÉVENTION LE PLUS PROCHE ?

Sur le site www.besafe.be, un moteur de recherche permet de trouver un conseiller en technoprévention sur la base de son code postal. N'hésitez pas à contacter cette personne et à prendre un rendez-vous. N'oubliez pas qu'il s'agit d'un service professionnel, objectif et entièrement GRATUIT.

CAMÉRAS DE SURVEILLANCE

Outre le respect des conditions légales, il importe également que les images puissent servir à rechercher les auteurs du vol.

Le recours à la surveillance par caméras est régi par la loi du 21 mars 2007, qui établit une distinction entre trois catégories de lieux, à savoir : les lieux ouverts (par exemple une place), les lieux fermés accessibles au public (par exemple un magasin) et les lieux fermés non accessibles au public (par exemple une entreprise, un entrepôt).

Pour pouvoir utiliser des caméras de surveillance, il faut satisfaire à un certain nom-

bre de formalités. Vous trouverez ci-dessous la liste de vérification relative à l'utilisation de caméras de surveillance dans des lieux fermés accessibles au public à l'aide de caméras de surveillance FIXES.

Liste de vérification relative à l'utilisation de caméras de surveillance dans des lieux fermés accessibles au public.

- Est-il clairement déterminé à quelle(s) fin(s) une surveillance par caméras est effectuée ? L'emplacement et l'utilisation des caméras satisfont-ils aux principes fixés dans la loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel ? En d'autres termes :
 - **Principe de finalité** : Les objectifs de sécurité que l'on souhaite atteindre sont-ils clairement déterminés ? Attention : vous pouvez uniquement utiliser les images dans le cadre de la finalité déterminée.
 - **Principe de subsidiarité** : Pouvez-vous démontrer qu'un système de caméras est le moyen approprié et nécessaire pour atteindre vos objectifs de sécurité ?
 - **Principe de proportionnalité** : Pouvez-vous démontrer qu'il y a un équilibre entre l'augmentation du niveau de sécurité et l'incidence sur le droit à la protection de la vie privée ?
- Une déclaration a-t-elle été faite auprès de la Commission pour la protection de la vie privée²¹ au plus tard la veille du jour où les caméras de surveillance ont été mises en service ?
- Une déclaration a-t-elle été faite au chef de corps de la zone de police concernée



au plus tard la veille du jour où les caméras de surveillance ont été mises en service ?

- Un pictogramme indiquant la présence de caméras de surveillance a-t-il été placé à l'entrée du lieu fermé accessible au public ?
- Les caméras sont-elles exclusivement dirigées vers les lieux pour lesquels le responsable du traitement traite lui-même les données ?
- Le visionnage des images en temps réel est-il uniquement effectué afin de pouvoir intervenir immédiatement en cas d'infraction, de dommage ou de trouble de l'ordre public ?
- L'enregistrement d'images vise-t-il exclusivement à réunir la preuve de nuisances, de faits constitutifs d'infraction ou générateurs de dommages, à rechercher et à identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes ?
- Si elles ne peuvent contribuer à apporter la preuve d'une infraction, d'un dommage ou d'une nuisance ou ne peuvent permettre d'identifier un auteur des faits, un perturbateur de l'ordre public, un témoin ou une victime, ces images ne sont-elles pas conservées plus d'un mois ?
- Les mesures de précaution nécessaires ont-elles été prises pour éviter que des personnes non autorisées aient accès aux images ?
- Les caméras ne fournissent-elles d'images qui portent atteinte à l'intimité d'une personne et ne visent-elles pas à recueillir des informations relatives aux opinions philosophiques, religieuses, politiques ou syndicales, à l'origine ethnique ou sociale, à la vie sexuelle ou à l'état de santé ?

Quelques conseils en vue d'un placement adéquat de la (des) caméra(s) :

- Placez la caméra à hauteur des yeux et évitez que des objets se trouvent dans le champ de vision de la caméra (ex. : des dispositifs de publicité) ;

Un pictogramme indiquant la présence de caméras de surveillance doit être placé à l'entrée du lieu fermé accessible au public.

- Le contre-jour et les reflets ont également une incidence sur la qualité des images ;
- Faites un test quotidien de la position de la caméra et vérifiez lors de la fermeture si la caméra n'a pas été endommagée, tournée ou couverte ;
- Veillez à ce que votre personnel sache où se trouve la caméra et comment elle doit être utilisée ;
- Mettez les appareils d'enregistrement dans un lieu sûr (invisible et dans une armoire/ un espace fermé(e) ;
- Contrôlez régulièrement la qualité des enregistrements.

AUTRES MESURES DE SÉCURISATION

Pour d'autres mesures de sécurisation telles que des systèmes de suivi, des alarmes, ..., nous vous renvoyons au site du SPF Intérieur²².

²¹ <https://www.privacycommission.be/elg/cameraMain.htm> - « déclaration thématique ».

²² www.vigilis.be.



4

Liens et sites web utiles

POLICE ON WEB



www.police-on-web.be est le guichet virtuel de la police ou un guichet électronique où vous pouvez **déposer plainte** pour les infractions figurant dans la liste ci-dessous, laisser un message d'absence et signaler votre alarme.

Police on web permet aux citoyens et aux entreprises d'enregistrer certaines plaintes sans se rendre au bureau de police. Les plaintes peuvent donc être déposées 7j/7, 24h/24, par le biais de n'importe quel PC connecté à Internet, et ce pour les faits suivants :

- Vol de vélo ;
- Vol de vélomoteur ;
- Vol à l'étalage ;
- Dégradations diverses ;
- Graffiti.

Pour introduire une plainte, vous devez vous identifier à l'aide :

- D'une carte d'identité électronique, du lecteur de carte d'identité et d'un ordinateur connecté à Internet ;
- D'un « token » : il s'agit d'une petite carte (format d'une carte bancaire) comportant 24 codes personnels et pouvant être obtenue par le biais du portail fédéral [federaal.be](http://www.federaal.be) ;
- D'un compte sur le portail fédéral [federaal.be](http://www.federaal.be) pouvant être créé sur la base du numéro de registre national, du numéro de la carte SIS et du numéro de la carte d'identité.

ECOPS



eCops est un point de contact en ligne où vous pouvez, en tant qu'utilisateur d'Internet, signaler des **délits commis sur ou via l'Internet**. Vous ne devez plus vous soucier de savoir quel service est compétent, eCops veille à ce que votre signalement soit examiné par le service adéquat.

Vous êtes tombé sur un site troublant contenant des informations trompeuses ? Vous avez reçu par e-mail des publicités non sollicitées ou une proposition frauduleuse ? Vous avez vu de la pédopornographie sur un site ?

Votre signalement peut entraîner une action de la part du SPF Économie, de la Police ou de la Justice. Vous remplissez votre demande étape par étape à l'aide du formulaire en ligne sur **www.ecops.be**

eCops n'est pas un centre d'appel urgent en ligne des services de police !

CHECKDOC



Il s'agit d'un site Internet de **vérification des documents d'identité belges** (passeport, carte d'identité, titre de séjour à puce).

Le site **www.checkdoc.be** permet de vérifier gratuitement et en temps réel partout dans le monde si un document d'identité belge a réellement été émis et s'il n'est pas connu des autorités publiques comme document volé, perdu, périmé, non valide. L'utilisateur peut être une société de location de voitures, une banque, un hôtel, un notaire, un commerçant.

www.checkdoc.be est un moteur de recherche effectuant une recherche dans le registre national et la banque de données relative aux passeports sur la base du numéro d'identification du document présenté. En l'espace de quelques secondes, l'utilisateur obtient une réponse sous la forme de « HIT » ou « NO HIT ». Il peut ainsi prendre une décision en connaissance de cause.

L'utilisation de Checkdoc.be est très simple ! La première fois, vous devez remplir un formulaire d'inscription et accepter les conditions d'utilisation du site. Vous recevez ensuite un code d'activation à l'adresse e-mail qui est indiquée dans le formulaire et qui constitue votre nom d'utilisateur.

Pour effectuer une vérification sur **www.checkdoc.be**, vous devez vous identifier (login), puis sélectionner l'un des deux modes suivants : un mode « basique » didactique et un mode « expert » rapide.

- Dans le mode « basique » : vous êtes aidé dans le choix du document par des photos indiquant l'emplacement du numéro que vous devez introduire. ►►

- ▶ • Le mode « expert » vous donne une réponse en 2 clics.

HIT / NO HIT

- **HIT** : lorsque le document faisant l'objet de la requête de vérification est connu par les autorités administratives belges comme volé, perdu, périmé ou non valide ou lorsqu'un document portant ce numéro n'a pas été émis par ces autorités. Vous ne recevez pas d'information sur la raison de ce « HIT » ;
- **NO HIT** : lorsque le document faisant l'objet de la requête de vérification a bien été émis par une autorité administrative belge et n'est pas connu comme volé, perdu, périmé ou non valide.

Soyez vigilants et détectez les faux documents ! Checkdoc.be vous donne aussi des conseils pratiques concernant la vérification des éléments de sécurité des documents d'identité belges.

DOC STOP



DOC STOP est un helpdesk permettant à tout titulaire d'un document d'identité belge de **signaler la perte ou le vol** de son document d'identité ou de voyage partout dans le monde 24 heures sur 24. Pour ce faire, il peut appeler le numéro gratuit 00800 2123 2123 (dans les pays



où le numéro d'appel 00800 n'est pas disponible, il convient de composer le numéro +32 2 518 2123).

Dans un premier temps, l'identité de l'appelant est vérifiée afin de s'assurer qu'il s'agit réellement du titulaire du document. L'opérateur bloque ensuite immédiatement les documents. Dès cet instant, toute vérification sur le site www.checkdoc.be débouchera sur un « HIT », sans que l'on doive attendre que le titulaire introduise une demande de renouvellement du document d'identité. Les citoyens peuvent ainsi éviter d'être victimes d'une utilisation frauduleuse de leurs documents d'identité (en vue, par exemple, de la location d'une voiture, d'un achat par la poste, d'un emprunt à leur nom, ...).

DOC STOP est un service gratuit, joignable 7j/7, 24h/24.

Important : DOC STOP permet uniquement de bloquer des documents d'identité belges.



Vol ou perte : que faire ?

- En cas de vol. Appelez immédiatement DOC STOP. Faites également une déclaration de vol au bureau de police le plus proche ou auprès de votre police locale.
- En cas de perte. Appelez immédiatement DOC STOP. Rendez-vous ensuite à votre administration communale. En dehors des heures d'ouverture, vous pouvez vous adresser à la police en vue d'une attestation provisoire.

Important : si le document perdu est un titre de séjour, il faut toujours faire une déclaration de perte auprès de la police avant de se rendre à l'administration communale.

Que se passe-t-il à l'issue de votre appel ?

- Cartes d'identité et titres de séjour. Vous recevez un courrier confirmant le signalement du document perdu ou volé. Si vous retrouvez votre document, vous disposez d'un délai de 7 jours, à

compter de votre appel, pour le débloquent. Passé ce délai, le document d'identité est déclaré non valide. Vous devez alors faire une demande de renouvellement auprès de votre administration communale.

Si le document perdu est un titre de séjour, il faut toujours faire une déclaration de perte auprès de la police avant de se rendre à l'administration communale.

- Passeports. Votre passeport est déclaré non valide dès le moment où vous appelez DOC STOP. Si vous devez voyager, demandez-en un nouveau en temps utile auprès de votre administration communale. ●

CHECKLIST

Appel téléphonique d'alerte à la bombe/extorsion

Date et heure de l'appel		Heure de la fin de l'appel				
Contenu du signalement						
Indication de l'endroit		Si oui, où ?				
Indication de l'heure		Si oui, laquelle ?				
Aspect	Petit paquet <input type="checkbox"/>	Véhicule <input type="checkbox"/>	Non mentionné <input type="checkbox"/>	Autre		
Type	Bombe <input type="checkbox"/>	Engin explosif <input type="checkbox"/>	Non mentionné <input type="checkbox"/>	Autre		
Raison						
Identité	Homme <input type="checkbox"/>	Femme <input type="checkbox"/>	Enfant <input type="checkbox"/>	Adulte <input type="checkbox"/>	Age possible	
Voix	Douce <input type="checkbox"/>	Dure <input type="checkbox"/>	Aiguë <input type="checkbox"/>	Grave <input type="checkbox"/>	Brusque <input type="checkbox"/>	lvre <input type="checkbox"/>

Accent	Local <input type="checkbox"/>	Régional <input type="checkbox"/>	Étranger <input type="checkbox"/>	Autre <input type="checkbox"/>
Élocution	Rapide <input type="checkbox"/>	Lente <input type="checkbox"/>	Claire <input type="checkbox"/>	Déformée <input type="checkbox"/>
	Balbutiement <input type="checkbox"/>	Nasillarde <input type="checkbox"/>	Bredouillement <input type="checkbox"/>	Murmurée <input type="checkbox"/>
Langage	Bon <input type="checkbox"/>	Moyen <input type="checkbox"/>	Mauvais <input type="checkbox"/>	

Comportement	Calme <input type="checkbox"/>	Excité <input type="checkbox"/>	Pressé <input type="checkbox"/>	Joyeux <input type="checkbox"/>	Ivre <input type="checkbox"/>
---------------------	--------------------------------	---------------------------------	---------------------------------	---------------------------------	-------------------------------

Bruits de fond	Machines <input type="checkbox"/>	Voitures <input type="checkbox"/>	Trains <input type="checkbox"/>	Animaux <input type="checkbox"/>
	Bruits de rue <input type="checkbox"/>	Ambiance de fête <input type="checkbox"/>	Avion <input type="checkbox"/>	Musique <input type="checkbox"/>

Infos complémentaires	
------------------------------	--

Personne ayant reçu le message	
---------------------------------------	--

La conversation a-t-elle été enregistrée ?	
---	--

Conseils et idées pour mieux protéger son entreprise

“MIEUX VAUT PRÉVENIR QUE GUÉRIR !”

La criminalité est un phénomène auquel n'échappent malheureusement pas les entreprises belges. Négliger les risques criminels peut entraîner pour elles de sérieux dommages. C'est dans ce contexte que la Fédération des Entreprises de Belgique (FEB) – en collaboration avec la Police judiciaire fédérale – a rédigé une brochure afin de vous sensibiliser aux mesures de prévention. Parallèlement à une approche générale des problèmes spécifiques de protection, la présente brochure contient une série de conseils et d'idées pratiques susceptibles de contribuer à une protection accrue de votre entreprise.



FEB ASBL

Rue Ravenstein 4
B-1000 Bruxelles
T + 32 2 515 08 11
F + 32 2 515 09 99
info@vbo-feb.be
www.feb.be