Baromètre de la Sécurité pour les entreprises : une étude exploratoire sur la sûreté dans les entreprises et la victimisation

Etude n° 1

Auteurs : Dormaels Arne & Verwee Isabel

Éditeur responsable : Karin Genoe

Éditeur : Institut Vias – Security and Innovation

Cette étude a été rendue possible grâce à la collaboration avec la FEB, UNIZO, Unisoc, Agrofront, UCM et UWE.

Contenu

Table des matières

Liste des figures et tableaux

1. Résumé

L'institut Vias a lancé le baromètre de la Sécurité : une étude exploratoire visant à savoir dans quelle mesure la sécurité et la sûreté font partie des priorités des entreprises et comment elles luttent contre la criminalité. 273 entreprises néerlandophones et francophones issues de secteurs divers ont été interrogées à ce propos entre juillet et octobre 2018.

Bien préparées ?

Il est frappant de constater que peu ou pas de contrôles au niveau de la sûreté sont organisés dans près de la moitié des entreprises interrogées. 43,4% ont affirmé qu'il n'existait pas de politique visant à lutter contre la criminalité dans l'entreprise, 19,87% ont indiqué qu'aucune mesure de sûreté n'avait été prise et 37,66% des personnes interrogées n'avaient pas le sentiment que leur entreprise était suffisamment préparée à d'éventuels incidents en matière de sécurité.

67,07% des entreprises ont signalé avoir investi dans un ou plusieurs systèmes destinés à améliorer la sûreté physique ou organisationnelle. Les investissements les plus fréquents sont les serrures, la surveillance caméra et les systèmes d'alarme. Dans 28,99% des entreprises, un screening méticuleux est réalisé à l'embauche de nouveaux collaborateurs.

Cybercriminalité comme risque

À la question de savoir à quels risques majeurs leur entreprise était exposée, les répondants ont principalement indiqué différentes sources de cybercriminalité. Mais un tiers des entreprises ont jugé qu'il était « (tout à fait) probable » qu'elles soient victimes au cours de l'année à venir d'hacking ou de phishing par exemple. « L'ingérence dans les données ou les systèmes via des virus, cryptoware ou attaques DDoS » (27,23%) et fraude sur Internet (20,56%) faisaient également partie du top cinq.

Même les entreprises qui jugent peu probable qu'elles soient victimes de cybercriminalité durant la prochaine année accordent de l'importance à la sûreté IT. 93,84% des répondants ont indiqué que la sûreté IT était primordiale. La plupart des entreprises appliquent quelques règles de base. 96,48% effectuent régulièrement des back-ups de leurs données, 92,96% mettent toujours à jour les systèmes d'administration et 92,96% sécurisent l'accès au wifi. 72,6% ont une politique de sûreté spécifique au niveau de l'IT.

La situation reste toutefois perfectible. 23,94% des entreprises ne disposaient ainsi pas de politique en matière de mots de passe. Dans 44,52% des entreprises, il n'y avait pas de formations régulières sur la sûreté IT ou les menaces actuelles et 24,65% ne sensibilisaient pas leur personnel aux menaces IT les plus fréquentes.

Tout est question d'image ?

Lorsque les entreprises investissent dans la sécurité, elles le font essentiellement pour protéger des personnes (collaborateurs et/ou clients par exemple). Pour 38,46% des entreprises, il s'agissait de la raison principale. Les autres raisons avancées sont la protection de l'infrastructure (18,27%), de l'information (15,39%) et des produits ou services de l'entreprise (13,46%). Seul 1,92% des entreprises ont désigné la protection de l'image comme raison principale.

78,08% des répondants ont indiqué que la sécurité dans l'entreprise était la responsabilité de l'employeur. 67,81% ont affirmé que chaque travailleur individuel dans l'entreprise était responsable de la sécurité.

Actes criminels sur le lieu de travail : ce n'est pas une plaisanterie

Il a été demandé aux entreprises qui indiquaient ne prendre aucune mesure de sécurité pour quelles raisons elles ne le faisaient pas. Près de la moitié d'entre elles (48,84%) déclaraient que « le risque d'être victime est faible ». Ce baromètre démontre néanmoins que le risque d'être victime d'actes criminels en tant qu'entreprise est bien réel. 42,6% des entreprises participantes ont été victimes d'une ou de plusieurs formes de cybercriminalité au cours des 12 derniers mois précédent l'étude. Il s'agit là d'un chiffre élevé, tout en sachant que les cybercriminels s'en sont pris à bien plus d'entreprises. La détérioration d'un véhicule (41,91%), la violence et l'agression (39,71%), la détérioration de propriété ou vandalisme (39,71%) et l'accès interdit sans violence (38,24%) étaient également des actes criminels fréquemment cités.

Plainte ou problème résolu personnellement ?

Dans la dernière partie du baromètre, il était question d'en savoir plus sur « fait le plus marquant » vécu par les entreprises ayant été victimes d'au moins un acte criminel au cours de l'année écoulée. Les victimes désignaient « la violence et l'agression » (19,3%), « la cybercriminalité : l'accès illégal aux systèmes IT « (8,77%) et « l'accès interdit sans violence » (7,9%) comme fait le plus marquant. Il est à noter que plus d'un quart des entreprises (28,32%) n'ont pas porté plainte à la police. « Parce que cela ne donne de toute façon aucun résultat » et « parce que l'on ne peut de toute façon rien y faire » selon respectivement 28,13% et 12,5% de ces entreprises. 15,63% n'ont pas porté plainte « parce qu'elles connaissaient l'auteur » et 12,5% « parce qu'elles trouvaient que l'affaire n'était pas assez grave ».

De nouveau plus d'un quart (28,83%) des entreprises victimes d'un acte criminel, ont indiqué avoir tenté de le résoudre elles-mêmes, par exemple en recherchant personnellement l'auteur et/ou en s'adressant directement à lui, en réglant l'affaire à l'amiable… Dans la majorité des cas, cette opération a coûté à l'entreprise moins d'un jour de travail et moins de 5.000 euros.

Travailleur criminel

Le baromètre de la sécurité montre que les entreprises victimes d'un acte criminel connaissaient son auteur dans 28,32% des cas. Dans plus d'un tiers des cas, il s'agissait d'un travailleur de l'entreprise ou d'un contractant.

Points de contact internes et personnes de confiance

Dans 36,80% des entreprises, il n'existait, au moment de l'étude, aucune procédure pour signaler les agissements suspects sur le lieu de travail et en dehors. Dans 45,60% des entreprises, il n'existait pas de point de contact anonyme. C'était souvent le cas dans les entreprises plus petites. La question est donc de savoir si les travailleurs de ces organisations savent bien à qui s'adresser s'ils sont victimes ou témoins d'un acte criminel sur le lieu de travail.

Concernant les suites réservées à un acte criminel, il n'est pas toujours évident de savoir où les travailleurs peuvent se rendre pour poser leurs questions ou faire part de leurs inquiétudes. 24,80% des entreprises participantes ont indiqué qu'il n'y avait pas de personne de confiance vers qui les travailleurs pouvaient se tourner pour leur parler de leur mésaventure. 15,20% ont indiqué qu'aucune aide psychosociale (interne ou externe) n'était proposées aux travailleurs victimes de criminalité.

2. Contexte

La sécurité constitue plus que jamais un aspect majeur de notre société et du monde de l'entreprise. L'institut Vias lance un baromètre visant à savoir dans quelle mesure la sécurité et la sûreté font partie des priorités des entreprises et comment elles luttent contre la criminalité. Il est capital que ce baromètre nous en apprenne plus sur le sujet pour nous faire une idée réaliste de la place qu'occupe la sécurité dans les entreprises et de la façon dont elles se protègent contre d'éventuels actes criminels. Pour obtenir ces informations, nous avons fait appel à la collaboration d'organisations représentant le secteur de l'entreprise.

Cette étude veut déboucher sur une culture de la sécurité dans tous les secteurs de la société belge. Les instances publiques, les entreprises, les organisations, les citoyens, tous doivent être conscients des opportunités et des menaces que représente la société actuelle. Il importe d'œuvrer à une société capable de se défendre dans laquelle les entreprises, les organisations et les citoyens sont en mesure de lutter contre les menaces et risques potentiels.

Le baromètre de la sécurité pour les entreprises a été créé en collaboration avec des partenaires divers et comprend différents modules. Il s'agit d'un baromètre analysant dans quelle mesure les entreprises et les PME accordent de l'importance à la sécurité et comment elles luttent contre la criminalité. Ce questionnaire ne traite donc pas de la sécurité alimentaire ni de la sécurité au travail ni de la sécurité incendie mais de la sécurité face aux actes criminels. Le baromètre aborde plusieurs thèmes tels que l'attention générale pour la sûreté, l'évaluation du risque, la culture et la politique de sécurité, la sûreté IT et physique et la victimisation.

Le questionnaire a été programmé en key survey en intégrant autant de catégories de réponse préprogrammées que possible, ce qui a facilité l'analyse des résultats. Les partenaires ont testé l'application et communiqué leurs remarques. Il a été tenu compte un maximum de ces remarques pour ensuite lancer le baromètre de la sécurité à l'été 2018.

Entre juillet et octobre 2018, les entreprises ont été invitées à prendre part au baromètre de la sécurité. Une fois les réponses traitées anonymement et globalement, nous avons analysé les résultats avec les organisations partenaires à l'occasion d'une session de travail interactive (SI) au cours de laquelle le but était d'une part de se pencher sur la signification des résultats pour le monde de l'entreprise. La session en question a également permis de discuter de ce que nous allons faire des résultats obtenus, d'avoir un aperçu des chiffres et de contextualiser les résultats.

Les résultats issus dudit questionnaire seront décrits dans ce rapport. Il sera ensuite question de considérations, réflexions et contextualisation des participants à la SI (les partenaires sont indiqués ci-après). Enfin, plusieurs recommandations seront formulées.

Cette étude a été rendue possible grâce à la collaboration d'organisations et de partenaires divers représentant le monde de l'entreprise. Nous tenons à remercier formellement les partenaires suivants : les fédérations de la FEB, Unizo, Unisoc, Agrofront, l'Union des classes moyennes (UCM) et l'Union Wallonne des Entreprises (UWE).

3. Résultats d'étude

3.1 Taux de réponse et caractéristiques de base des entreprises

273 répondants ont pris part à ce baromètre, parmi lesquels 79,5% ont complété le questionnaire en néerlandais et 20,5% en français.

89,97% des répondants ont indiqué que le cœur de leurs activités se trouvait en Belgique. 10,04% ont donc répondu que la plupart de leurs activités économiques étaient effectuées à l'étranger. Les provinces belges les plus citées sont la Flandre-Orientale, Anvers, la Région de Bruxelles-Capitale et la Flandre-Occidentale.

De nombreuses petites entreprises voire des entreprises de taille moyenne ont participé à cette étude. À la question « Combien de collaborateurs travaillent dans votre entreprise ? », nous obtenons les pourcentages suivants :

- 34,43% entre 0 – 10 collaborateurs
- 17,22% entre 11 – 50 collaborateurs
- 19,41% entre 51 - 250 collaborateurs
- 10,26% entre 251 – 500 collaborateurs
- 7,33% entre 501 – 1000 collaborateurs
- 11,36% plus de 1001 collaborateurs

À la question de savoir si la personne interrogée occupe une fonction dirigeante, 77,29% ont indiqué que c'était le cas. 22,71% n'occupaient dès lors pas de fonction dirigeante.

Le secteur dont fait partie l'entreprise était :

- 16,35% transport et entreposage
- 15,97% santé humaine et action sociale
- 13,69% agriculture, sylviculture et pêche
- 11,03% industrie extractive
- 8,75% « autre »
- 7,99% industrie alimentaire
- 6,46% activités financières et d'assurances
- 6,84% industrie
- …

3.2 Les travailleurs accordent moins d'attention à la sûreté dans une entreprise que les employeurs

	Pas du tout d'accord					Tout à fait d'accord	Ne sait pas/pas de réponse
Notre entreprise accorde de l'attention à la sûreté	2,90%	1,45%	5,31%	9,18%	24,16%	54,59%	2,42%
Notre direction accorde de l'attention à la sûreté	2,90%	2,42%	5,31%	10,15%	22,22%	55,07%	1,93%
Nos collaborateurs accordent de l'attention à la sûreté	3,38%	5,80%	6,76%	20,77%	30,92%	29,47%	2,90%
Des activités de conscientisation sont organisées dans notre entreprise dans le cadre de la sûreté	8,21%	12,08%	9,18%	13,53%	22,71%	29,47%	4,83%
Un test ou un contrôle est régulièrement organisé dans notre entreprise	18,84%	16,91%	11,59%	15,46%	14,49%	18,36%	4,35%

Tableau 1: Attention générale à la sécurité dans une entreprise (N=207)

Il a été demandé aux répondants d'indiquer sur une échelle de 1 (pas du tout d'accord) à 6 (tout à fait d'accord) dans quelle mesure ils sont d'accord avec les affirmations susmentionnées. Premier résultat interpellant : 55,07% des répondants étaient « tout à fait d'accord » avec l'affirmation « Notre direction accorde de l'attention à la sûreté » et quasiment autant de répondants (à savoir 54,59%) étaient d'accord avec l'affirmation « Notre entreprise accorde de l'attention à la sûreté ». Ces chiffres entrent en contradiction avec les 29,47% de répondants qui ont indiqué être « tout à fait d'accord » avec l'affirmation « Nos collaborateurs accordent de l'attention à la sûreté ». Ce résultat est nettement inférieur aux résultats obtenus pour « notre entreprise » et « notre direction ».

Un autre constat frappant était que les répondants ont le plus souvent répondu « pas du tout d'accord » et « plutôt pas d'accord » aux affirmations suivantes : « Un test ou un contrôle au niveau de la sûreté est régulièrement organisé dans notre entreprise » et « des activités de sensibilisation sont organisées dans notre entreprise dans le cadre de la sûreté ».

L'employeur est le plus fréquemment cité comme responsable de la sûreté de l'entreprise et de la prise de mesures visant à garantir la sécurité de l'entreprise. Ce qui est souvent oublié, c'est que le travailleur joue un rôle tout aussi important dans la sûreté de l'entreprise, en choisissant scrupuleusement ses mots de passe et en installant ses mises à jour. Les instances fédérales précisent ainsi que de nombreux incidents pourraient être évités si les travailleurs étaient conscients de l'importance de la cybersécurité (Service Public Fédéral, 2017).

3.3 Cybercriminalité comme risque

Le questionnaire comportait plusieurs questions spécifiques relatives à la sécurité. Il a ainsi été demandé dans quelle mesure l'entreprise pourrait être victime de certaines formes de criminalité au cours des 12 mois à venir. Certains faits ont été qualifiés de très probables, d'autres comme moins probables.

Voici le top 5 des faits dont on a estimé qu'il était « pas du tout probable » ou « pas probable » d'en être victime.

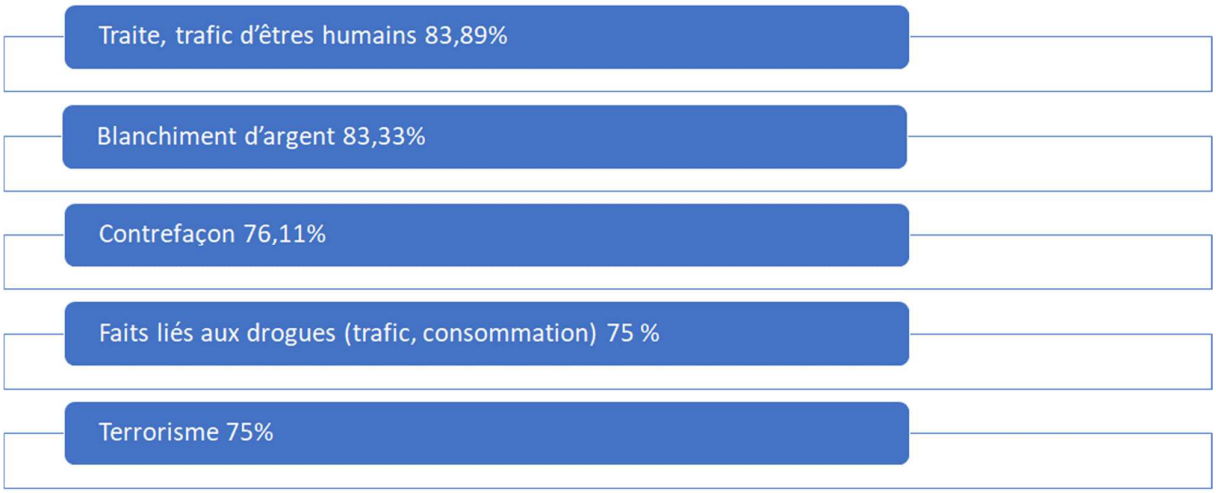

Figure 1: « Pas du tout probable », « pas probable » d'être victime de… au cours des 12 prochains mois (N = 180)

La figure 1 montre que les faits « traite, trafic d'êtres humains » et « blanchiment d'argent » sont perçus comme les moins à risque par les entreprises interrogées. L'une des explications possibles se situe dans la prévalence de ces formes de criminalité. Nous notons ainsi que le nombre de plaintes pour traite d'êtres humains est en baisse ces dernières années (police fédérale, 2018 ; AD, 2019). On ignore si c'est la conséquence d'une baisse effective de cet acte criminel ou s'il s'agit plutôt d'une baisse du nombre de plaintes mais cela peut veiller à faire moins attention à ces pratiques, ce qui peut constituer une explication à la faible évaluation du risque. Ce lien n'apparaît pas pour les faits liés aux drogues et au terrorisme. Selon Belga, la production de cannabis et de drogues synthétiques est en hausse en Belgique (Belga, 2018) et d'après le parlement européen, les menaces terroristes et les attentats djihadistes sont en augmentation (parlement européen, 2018).

L'acte criminel considéré comme le plus probable de survenir (cela va de « probable » à « tout à fait probable ») est la cybercriminalité. 34,4% des entreprises ont désigné qu'il était « très probable » ou « probable » qu'elles soient victimes d'une forme de cybercriminalité au cours des 12 mois à venir.

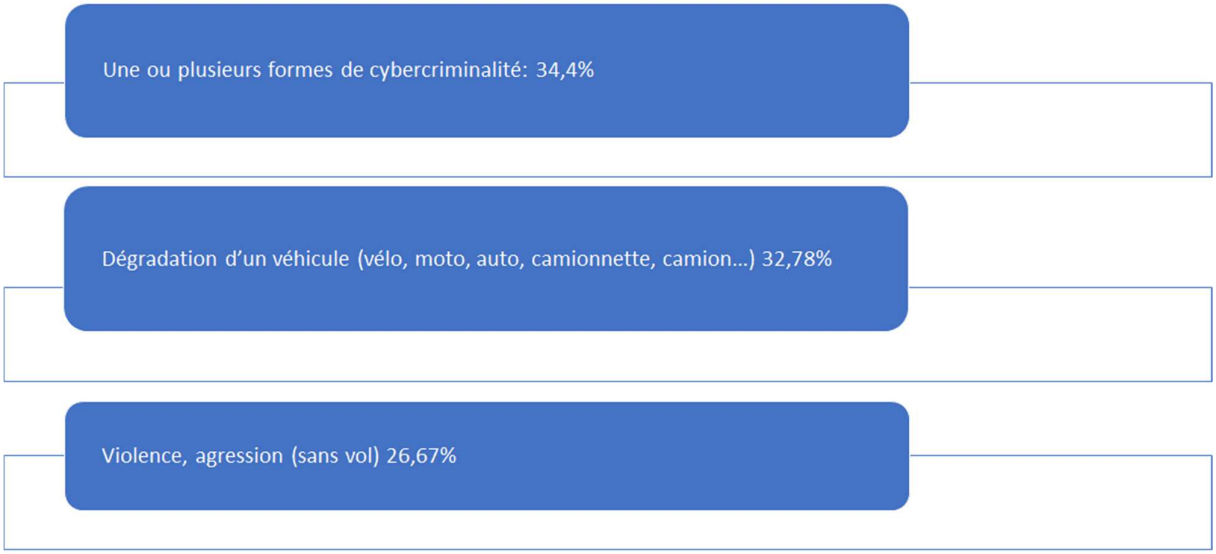

Figure 2 : « Tout à fait probable », « probable » d'être victime de… au cours des 12 prochains mois (N=180)

Le tableau suivant montre pour chaque forme de cybercriminalité, le degré de probabilité d'en être victime.

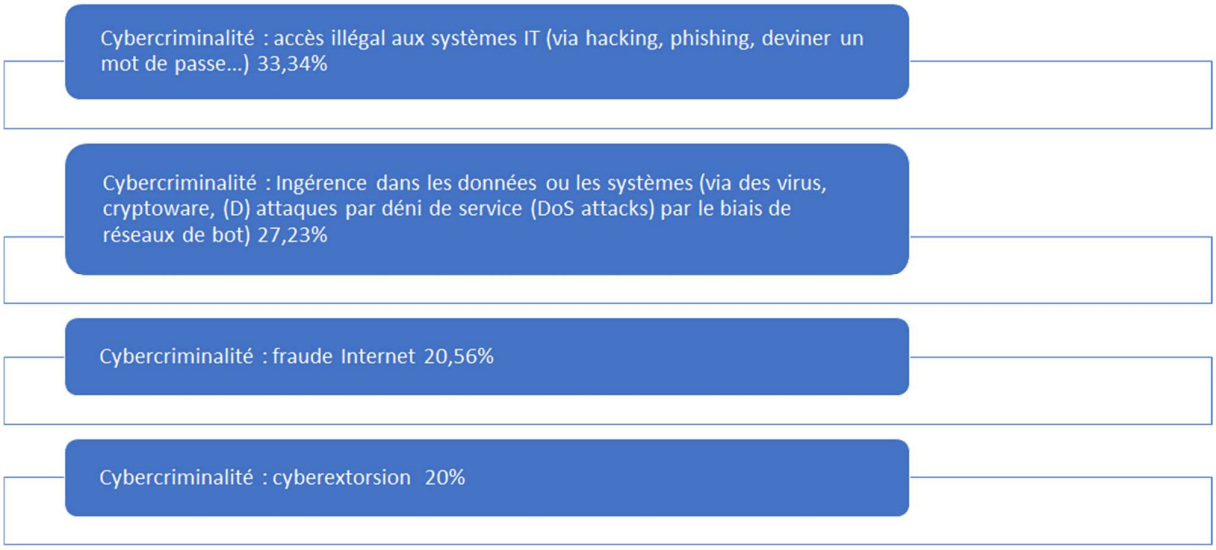

Figure 3 : « Tout à fait probable », « probable » d'être victime d'une forme de cybercriminalité au cours des 12 prochains mois (N=180)

La Figure 2 nous apprend que la cybercriminalité est considérée comme un risque réel : plus d'un tiers des répondants ont indiqué qu'elle représentait un risque. Etant donné qu'il existe de multiples formes de cybercriminalité, le répondant a été soumis à diverses formes. La cybercriminalité causée par des accès illégaux a été perçue comme celle comportant le plus de risques. La deuxième plus grande cybermenace concernait l'ingérence dans les données ou systèmes via des virus, cryptoware ou des attaques DOS (D) par le biais de réseaux de bots. Quelque 20% des entreprises interrogées ont indiqué qu'elles considéraient la fraude sur Internet et la cyberextorsion comme un risque réel dans les 12 mois à venir.

Cette évaluation du risque a également été abordée dans le Global Risk Report. La croissance de la cybercriminalité s'exprime tant dans la prévalence que dans son potentiel disruptif : "*Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace*". Les coûts les plus importants de 2017 étaient dus aux attaques par rançongiciels, dont 64% concernaient des e-mails malveillants. Une autre tendance en hausse est le recours aux cyberattaques contre des infrastructures critiques et des secteurs industriels stratégiques dans le but d'instiguer une certaine peur et de creuser, dans le pire des cas, une faille dans ce qui fait tourner la société (World Economic Forum, 2018).

Dans la Global Risk Perception Survey (2018), 7% des répondants ont indiqué que le nombre de risque était en baisse. Il y a quatre sources d'inquiétude : 1) inégalité et injustice persistantes, 2) tensions politiques nationales et internationales, 3) changements environnementaux et 4) les cybervulnérabilités.

Contrairement à 2017, où l'on se souciait peu des risques informatiques, cyberattaques et la fraude massive de données faisaient partie en 2018 du top 5 des formes de criminalité dont la probabilité d'en être victime est élevée.

Les intrusions informatiques (cyber-effraction) enregistrées par les entreprises ont doublé en l'espace de 5 ans : leur nombre est passé de 68 par entreprise en 2012 à 130 par entreprise en 2017 (World Economic Forum, 2018). Les cybercriminels disposent d'un nombre exponentiel de cibles potentielles vu la hausse de l'utilisation des services de cloud et *the Internet of Things* s'attend à ce que cette hausse se poursuive dans les années à venir. Ce que l'on considérait avant comme des cyberattaques à petite échelle sont désormais qualifiées d'attaques ordinaires. Les assaillants sont davantage persistants et le coût financier grimpe. Il est référé au coût financier de la WannaCry attack. Outre le coût financier, cette attaque s'en prend aussi aux infrastructures critiques et stratégiques : "*the WannaCry attack disrupted critical and strategic infrastructure across the world, including government, ministries, railways, banks, telecommunications providers, energy companies, car manufacturers and hospitals*" (Global Risk Perception Survey, 2018).

Plusieurs attaques perpétrées dans des systèmes critiques et stratégiques ne sont pas parvenues à leur fin mais la combinaison des succès isolés et une liste croissante de tentatives d'attaques montrent que les risques

connaissent aussi une hausse. La croissance de l'interconnectivité mondiale veille à ce que les tentatives, quand elles aboutissent, causent des dégâts systématiques radicaux et irréversibles.

L'Aons' Global Risk Management Survey de 2017 a été conçue pour aider les organisations à mieux comprendre "*to compete in this increasingly complex operation environment*". 1843 décideurs issus de petites, moyennes et grandes entreprises publiques et privées dans 33 secteurs industriels répartis dans 60 pays ont été interrogés sur la question.

Les résultats montrent que les entreprises doivent faire faire face à une foule de nouveaux risques, et qu'il n'y a pas de consensus sur l'ordre de priorité du traitement de ces risques ni sur la façon d'y réagir. Ici aussi, nous remarquons que les cyber-risques occupent le top 5 alors que les risques/incertitudes politiques faisaient partie du top 10. Le lien entre les risques/incertitudes politiques et la cybercriminalité est accentué par de nombreux événement survenus en 2016 tels qu'une augmentation de la cybercriminalité, ce qui a eu un impact direct sur les institutions gouvernementales, les partis politiques et les infrastructures globales.

L'on constate une différence au niveau de l'estimation du risque selon la taille de l'entreprise. Les entreprises plus grandes désigneront plus vite la cybercriminalité/les virus/les codes malveillants comme des risques en comparaison des entreprises de plus petite taille (Aons' Global Risk Management Survey, 2017).

Nous retrouvons une évaluation du risque analogue dans le baromètre Allianz Risk de 2018 (établi sur la base de réflexions émanant de 1911 experts en matière de risques issus de 80 pays différents). L'interruption de travail a été désignée comme première inquiétude à l'avenir et les incidents liés à la cybersécurité comme deuxième préoccupation future (Baromètre Allianz Risk, 2018).

Hormis la cybercriminalité, deux autres formes de criminalité ont été avancées dans ce baromètre de la sécurité, à savoir la détérioration d'un véhicule (voiture, moto, vélo) et la violence et l'agression (sans vol). L'on estime également que l'entreprise ou un collaborateur en sera victime au cours des 12 mois à venir.

En croisant dans notre étude l'évaluation du risque avec la question « Combien de collaborateurs travaillent dans votre entreprise ? », nous avons observé quelques liens statistiquement significatifs[1]. Nous avons relevé un lien modéré entre la violence, l'agression (sans vol) et le terrorisme. Les répondants qui travaillent dans des entreprises de plus petite taille (plus précisément des entreprises qui comptent moins de 250 collaborateurs) ont jugé plus souvent qu'il était « pas du tout probable », « pas probable » ou « plutôt pas probable » d'être victimes de violence et d'agression (sans vol). Pour ce qui est du « terrorisme », nous avons également relevé que les entreprises de plus petite taille indiquaient plus fréquemment « pas du tout probable » et « pas probable, alors que les entreprises plus importantes ont davantage nuancé leurs réponses en indiquant « pas probable » et « plutôt pas probable ».

3.4 Culture de la sécurité, gestion et politique en matière de sûreté dans votre entreprise

3.4.1 **Connaître et mettre en œuvre une politique de sécurité**

Le troisième thème abordé dans le baromètre était la culture de la sécurité, la gestion et la politique en matière de sûreté dans les entreprises. 73,91% des répondants ont indiqué avoir connaissance de prescriptions et de dispositions légales relatives à la sûreté dans leur entreprise. 26,09% n'en savent rien.

À la question de savoir s'ils ont connaissance des modifications au niveau des prescriptions et des dispositions légales relatives à la sûreté dans leur entreprise, 68,94% ont répondu « oui » et 31,06% « non ». En outre,

[1] Le croisement de variables permet de vérifier s'il y a un lien entre elles deux. Nous examinons si le lien est statistiquement significatif et si tel est le cas, le degré d'association est analysé. Dans le cadre d'une étude sociologique/criminologique, l'on utilise généralement la pertinence d'un lien :

- Très faible/pas de lien : 0 - .10
- Lien faible : .11- .30
- Lien modéré : .31 - .50
- Lien fort : .51 - .80
- Lien très fort : .81 - .99
- Parfaitement lié : 1

56,6% des répondants ont indiqué qu'il existait une politique de sûreté contre la criminalité et 43,4% ont répondu que ce n'était pas le cas.

Pour savoir s'il existe un lien significatif entre la présence d'une politique de sûreté contre la criminalité et le nombre de travailleurs dans une entreprise, ces deux affirmations ont été croisées. Ce croisement a débouché sur un lien modérément significatif. Plusieurs répondants travaillant pour une petite entreprise ont répondu « non » à la question de savoir s'il existait une politique de sûreté contre la criminalité au sein de leur entreprise. Ce résultat est confirmé par Techzine (2018). Il est ainsi avancé que les petites et moyennes entreprises connaissent souvent un certain retard sur le plan de la sécurité. Elles fonctionnent souvent avec des budgets plus limités et des connaissances technologiques sommaires (Techzine, 2018).

Les personnes qui ont répondu positivement à la question de savoir s'il existait une politique de sûreté contre la criminalité ont dû répondre à une autre question, à savoir si la politique de sûreté avait été adaptée au cours des 24 derniers mois. La majorité a répondu par l'affirmative.

Une large majorité (78,65%) a également indiqué que cette politique de sécurité était communiquée aux collaborateurs de l'entreprise, seuls 14,61% ont répondu que ce n'était pas le cas. 6,74% ont indiqué « ne sait pas/pas de réponse ».

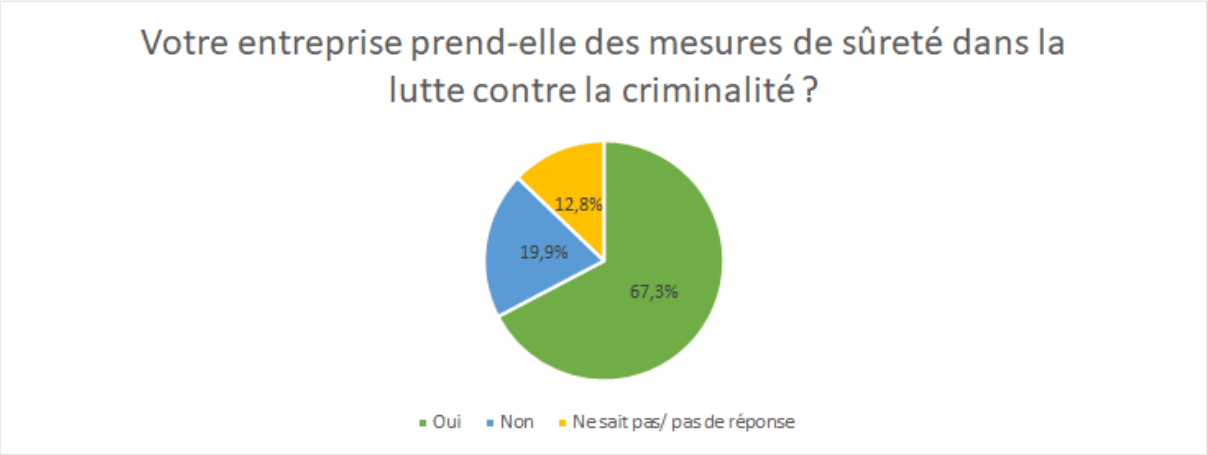

Figure 4 : Votre entreprise prend-elle des mesures de sûreté dans la lutte contre la criminalité ? (N=156)

La figure ci-dessus nous indique que 67,3% des répondants ont répondu positivement à la question de savoir si leur entreprise prenait des mesures de sûreté dans la lutte contre la criminalité. 19,87% ont répondu « non » soit un cinquième des entreprises ont indiqué ne pas avoir pris de mesures à cet égard. Les employeurs sont de plus en plus conscients de l'importance de la sécurité au sein de leur entreprise mais malgré cela, trop peu de mesures sont prises (Belga, 2015). 12,82% ont indiqué « ne sait pas » ou n'ont pas répondu.

Parmi les entreprises qui ont répondu « oui », 75% estimaient qu'il s'agissait de mesures adaptées ou correctes, 5,77% ont affirmé que ce n'était pas le cas et 19,23% ont indiqué « ne sait pas/pas de réponse ».

UNIZO a interrogé 783 membres sur leur politique de sûreté. L'on s'est entre autres penché sur la question de savoir pourquoi l'on n'investissait peu voire rien dans la politique de sécurité. Près de 30% des répondants ont indiqué qu'ils n'étaient pas informés des possibilités qui s'offraient à eux pour se protéger. Un quart des répondants déclarent que ça coûte trop cher. Enfin, 40% affirment que le risque d'être victime est trop faible (UNIZO, 2016).

3.4.2 Investir dans la sécurité = protéger les personnes, l'infrastructure et les informations

La figure ci-dessous indique les principales raisons avancées par les répondants pour investir dans la sécurité en tant qu'entreprise.

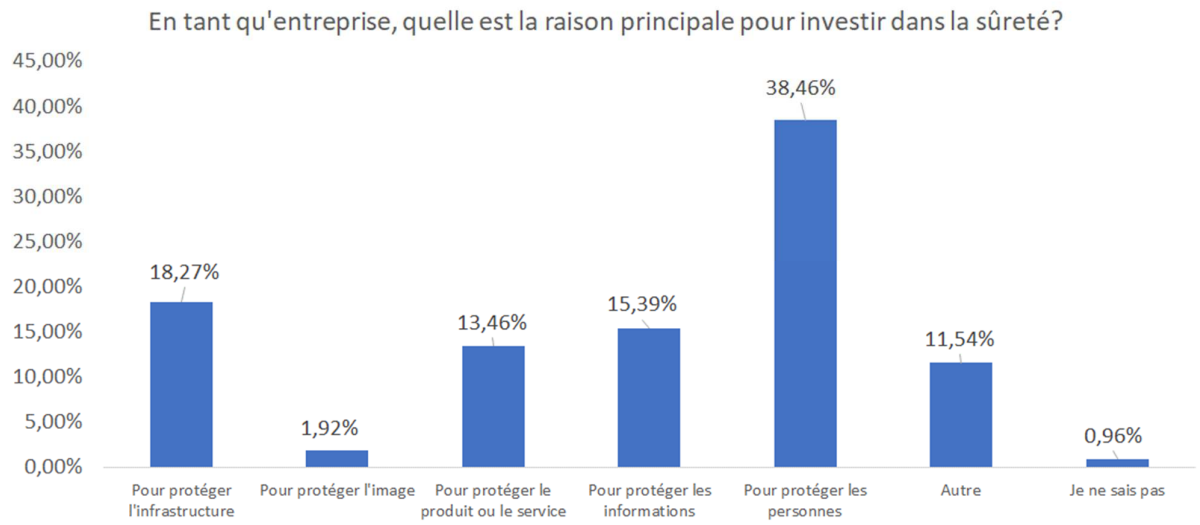

Figure 5 : En tant qu'entreprise, quelle est la raison principale pour investir dans la sécurité ? (N=104)

La principale raison pour investir, en tant qu'entreprise, dans la sécurité est :

1. la protection de personnes
2. la protection de l'infrastructure
3. la protection des informations
4. la protection du produit ou du service

À la question de savoir s'il était possible d'adapter les mesures de sécurité dans l'entreprise en fonction des menaces éventuelles, par exemple après une hausse du niveau de menace de l'OCAM, 61,54% ont répondu positivement. Un cinquième des répondants (20,19%) n'ont pas répondu ou répondu qu'ils ne savaient pas. 18,27% ont répondu « non ».

Les répondants qui ont indiqué que leur entreprise ne prenait pas de mesures de sécurité devaient préciser pourquoi. Près de la moitié de ces répondants – 48,84% - ont indiqué que le « risque d'être victime était trop faible ». 18,61% ont répondu qu'ils n'étaient pas au courant des possibilités qui s'offraient à eux pour se protéger. 13,95% ont indiqué que le coût était trop élevé tandis que 11,63% ont pointé du doigt un manque de temps.

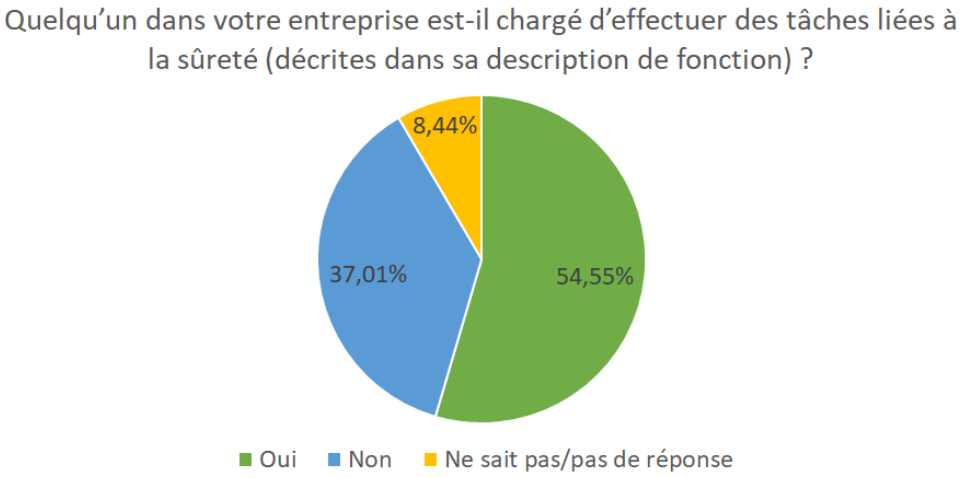

Figure 6 : Quelqu'un dans votre entreprise est-il chargé des tâches liées à la sûreté ? (N=154)

Comme le montre la figure ci-dessous, il a également été demandé aux répondants si certaines personnes étaient chargées de tâches liées à la sûreté. La plupart d'entre eux ont indiqué qu'il y avait dans leur entreprise des personnes chargées de tâches liées à la sûreté, lesquelles étaient reprises dans la description de fonction.

37,01% ont déclaré que ce n'était pas le cas et 8,44% ont indiqué qu'ils ne savaient pas ou n'ont pas donné de réponse.

En croisant cette question avec le nombre de collaborateurs dans une entreprise, nous obtenons un lien significatif : les toutes petites entreprises (0-10 collaborateurs) indiquaient le plus souvent « non » ou « ne sait pas/pas de réponse ».

A la question « Faites-vous appel à une firme externe dans le cadre de la sûreté, par exemple pour vous protéger contre certaines formes de criminalités ?», un peu plus de la moitié des entreprises interrogées ont répondu négativement (52,94%) contre 43,79% qui ont indiqué « oui ». Le reste ne savait pas ou n'a pas répondu. À la question de savoir si les travailleurs étaient au courant des mesures prises par la firme externe, 86,57% ont indiqué qu'ils l'étaient. 71,64% se concertent régulièrement avec cette firme externe et 14,93% ne le font pas régulièrement.

3.4.3 Toutes les entreprises ne sont pas en mesure de détecter les risques liés à la sécurité

	Pas du tout d'accord	Pas d'accord	Plutôt pas d'accord	Plutôt d'accord	D'accord	Tout à fait d'accord	Ne sait pas/pas de réponse
Notre entreprise est en mesure de détecter les risques liés à la sécurité	6,85%	9,59%	17,12%	14,38%	25,34%	22,60%	4,11%
Notre entreprise est prête si des problèmes de sûreté viennent à survenir	8,90%	15,75%	13,01%	15,07%	27,40%	15,75%	4,11%
Il existe un plan d'approche au cas où un problème de sûreté surviendrait	11,64%	15,75%	10,27%	17,12%	26,03%	14,38%	4,80%

Tableau 2 : Pouvez-vous indiquer dans quelle mesure vous êtes d'accord avec... (N=146)

62,32% des répondants étaient « tout à fait d'accord » ou « plutôt d'accord » avec l'affirmation « Notre entreprise est en mesure de détecter les risques liés à la sécurité ». Ceci signifie qu'environ 33% des répondants estiment que l'entreprise n'est pas ou plutôt pas en mesure de détecter les risques liés à la sécurité. Un peu moins de 60% (58,22%) étaient « tout à fait d'accord » ou « plutôt d'accord » avec l'affirmation selon laquelle l'entreprise est prête si des problèmes de sécurité venaient à survenir ». 37,66% n'étaient « pas du tout d'accord » ou « plutôt pas d'accord » avec cette affirmation. Nous avons relevé les mêmes pourcentages pour l'affirmation « Il y a un plan d'approche au cas où un problème de sûreté surviendrait ».

Ces affirmations ont une nouvelle fois été croisées avec la question « Combien de collaborateurs environ travaillent dans l'entreprise ? ». Un lien statistiquement significatif a été établi pour les trois affirmations. Pour les deux premières affirmations, nous avons noté un faible lien en les croisant avec le nombre de collaborateurs. Pour la dernière affirmation « Il y a un plan d'approche au cas où un problème de sûreté surviendrait », nous avons relevé un lien modéré. Les entreprises qui n'étaient « pas du tout d'accord » ou « plutôt pas d'accord » étaient celles de plus petite taille, à savoir celles qui employaient 0 à 10 collaborateurs. Les entreprises de plus grande taille (comptant plus de 251 collaborateurs) ont répondu plus souvent « plutôt d'accord », « d'accord », ou « tout à fait d'accord ».

Enfin, dans le cadre du thème culture de la sécurité, gestion et politique en matière de sûreté dans l'entreprise, l'on a demandé aux répondants quel acteur ou quelle instance est responsable de la lutte contre la criminalité.

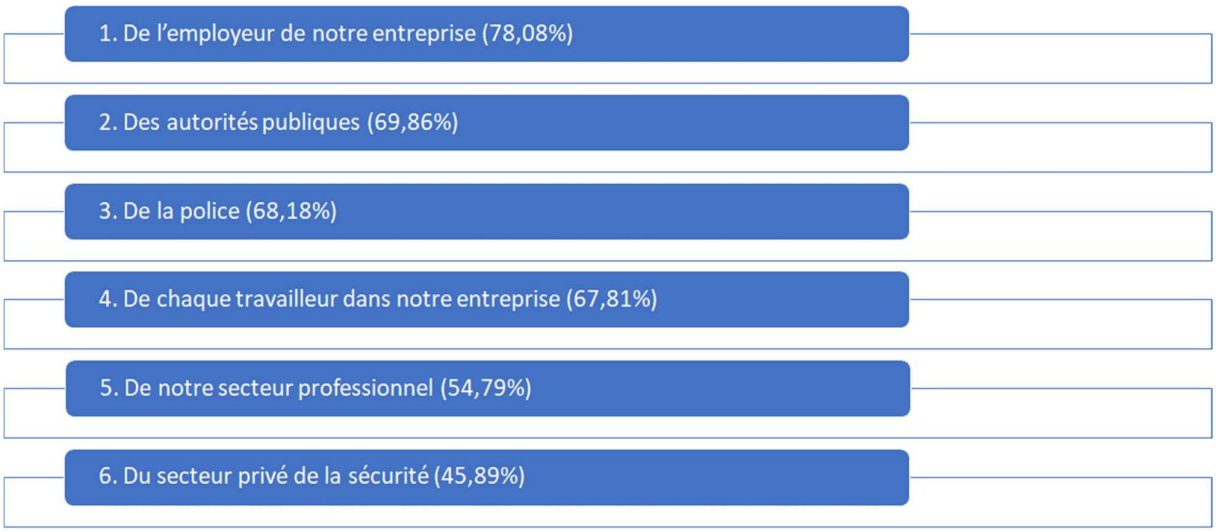

Figure 7 : La sécurité dans la lutte contre la criminalité est une responsabilité de : (N=146)

Le top 6 ci-dessus nous montre que celui que l'on considère comme le principal responsable de la sécurité dans l'entreprise est l'employeur. Viennent ensuite les autorités publiques et la police. La quatrième place est occupée par « chaque travailleur dans notre entreprise ». Le secteur professionnel et le secteur privé de la sécurité viennent clôturer ce top 6. Ces pourcentages se basent sur le pourcentage de répondants ayant répondu être « tout à fait d'accord » ou « d'accord ».

Ces chiffres confirment la conclusion que nous avons tirée précédemment, à savoir que l'employeur est jugé responsable de la sûreté de l'entreprise.

3.5 La sûreté IT est capitale dans une entreprise

À la question de savoir dans quelle mesure la sûreté IT est importante dans l'entreprise, 93,84% des répondants ont indiqué « tout à fait importante » ou « importante ». Les entreprises employant plus de 11 collaborateurs ont indiqué le plus souvent « tout à fait importante ».

82,19% ont signalé que quelqu'un était chargé de la sûreté IT. Le croisement de cette question avec le nombre de collaborateur a livré un lien modérément significatif. Les entreprises de grande taille ont répondu globalement positivement alors que les entreprises comptant 0 à 10 collaborateurs ont le plus souvent indiqué que personne n'était chargé de la sûreté IT dans l'entreprise.

72,6% ont indiqué que l'entreprise disposait d'une politique de sûreté spécifique au niveau de l'IT. Les grandes entreprises ont répondu plus positivement à cette question alors que les entreprises de très petite taille (0-10 collaborateurs) ont répondu le plus souvent négativement.

82,19% ont indiqué qu'il y avait un système de sûreté dans l'entreprise. Les grandes entreprises ont répondu le plus souvent « oui ».

La question « Par rapport à l'année passée, quel était le budget cette année pour la sûreté IT ? » a livré les résultats suivants :

- 26,03% : il est resté le même
- 23,97% : je ne sais rien à propos du budget
- 23,29% : il est un peu plus élevé
- 19,18% : il est beaucoup plus élevé
- 6,16% : j'ignore si le budget a augmenté
- 1,35% : il était inférieur à celui de l'année passée

Un peu plus de la moitié des répondants ont répondu « oui » à la question « Recevez-vous ou d'autres travailleurs dans votre entreprise reçoivent-ils une formation sur la sûreté et les menaces actuelles au niveau IT ». 44,52% ont indiqué que ce n'était pas le cas. Un lien statistiquement significatif avec la taille de l'entreprise a été établi : dans les entreprises de petite taille, peu ont indiqué avoir reçu une formation sur la sûreté et les menaces actuelles au niveau IT.

Dans la société technologique actuelle, il convient d'accroître l'attention et le budget pour la sécurisation IT pour éviter d'être victime d'un acte criminel. De même, les entreprises sont priées de traiter précautionneusement les données. Depuis la modification de la loi relative à la vie privée de 1992 en General Data Protection Regulation (2018), des amendes peuvent être imposées si cette réglementation n'est pas respectée (Hoeffnagel, 2016).

Par la suite, plusieurs questions de sécurisation ont été posées, lesquelles se basent sur plusieurs règles pratiques fixées par le SPF Economie (2017) concernant la sécurisation IT dans une entreprise.

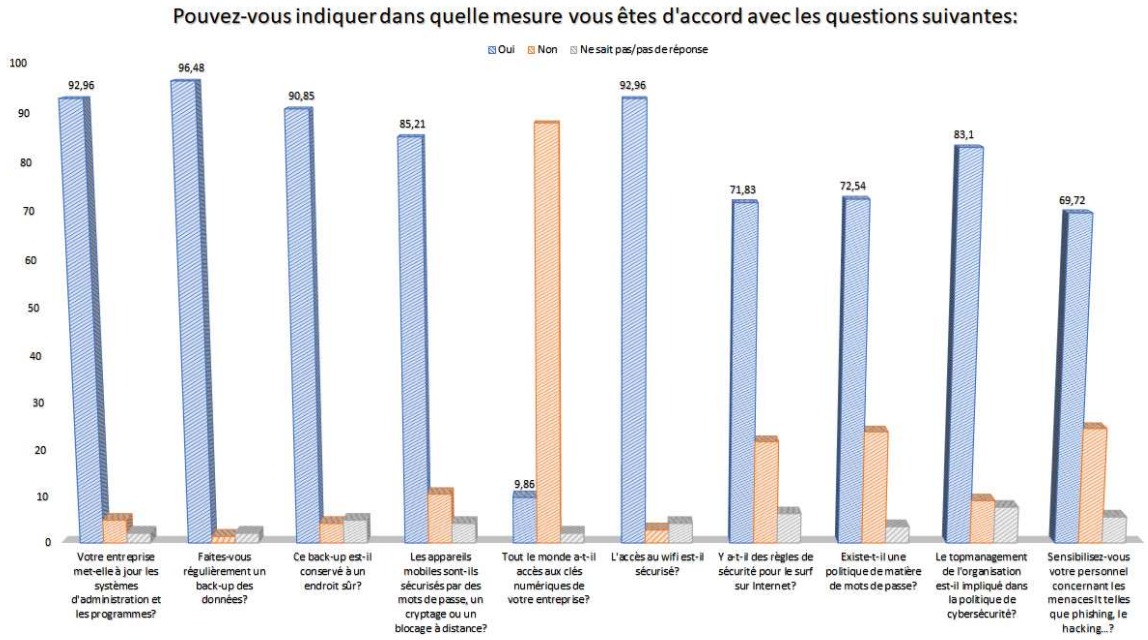

Figure 8 : Pouvez-vous indiquer dans quelle mesure vous êtes d'accord avec les questions suivantes : (N=142)

96,48% font régulièrement un back-up de leurs données. Seul 1,41% ne le fait pas et 2,11% n'ont pas répondu à cette question ou ne savaient pas. 92,96% ont indiqué que l'entreprise mettait à jour les systèmes d'administration et les programmes. À la question de savoir si le back-up est conservé à un endroit sûr, 90,85% ont répondu positivement. 92,96% ont déclaré que l'accès au wifi était sécurisé. Selon 88,03% des répondants, tout le monde n'a pas accès aux clés numériques de l'entreprise. D'après 83,1% des répondants, le topmanagement est impliqué dans la politique de sûreté IT ; selon 9,16%, ce n'est pas le cas et 7,75% n'ont pas répondu à cette question ou ne savaient pas. À la question de savoir si « les appareils mobiles étaient sécurisés par des mots de passe, un cryptage ou un blocage à distance », 85,21% ont déclaré que ce n'était pas le cas et 4,23% ne savaient pas ou n'ont pas répondu à cette question.

72,54% ont déclaraient qu'il existait une politique en matière de mots de passe alors que 23,94% ont signalé que ce n'était pas le cas. 3,52% ne savaient pas ou n'ont pas répondu. À la question de savoir s'il y avait des règles de sécurité pour le surf sur Internet 21,83% ont répondu que non, 71,83% ont indiqué que c'était le cas et 6,34% n'ont pas donné de réponse ou ne savaient pas. A la question « Sensibilisez-vous votre personnel concernant les menaces IT telles que le phishing, hacking… ? », 69,72% ont répondu positivement, 24,65% ont répondu négativement et 5,63% ne savaient pas ou n'ont pas pu donner de réponse.

L'Aons' Global Risk Management Survey de 2017 ne s'est pas uniquement penchée sur le top 10 des risques mais a également interrogé les répondants pour savoir dans quelle mesure ils étaient préparés aux risques, ce qu'on appelle « risk-preparedness ». Vu le coût considérable engendré par les cybercrimes et étant donné qu'il faut attendre longtemps avant qu'ils soient réglés, il importe pour les entreprises de se préparer aux cybercrimes. La plupart des entreprises indiquent qu'elles s'y préparent en planifiant une façon de gérer les

risques en question. Il ressort de cette enquête que 79% des entreprises sont prêtes à faire face au cybercrime/hacking/virus/code malveillants. Ce pourcentage de « readiness » est le plus élevé en comparaison des autres délits (Aons' Global Risk Management Survey, 2017).

En 2017, Tech Pro Research IT a interrogé des professionnels IT sur leur « *companies' cybersecurity readiness in the face of threats presented by mobile and IoT-connected devices* » Voici quelques-uns de leurs résultats majeurs :

- La plupart des répondants (39%) ont attribué à leur entreprise un score au-dessus de la moyenne en matière de *cybersecurity readiness*.
- Près de la moitié des répondants (49%) ont affirmé que cette *readiness* s'était améliorée au cours de la dernière année. Seuls 8% ont indiqué qu'elle avait régressé.
- Parmi tous les risques au niveau de la cybersécurité, les répondants ont indiqué que les plus menaçants pour leur entreprise étaient le phishing, le ransomware et les virus.
- Les méthodes les plus utilisées pour mettre en place la cybersécurité sont l'utilisation de produits malware, l'application de patches et de mise à jour et des méthodes de sécurité physique ;
- Les trois techniques les plus populaires pour la création d'une culture de la sécurité étaient l'instruction des utilisateurs, le personnel IT et les annonces en matière de sécurité.

Tech Pro Research a analysé en 2018 la stratégie de cybersécurité utilisée par les entreprises. 236 professionnels ont été interrogés sur leur stratégie en la matière. L'on s'est également penché sur la mise en pratique de cette stratégie. Voici la conclusion du rapport « Cybersecurity strategy research: Common tactics, issues with implementation, and effectiveness de 2018 » par Tech Pro Research :

- De manière générale, les résultats ont révélé que la plupart des entreprises ont recours à plusieurs procédés pour se protéger contre les transgressions et les attaques si bien que personne n'est pris en défaut dans ce domaine. Les problèmes résident toutefois dans la mise en place de mesures de sécurité.
- Beaucoup de répondants ont indiqué que la délégation du personnel constituait la pierre d'achoppement et, un groupe presque aussi significatif de répondants a signalé que la direction et l'obtention de fonds suffisants représentaient des défis. Enfin la majorité des répondants interrogés par Tech Pro Research ont indiqué qu'ils étaient un peu voire moyennement familiarisés avec les possibilités offertes par une entreprise pour se protéger contre la cybercriminalité.

Au niveau des données européennes, nous retrouvons ces statistiques belges dans Eurostat. Il est fait référence dans un rapport sur la sécurité ICT en entreprise. Les données ont été collectées sur la base de la *Community Survey on ICT usage and e-commerce in enterprises*[2] de 2015. Dans ce contexte, la sécurité ICT renvoie aux incidents pertinents, aux mesures, aux contrôles et aux procédures appliquées par les entreprises en vue d'assurer l'intégrité, la confidentialité et la disponibilité de leurs données et systèmes ICT. Il a été demandé aux entreprises dans quelle mesure elles disposaient d'une politique formelle de sécurité IT. En jetant un coup d'œil à l'Europe des 28 (l'UE dans sa composition actuelle), nous notons que 32% de l'ensemble des entreprises ont indiqué avoir une politique formelle de sécurité ICT. Ceci signifie que près d'un tiers des entreprises disposent d'une politique de sécurité ICT dans ce domaine. Si nous nous concentrons sur le pourcentage belge, l'on obtient 32% des entreprises belges interrogées. Il est fait une distinction entre les petites, moyennes et grandes entreprises. 72% des grandes entreprises[3], 51% des moyennes[4] et 27% des petites entreprises[5] ont indiqué disposer d'une politique de sécurité ICT.

783 des membres d'UNIZO ont été interrogés en 2016 sur la cybercriminalité et d'autres formes de criminalité (UNIZO, 2016). 7/10 des personnes interrogées prennent personnellement des mesures de sûreté. 43% disposent d'outils de sûreté élargis comme un système de back-up, un pare-feu, un antivirus… 30% confient leur sûreté IT à un partenaire IT ou une entreprise de sûreté. 10% d'entre eux déclarent ne pas être au courant du type de mesures proposées par le fournisseur IT.

UNIZO constate que des entreprises sont très peu ou à peine sécurisées quand d'autres investissent des sommes colossales dans la sûreté. Ces dernières qui entretiennent beaucoup de contacts avec le partenaire

[2] Ces données sont basées sur les chiffres de 2015. Près de 148.800 entreprises, employant plus de 10 travailleurs, sur 1,5 million en Europe des 28 ont été interrogées. L'on estime que ce 1,5 million d'entreprises, près de 83% emploient entre 10 et 40 collaborateurs, 14% entre 50 et 249 collaborateurs et 3% plus de 250 collaborateurs.
[3] Il s'agit des entreprises employant plus de 250 personnes.
[4] Il s'agit des entreprises employant entre 50 et 249 personnes.
[5] Une petite entreprise est une entreprise employant entre 10 et 49 personnes.

IT qui sécurise leur entreprise, souffriraient moins de cybercriminalité. UNIZO souhaite que chaque entreprise se pose la question de savoir comment mieux se protéger et comment y arriver. Il importe de faire preuve de vigilance à l'égard de toutes les formes de criminalités sur Internet.

3.6 Sûreté physique et organisationnelle

Outre le degré d'implication d'une entreprise dans la sécurisation IT, des questions ont également été posées sur la sûreté physique et organisationnelle.

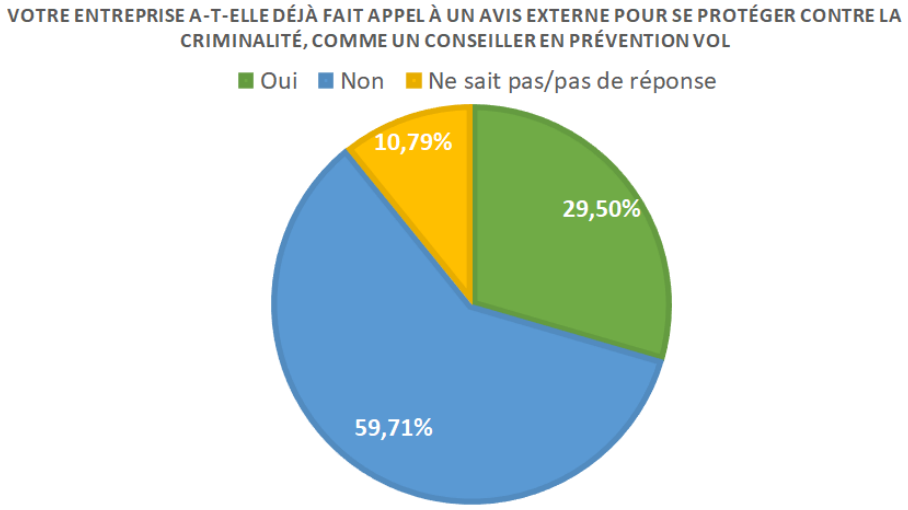

Figure 9 : Votre entreprise a-t-elle déjà fait appel à un avis externe pour se protéger contre la criminalité ? (n=139)

Comme nous le montre la Figure 9, 60% des entreprises interrogées ont indiqué que leur entreprise n'avaient pas fait appel à un avis externe pour se protéger contre la criminalité. Un peu moins de 30% ont répondu « oui » et 10,79% ont répondu « ne sait pas » ou n'ont pas donné de réponse.

À la question de savoir si l'entreprise avait déjà investi dans un ou plusieurs systèmes visant à la sûreté physique ou organisationnelle (contre la criminalité par exemple) 69,07% ont répondu positivement et 24,46% négativement tandis que 6,48% n'ont pas donné de réponse ou ne savaient pas.

Les répondants qui ont répondu « oui » se sont vu proposer toutes sortes de formes de sûreté physique ou organisationnelle comme le montre la figure ci-dessous.

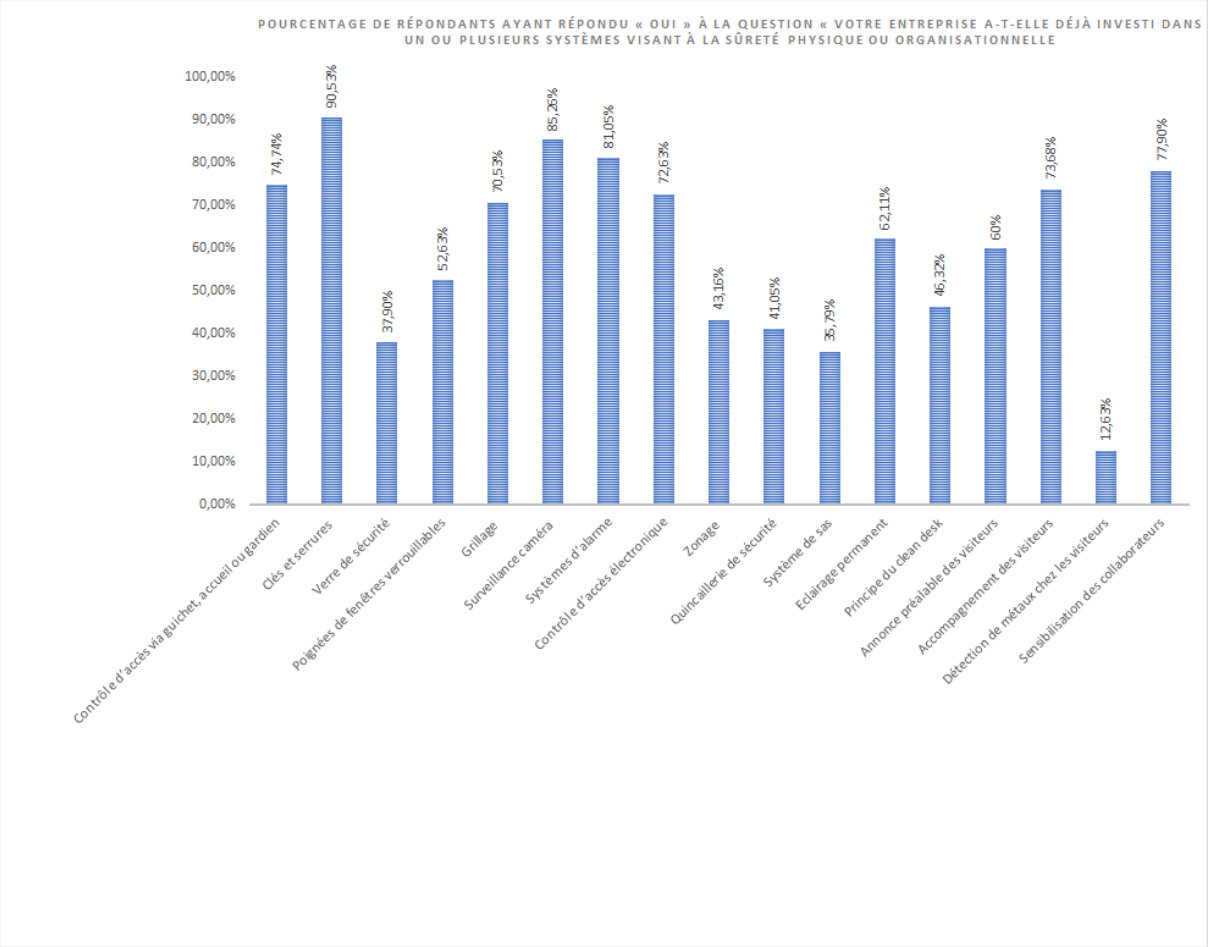

Figure 10 : Pourcentage de répondants ayant répondu « oui » à la question « Votre entreprise a-t-elle déjà investi dans un ou plusieurs systèmes visant à la sûreté physique ou organisationnelle (contre la criminalité par exemple) » ? (N=95)

Les répondants qui ont indiqué que leur entreprise avait investi dans la sûreté physique ou organisationnelle l'ont principalement fait dans les formes suivantes : contrôle d'accès via guichet ou accueil (74,74%), clés st serrures (90,53%), grillage (70,53%), surveillance caméra (85,26%), systèmes d'alarme (81,05%), contrôle d'accès électronique (72,63%), éclairage permanent (62,11%), annonce préalable des visiteurs (60%), accompagnement des visiteurs (73,68%) et sensibilisation des collaborateurs (77,90%).

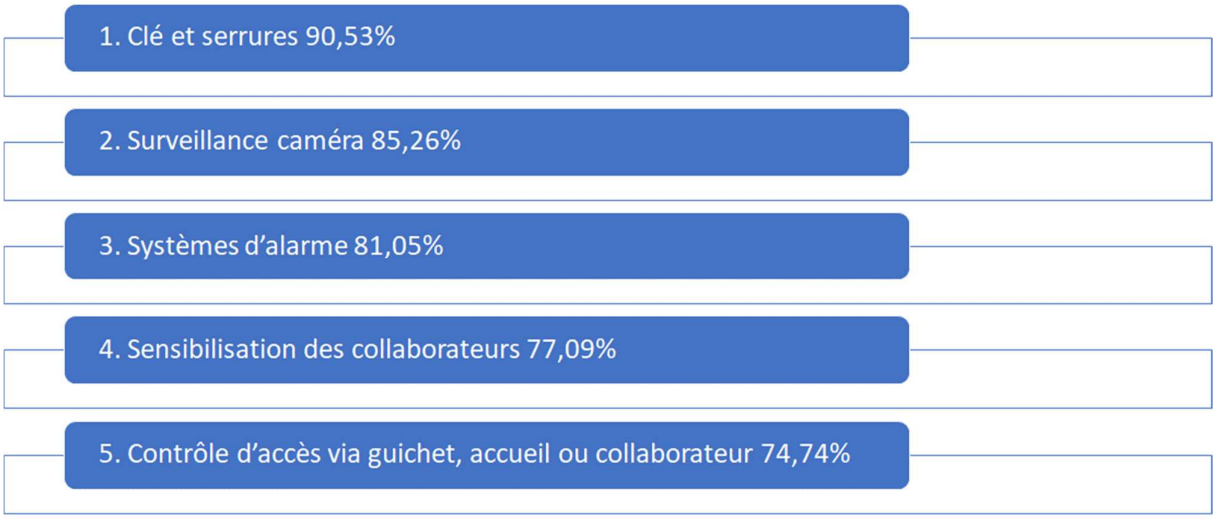

Figure 11 : Top 5 des formes les plus courantes de sûreté physique ou organisationnelle (N = 95)

Il est à noter que les méthodes de sûreté traditionnelles sont largement prisées. Les pourcentages élevés dans les catégories clés et serrures (90,53%) et contrôle d'accès via guichet ou accueil (74,74%) le prouvent.

L'investissement le moins souvent cité est « détection de métaux chez les visiteurs » (12,63%). Les personnes ayant indiqué « autre » comme systèmes de sûreté ont généralement donné les réponses suivantes : système de badge pour obtenir certains accès spécifiques, surveillance électronique et systèmes de contrôle d'accès spécifiques avec solutions, caméras, chien…

Plusieurs questions ont également été posées sur la sûreté générale dans le questionnaire UNIZO (UNIZO, 2016). 68% des répondants ont déjà investi dans un ou plusieurs systèmes de sûreté. La moitié d'entre eux ont installé un système d'alarme et l'autre moitié souhaitait faire partie d'un Partenariat Local de Prévention (11% ont déjà été membre d'un PLP).

En croisant les questions sur la présence d'un ou de plusieurs systèmes visant à une sûreté physique ou organisationnelle avec le nombre de collaborateurs au sein d'une entreprise, nous avons observé plusieurs liens significatifs.

Nous avons relevé un lien fort significatif statistiquement entre le nombre de collaborateurs et l'utilisation d'une surveillance caméra et le contrôle d'accès via un guichet, un accueil ou un collaborateur. Plus l'entreprise est grande, plus il est recouru à ce type de mesures.

En outre, nous avons établi plusieurs liens modérément significatifs d'un point de vue statistique entre la taille de l'entreprise et l'investissement dans certaines mesures. Les entreprises employant jusqu'à 250 collaborateurs ont plus souvent répondu « non » à la question de savoir s'ils utilisaient du verre de sécurité. Les poignées de fenêtre verrouillables, le contrôle d'accès électronique, un système de sas, un éclairage permanent, ou un principe de « clean desk » sont plus souvent cités dans les grandes entreprises que dans les entreprises de petite taille. Ne pas annoncer et ne pas accompagner les visiteurs au préalable sont les mesures les plus souvent citées dans les entreprises employant seulement 0-10 collaborateurs. Enfin, nous notons une parité concernant l'usage d'un système d'alarme.

3.7 Screening du personnel

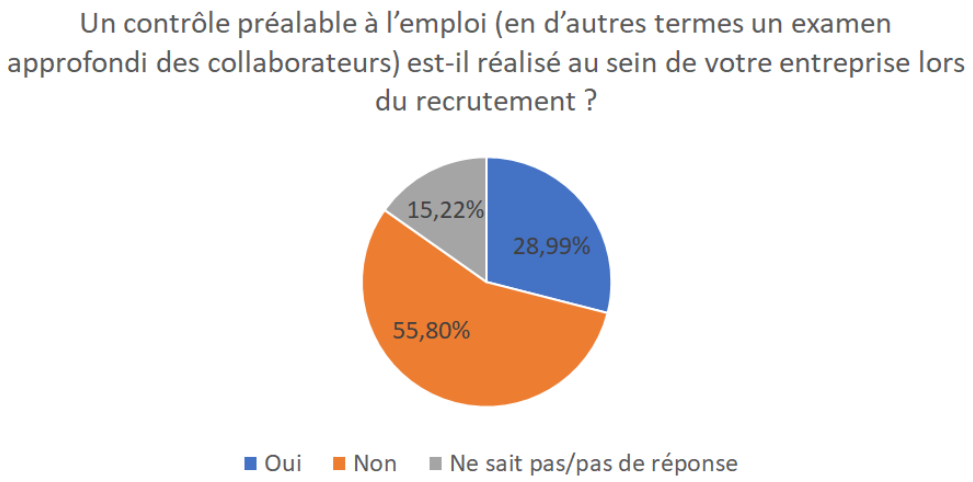

Figure 12 : Un contrôle préalable à l'emploi est-il réalisé ? (N=138)

Un peu plus de la moitié des répondants (à savoir 55,8%) ont répondu « non » à la question de savoir si un contrôle préalable à l'emploi était réalisé. 28,99% ont indiqué que c'est bien la cas et 15,22% ne savaient pas ou n'ont pas donné de réponse. Il a été demandé aux répondants qui ont répondu « oui » si ce contrôle était effectué pour toutes les fonctions. 75% d'entre eux ont répondu positivement. 15% ont déclaré que le contrôle n'était réalisé que pour certaines fonctions spécifiques à la sécurité et 5% ont répondu « non ». La question suivante concernait les différents aspects susceptibles d'être passés au crible. Les aspects les plus contrôlés sont « le contrôle actif des références » (indiqué par 85% des répondants), « les trous dans les CV » (82,5% ont répondu « oui »), « le contact avec l'ancien employeur » (75%) et « consulter les médias sociaux » (65% ont répondu positivement). Consulter d'autres sources ouvertes (ex. : Moniteur Belge) a été indiqué par 50% des répondants et 27,5% ont affirmé qu'ils sollicitaient un bureau externe pour effectuer ce contrôle.

Il a été demandé aux répondants ayant indiqué qu'il y avait un contrôle préalable à l'emploi au sein de leur entreprise si ce contrôle se faisait aussi par d'autres instances. Un peu plus de 60% ont signalé que c'était le cas. 30% ont affirmé que ce n'était pas le cas et 7,5% ne savaient pas ou n'ont pas donné de réponse. Il a aussi été demandé si un contrôle était effectué au cours de la carrière du travailleur, comme une réévaluation des travailleurs déjà engagés. 60,29% ont répondu « non », 30,88% ont répondu « oui » et 8,82% ne savaient pas ou n'ont pas répondu.

À l'heure actuelle, un contrôle via toutes sortes de canaux médiatiques tels que Facebook, Twitter et Linkedin est vite réalisé, ce qui est confirmé par Bafort (2016). Il en est ressorti qu'un candidat avec une bonne photo de profil recevait jusqu'à 21% de réactions plus positives lors de son entretien d'embauche qu'un candidat dont la photo de profil est moins bonne (Bafort, 2016).

3.8 Victimisation

3.8.1 Au cours des 12 derniers mois, les entreprises ont été le plus souvent victimes de cybercriminalité

Un volet important de ce questionnaire était le module « victimisation » dans lequel il a été demandé aux répondants si leur entreprise avait été victime d'un fait déterminé au cours des 12 derniers mois.

Dans ce qui suit, nous énumérons les faits dont a été le moins fréquemment victime l'entreprise ou un collaborateur au cours des 12 derniers mois :

Terrorisme (2,94% en ont été victimes)
Traite/trafic d'êtres humains (5,88% en ont été victimes)
Blanchiment d'argent (5,88% en ont été victimes)
Vol à main armée (7,35% en ont été victimes)
Chantage ou extorsion (pas via Internet) (8,82% en ont été victimes)
Cybercriminalité : cyberextorsion (9,56% en ont été victimes)
Accès interdit avec violence (9,56% en ont été victimes)
Sabotage (11,03% en ont été victimes)
Cybercriminalité : fraude Internet (11,77% en ont été victimes)

Tableau 3 : Au cours des 12 derniers mois, est-ce que votre entreprise ou un collaborateur de votre entreprise a été victime au travail de (N=136)

Le terrorisme, la traite/le trafic d'êtres humains et le blanchiment d'argent sont les faits dont a été le moins souvent victime une entreprise au cours des 12 derniers mois. Ces actes criminels ont aussi été évoqués dans la question relative à l'estimation du risque. Les répondants ont indiqué qu'il était très improbable d'être victimes des actes criminels suivants : traite des êtres humains (83,89%), blanchiment d'argent (83,33%), contrefaçon (76,11%) et terrorisme (75%).

Le tableau 4 montre le top 4 des actes criminels dont a été victime l'entreprise ou un collaborateur de l'entreprise au cours des 12 derniers mois :

		Oui	Non	Ne sait pas/pas de réponse
1	Une ou plusieurs formes de cybercriminalité	42,6%	53,7%	3,7%
2	Dégradation d'un véhicule (vélo, moto, auto, camionnette, camion…)	41,91%	53,68%	4,41%
3	Violence, agression (sans vol)	39,71%	55,15%	5,15%
3	Dégradation de propriété (pas de véhicule) ou vandalisme	39,71%	58,09%	2,21%
4	Accès interdit sans violence	38,24%	58,09%	3,68%

Tableau 4 : Top 4 des faits dont a été victime une entreprise ou un collaborateur d'une entreprise au cours des 12 derniers mois (N=136)

Près de 43% des entreprises interrogées ont signalé qu'elles avaient été victimes d'une des 5 formes de cybercriminalité au cours des 12 derniers mois. 41,91% ont indiqué qu'elles avaient été victimes d'une détérioration d'un véhicule (comme un vélo, une moto, une auto, une camionnette, un camion) et 2% de moins ont indiqué avoir été victimes d'une dégradation de propriété (pas de véhicule) ou de vandalisme au cours des 12 derniers mois. Un pourcentage similaire, à savoir 39,71%, a indiqué avoir été victime de violence et d'agression (sans vol), ce qui signifie qu'1 entreprise sur 3 a été victime de violence, d'agression (sans vol), ou d'une quelconque forme de dégradation de véhicule ou de propriété.

Les deux formes de cybercriminalité les plus signalées sont les suivantes :

		Oui	Non	Ne sait pas/pas de réponse
1	Cybercriminalité : accès illégal aux systèmes IT (via hacking, phishing, deviner un mot de passe…)	33,09%	60,29%	6,62%
2	Cybercriminalité : Ingérence dans les données ou les systèmes (via des virus, cryptoware, (D) attaques par déni de service (DoS attacks) par le biais de réseaux de bot)	29,41%	63,97%	6,62%

Tableau 5 : Deux formes de cybercriminalité les plus courantes dont une entreprise ou un collaborateur a été victime au cours des 12 derniers mois (N=136)

Les faits issus des tableaux 4 et 5 ont été croisés avec le nombre de collaborateurs travaillant dans l'entreprise. Différents liens modérément significatifs ont été établis. Nous remarquons que les entreprises employant plus de 251 collaborateurs étaient plus fréquemment victimes de « violence, d'agression (sans vol) ». L'acte criminel « vol d'un véhicule (vélo, moto, auto, camionnette, camion…) » donne lieu à un lien statistiquement significatif s'il est croisé avec le nombre de collaborateurs dans l'entreprise. La moitié des répondants issus des entreprises employant 251 et 500 collaborateurs ou plus de 1001 collaborateurs, ont répondu « oui » à cette question. Les entreprises employant moins de 250 collaborateurs, ont répondu « non » dans 90% des cas.

La majorité des répondants n'ont pas été victimes de « vol à main armée », seules les grandes entreprises employant plus de 1001 collaborateurs ont signalé ce fait de temps à autre. Même constat pour l'acte criminel « vol avec violence – sans arme ».

Les répondants qui ont été victimes d' « accès interdit avec violence » au cours des 12 derniers mois sont peu nombreux et travaillent principalement dans les entreprises de grande taille. À la question de savoir si les

entreprises avaient été victimes de dégradations de véhicules (vélo, moto, voiture, camionnette, camion…), les réponses étaient partagées. Ce sont principalement les entreprises comptant entre 251 et 1000 collaborateurs qui ont indiqué être victimes de ce fait. Les entreprises employant plus de 501 collaborateurs ont été plus fréquemment victimes de « détérioration de propriété (pas de véhicule) ou de vandalisme ».

Ce sont surtout les grandes entreprises (comptant plus de 1001 collaborateurs) qui ont été victimes, au cours des 12 derniers mois, d'une « forme de fraude (sociale, fraude en matière de gestion des déchets…), qui n'est pas commise par Internet ». Nous retrouvons des résultats d'étude similaire en matière de « chantage ou extorsion (pas via internet) » et de « sabotage ».

Un lien statistiquement significatif est apparu pour « fausse monnaie » : les petites et moyennes entreprises (employant jusqu'à 500 collaborateurs) ont indiqué plus souvent « non » à la question de savoir si elles avaient victimes de cet acte criminel au cours des 12 derniers mois. Près de 43% des entreprises dans lesquelles plus de 1001 collaborateurs travaillent ont été victimes de « document faux ou falsifiés ». Les entreprises de plus petite taille ont indiqué ne pas en avoir été victimes.

Nous avons également demandé aux entreprises si elles avaient été victimes de certaines formes de cybercriminalité. Voici les formes de « cybercriminalité » dont elles ont été victimes au cours des 12 derniers mois : accès illégal aux systèmes IT (via hacking, phishing, deviner un mot de passe …) ». Un lien significatif d'un point de vue statistique a été établi en croisant avec le nombre de collaborateurs travaillant dans l'entreprise. Les entreprises de toutes tailles en ont été victimes mais les entreprises employant plus de 1001 collaborateurs ont indiqué le plus souvent en avoir été victimes. Nous avons relevé le même constat pour la « cybercriminalité » : ingérence dans les données ou les systèmes (via virus, cryptoware, (D) attaques Dos par le biais de réseaux de bots) » et « cybercriminalité » : « fraude sur Internet ».

En matière de « cybercriminalité » : la majorité des entreprises n'a pas été victime de cyberextorsion. Dans le peu de cas où cet acte criminel a été indiqué, cela concernait les entreprises employant plus de 1001 collaborateurs.

Enfin, un lien significatif statistiquement a été observé entre les « faits liés aux drogues (trafic, consommation) » et le nombre de collaborateurs dans l'entreprise. Près de 40% des entreprises employant plus de 501 collaborateurs ont indiqué en avoir été victimes au cours des 12 derniers mois.

783 membres d'UNIZO ont été interrogés en 2016 sur la cybercriminalité et d'autres formes de criminalité (UNIZO, 2016). 49,8% ont été victimes d'une forme de cybercriminalité en 2016, soit une hausse par rapport à 2014 et 2015 (environ de 40% et de 30%).

Dans 15% des cas, il était question de systèmes IT qui avaient été hackés. Plusieurs entrepreneurs ont connu des problèmes liés aux paiement effectués via Internet et 23% ont été victimes de phishing. Dans les chiffres de criminalité enregistrés par la police, la cybercriminalité est décrite comme un phénomène indépendant géographiquement (police fédérale, 2016). Il existe des différences suivant la nature de l'entreprise (cf. secteur économique). La police fédérale signale que les dommages occasionnés par fait sont en hausse et que les formes de cybercriminalité évoluent de façon telle que les entreprises constituent une cible plus prisée que les particuliers.

En outre, UNIZO a interrogé les entrepreneurs sur plusieurs aspects liés à la sécurité. 10% des 783 entrepreneurs interrogés ont été victimes d'effraction/de vol au cours de l'année écoulée. Cela concernait essentiellement les petits commerçants (23%) et le secteur de la construction (16%). Près de 30% des entrepreneurs ont déjà été victimes d'une forme d'agression : il s'agissait généralement d'agression verbale.

Consécutivement à la menace terroriste, l'état d'inquiétude des répondants a également été passé au crible. Il en est ressorti que près de la moitié se sont montrés inquiets après les attentats et qu'un quart des entreprises interrogées ont investi davantage dans la sécurité (UNIZO, 2016).

3.8.2 La violence, l'agression sans vol : fait le plus marquant

Si l'entreprise ou un collaborateur de l'entreprise a été victime de l'une des formes de criminalité susmentionnées, il lui a été demandé lequel de ces faits a été le plus marquant. Les victimes ont le plus souvent indiqué les faits suivants : « violence, agressions sans vol » (19,3%), « cybercriminalité : accès illégal aux systèmes IT (via hacking, phishing, deviner un mot de passe …) » (8,77%), « accès interdit sans violence » (7,9%) et « vol de chargement » (7,9%).

Les raisons pour lesquelles un fait a été considéré comme marquant sont variées : financier, image, personnel, crainte du personnel… Les pourcentages les plus élevés concernaient la violence, l'agression sans vol, le fait qu'un individu ait été personnellement impliqué.

3.8.3 Un tiers des répondants ne portent pas plainte à la police

Les questions suivantes dans le baromètre ont trait au fait le plus marquant dont a été victime l'entreprise ou un collaborateur.

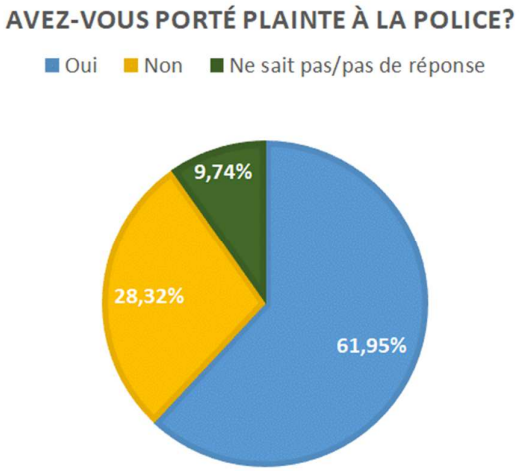

Figure 13 : Avez-vous porté plainte à la police ? (N=113)

En interprétant la figure ci-dessus, nous notons que 61,95% des répondants ont porté plainte au sujet de la forme de criminalité la plus marquante dont ils ont été victimes au cours des 12 derniers mois. Un tiers des victimes interrogées n'ont pas porté plainte et à peine 10% ne savaient pas ou n'ont pas donné de réponse.

En croisant cette question avec le nombre de collaborateurs dans l'entreprise, un lien statistiquement significatif est apparu. Les entreprises employant un nombre élevé de collaborateurs ont répondu plus fréquemment « oui » que les entreprises de moyenne et de petite taille.

Les principales raisons (attention lors de l'interprétation de ces résultats car les répondants ont pu indiquer plusieurs réponses) pour lesquelles les répondants ont porté plainte à la police sont les suivantes :

- Parce qu'il s'agit d'empêcher que de tels faits ne se reproduisent (42,86%)
- Parce que nous jugions l'affaire suffisamment grave (41,43%)
- Parce que l'auteur doit être arrêté ou sanctionné (37,14%)
- Parce que nous souhaitions une attestation pour l'assurance (34,29%)
- Parce que signaler les faits est un devoir (22,86%)
- Parce que l'organisation policière doit prendre des mesures (20%)

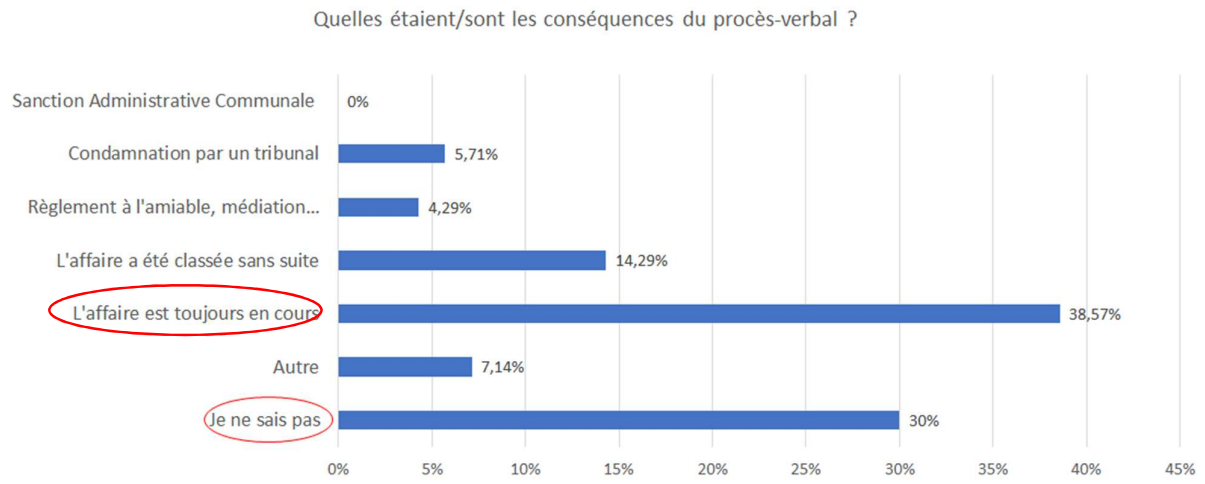

Figure 14 : Quelles étaient/sont les conséquences du procès-verbal ? (N=70)

Pour observer un lien éventuel entre le fait de porter plainte ou non, il a également été demandé aux répondants quelles étaient les conséquences du procès-verbal. Parmi eux, 38,57% ont indiqué que l'affaire était toujours en cours alors que 30% ont déclaré ne pas savoir. 14,29% ont répondu que l'affaire avait été classée sans suite.

Il a été demandé aux victimes qui n'ont pas porté plainte à la police pour quelles raisons elles avaient agi ainsi. Les motifs les plus souvent avancés étaient :

- Parce que cela ne donne de toute façon aucun résultat (28,13%)
- Parce que nous connaissons l'auteur (15,63%)
- Autre (15,63%)
- Parce que nous trouvions que l'affaire n'était pas assez grave (12,5%)
- Parce qu'il n'y a eu aucun ou très peu de dommages (12,4%)
- Parce que l'on ne peut de toute façon rien y faire (12,5%)

La propension à dénoncer un acte criminel est une donnée cruciale, et pas seulement pour la Belgique. Les statistiques de la police en matière de criminalité sont mises à jour et génèrent un indicateur ou baromètre de la criminalité enregistrée. Ceci permet entre autres à la police d'évaluer son fonctionnement à court et long terme ou de parfaire son fonctionnement opérationnel (police fédérale, 2018). En outre, les décideurs politiques peuvent se baser sur ces chiffres pour élaborer une stratégie et des mesures de sécurité.

D'une part, la police peut agir proactivement (criminalité quérable) et partir en quête de criminalité par le biais d'actions ou de contrôles. Outre la criminalité quérable, il est également question de criminalité rapportée lorsque les victimes portent plainte et qu'un procès-verbal est rédigé. Vu la capacité et les moyens limités, la criminalité rapportée constitue la principale source d'informations. La dénonciation de la criminalité est dès lors d'une importance capitale (Versteegh, 2007), mais il s'avère dans la pratique que ce n'est pas une sinécure.

Il est fait mention dans les tendances 2016-2017 de la police fédérale de la plus petite quantité de données chiffrées consignées depuis le début des comptages en 2000. Toutes sortes de raisons sont avancées comme un 'International crime drop' : de meilleures stratégies et techniques policières, une protection technoprotectrice, une hausse des caméras publiques, des firmes de surveillance privées … (van Dijk, Tseloni & Farrell, 2012). Cette tendance à la baisse est une donnée internationale que nous retrouvons également aux Pays-Bas. Le chef de corps Akerboom a affirmé que les chiffres de la police néerlandaise en 2017 étaient en baisse pour la cinquième année consécutive. Hormis l'International crime drop, il est également probable que les citoyens dénoncent moins les actes criminels. Dans un rapport 'Veilige buurt', l'on s'est penché sur les raisons pour lesquelles les victimes ne portaient pas plainte auprès de la police. 39% des répondants ont indiqué ne pas avoir porté plainte car « ça ne servait à rien » (Veilige buurt, 2017).

La raison « parce que cela ne donne de toute façon aucun résultat » est décrite dans la littérature comme l'approche du choix rationnel. Les coûts engendrés par le dépôt de plainte et les formalités complémentaires étaient supérieurs au profit. Ce choix rationnel entre aussi en considération au niveau de l'explication « parce que nous connaissons l'auteur ». Dans ce cas les faits ne sont pas dénoncés car la honte et les représailles

éventuelles ne contrebalancent pas les conséquences possibles de la plainte, comme d'éventuelles poursuites. En d'autres termes, le coût l'emporte sur le profit réel (Smets, De Kinder & Moor, 2011).

3.8.4 Caractéristiques de l'acte criminel

Il a été demandé aux répondants victimes d'un acte criminel s'ils connaissaient ou non l'auteur. La figure ci-dessous nous indique que 71,68% des victimes ne connaissaient pas l'auteur tandis contre 28,32% qui le connaissaient.

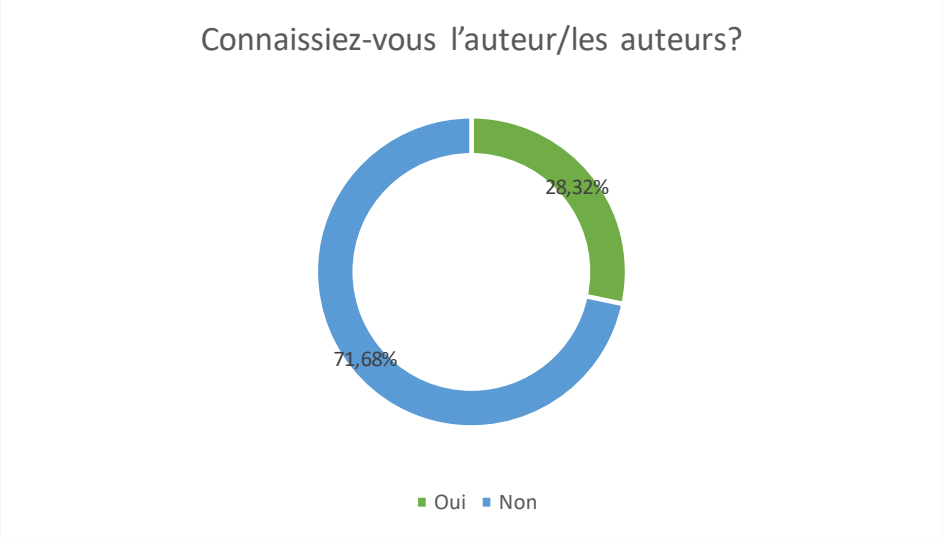

Figure 15 : Connaissiez-vous l'auteur/les auteurs ? (N=113)

Si l'auteur était connu, les répondants devaient indiquer de qui il s'agissait.

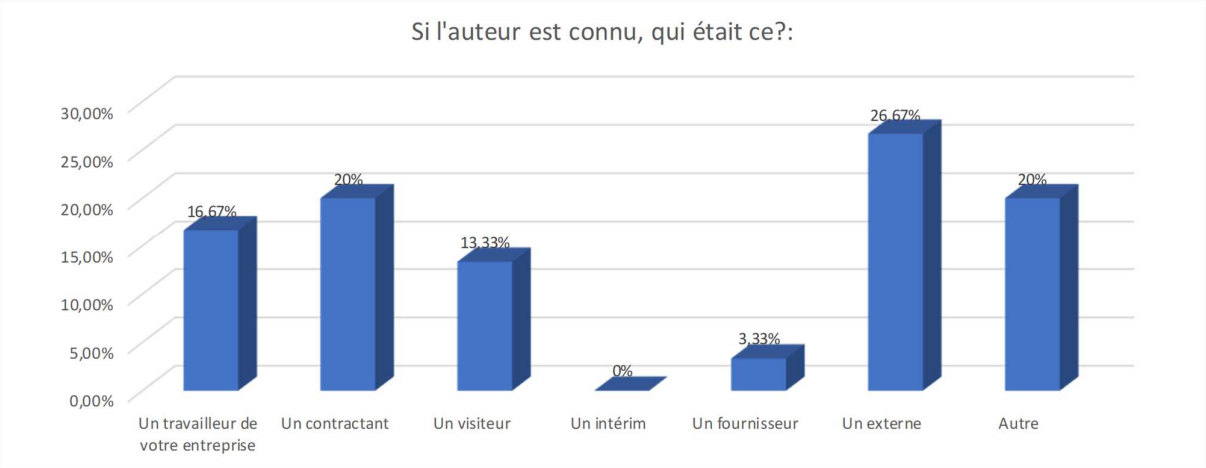

Figure 16: Si l'auteur est connu, qui était-ce ? (N=30)

La Figure 16 montre que si l'auteur était connu, il s'agissait dans 26,67% des cas d'un externe, dans 20% des cas d'un contractant ou « autre » et dans 16,67% des cas d'un travailleur de l'entreprise.

Bien que ce phénomène soit peu étudié, l'on estime depuis longtemps que la criminalité est en hausse chez les travailleurs. La notion de criminalité des travailleurs est difficilement définissable et est rarement visible, ce qui fait que l'ampleur du problème est souvent minimisée. La grande partie de la criminalité des travailleurs concerne la criminalité des biens (Guinevere, 2010) mais d'autres formes sont également en vogue. Une récente étude a montré que plus d'un tiers des actes frauduleux en entreprise étaient commis par le personnel propre à l'entreprise (De Tijd, 2018).

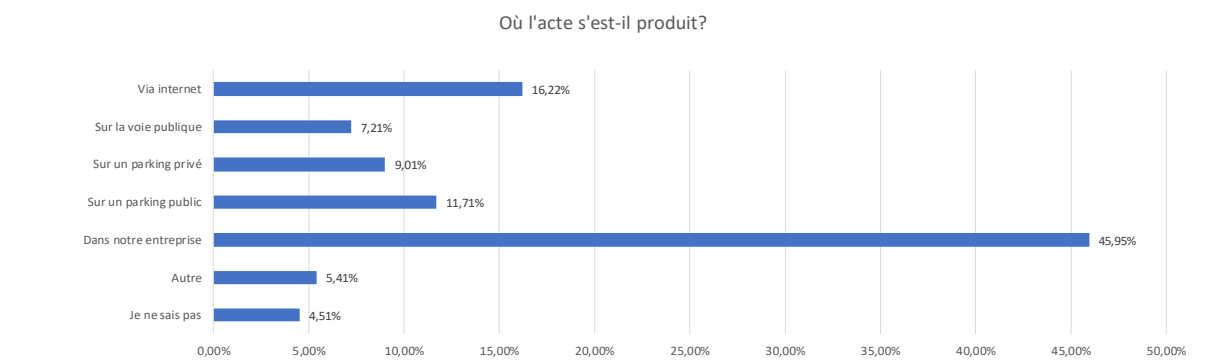

Figure 17 : Où cet acte criminel s'est-il produit ? (N=111)

Dans 45,95% des cas, l'acte criminel s'est produit dans l'entreprise même. 16,22% des répondants ont été victimes d'actes criminels via Internet et 11,71% sur un parking public.

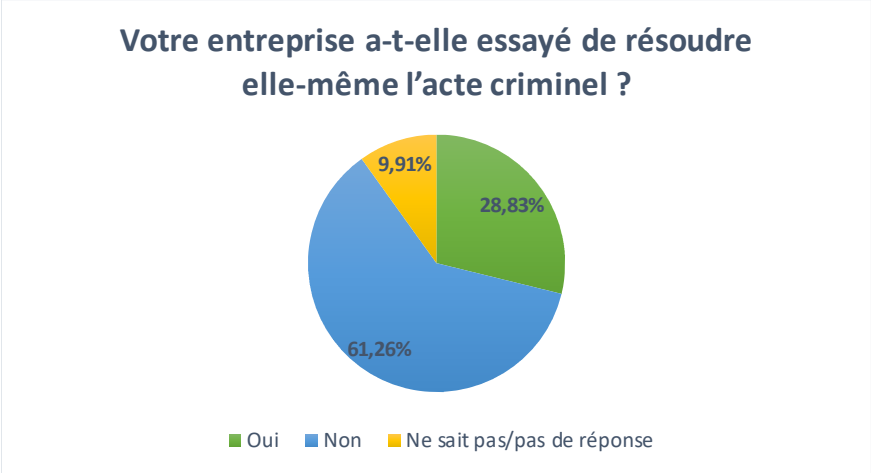

Figure 18 : Votre entreprise a-t-elle essayé de résoudre elle-même l'acte criminel ? (N=111)

À la question de savoir si l'entreprise a essayé de résoudre elle-même l'acte criminel par exemple en recherchant ou en contactant l'auteur, en réglant l'affaire à l'amiable… nous remarquons sur la base de la figure 18 que la majorité des répondants ont indiqué que ce n'était pas le cas. A l'inverse, un tiers des répondants (28,83%) ont indiqué que c'était le cas. Il est ressorti de l'étude Guinevere (2010) sur la criminalité des travailleurs que 20% avaient prévenu le patron en cas de vol, 44% ont contacté le travailleur, 44% n'ont rien dit et 0% a averti la police. Les entreprises font de plus en plus appel à des services de dépistage privés et/ou des départements de recherche internes pour lutter contre toutes formes de criminalité des travailleurs (WODC, 2010).

En croisant cette question avec le nombre de travailleurs dans une entreprise, l'on observe un lien statistiquement significatif : les entreprises employant jusqu'à 250 collaborateurs ont répondu plus souvent « non » à la question : « votre entreprise a-t-elle essayé de résoudre elle-même l'acte criminel (par exemple en recherchant ou en contactant l'auteur, en réglant l'affaire à l'amiable …) ».

Il a ensuite été demandé aux victimes combien d'heures avaient été nécessaires au personnel pour résoudre l'acte criminel. 33,33% ont répondu « pas d'application », 18,02% ont indiqué « entre 1 heure et 1 demi-journée », 14,41% « entre une demi-journée et une journée » et 13,51% « moins d'1 heure ». 11,71% ont indiqué « 1 semaine ou plus".

Encore plus de répondants – à savoir 64,87% - ont répondu « pas d'application » à la question de savoir combien d'heures avaient été nécessaires à une société externe pour résoudre l'acte criminel. Un peu moins de 10% ont indiqué « moins d'une heure » et 8,11% ont répondu « entre un jour et une semaine ».

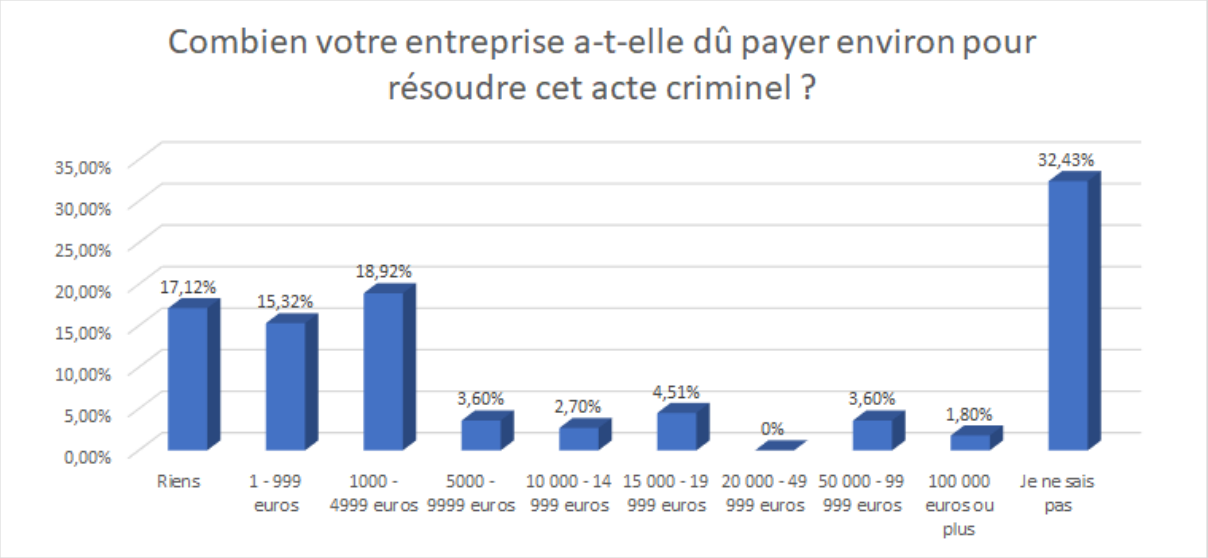

Figure 19 : Combien votre entreprise a-t-elle dû payer environ pour résoudre cet acte criminel ? (N=111)

À la question de savoir combien l'entreprise a-t-elle dû payer pour résoudre l'acte criminel, 32,43% ont répondu « je ne sais pas ». 18,92% ont répondu entre 1000 et 4999 euros, 17,12% ont déclaré que ça ne leur avait rien coûté et 15,32% ont signalé qu'elles avaient dû débourser entre 1 et 999 euros.

Il a également été demandé qui a payé ces frais. 43,24% ont répondu que c'était l'entreprise même. 26,13% n'ont pas répondu à cette question, 12,61% ont répondu que l'assurance s'en était chargée et 11,71% ont répondu « ne sait pas ».

Ensuite, la question des dégâts subis a été abordée, voici les résultats.

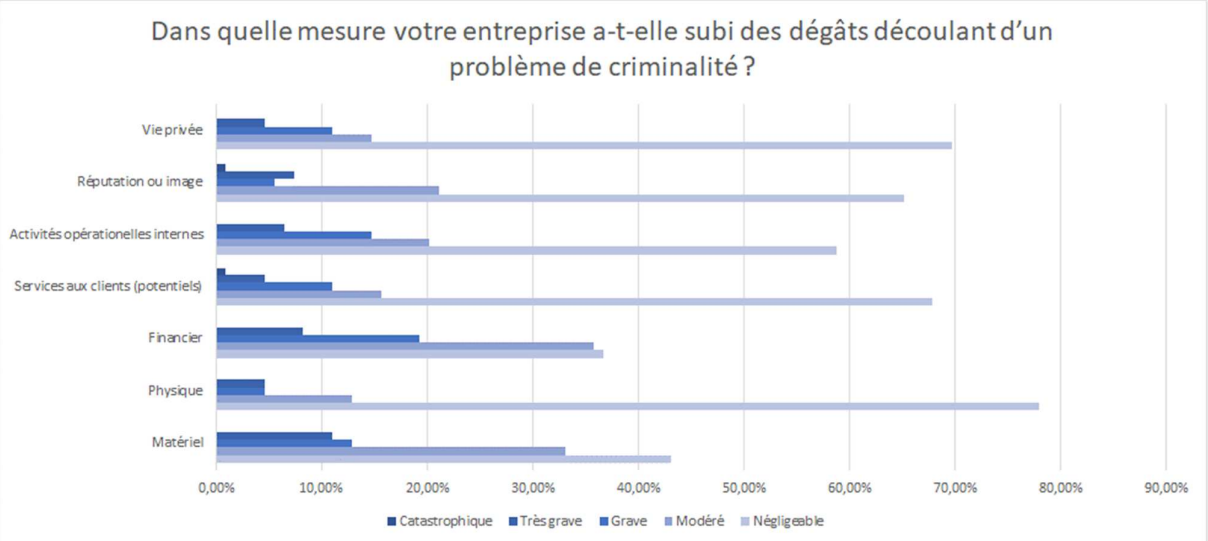

Figure 20 : Dans quelle mesure votre entreprise a-t-elle subi des dommages découlant d'un problème de criminalité ? (N=109)

La Figure 20 montre que les dommages subis par une entreprise découlant d'un acte criminel étaient négligeables dans beaucoup de cas. 27,53% des répondants ont indiqué que les dommages au niveau financier étaient « graves voire très graves » au niveau financier, 23,85% ont répondu qu'ils étaient « graves voire très graves » au niveau matériel et 21,10% ont signalé qu'ils étaient « graves voire très graves » concernant les activités opérationnelles internes.

Certains répondants suggèrent une autre forme de dommages comme des dommages émotionnels en raison d'une menace, des dégâts causés aux clôtures, l'abandon d'importants projets, une porte d'accès forcée…

À la fin du questionnaire, plusieurs questions étaient posées sur l'attention et le suivi de la victimisation.

	Oui	Non	Ne sait pas/pas de réponse
Il existe une organisation qui aide et soutient les entreprises qui subissent des actes criminels	38,40%	22,40%	39,20%
Nous avons déjà fait appel à une organisation qui aide et soutient les entreprises qui subissent des actes criminels	20,80%	65,60%	13,60%
Il existe des aides psychosociales pour les collaborateurs victimes d'actes criminels	66,40%	15,20%	18,40%
Nous estimons qu'il existe suffisamment d'aides psychosociales au sein de notre entreprise au cas où quelqu'un serait victime d'actes criminels	52%	26,40%	21,60%
Il y a une personne de confiance en charge de cette matière dans notre entreprise	65,60%	24,80%	9,60%
Il existe un point de contact anonyme au sein de notre entreprise	45,60%	45,60%	8,80%
Il existe au sein de notre entreprise une procédure pour signaler les agissements suspects sur le lieu du travail et en dehors ?	54,40%	36,80%	8,80%
Il existe un point de contact externe (aide à la victime, IDEWE) dans ce domaine	56,80%	30,40%	12,80%
Il existe un point de contact interne (psychologue en entreprise, médecin) dans ce domaine	40,80%	45,60%	13,60%

Tableau 6 : Indiquez si vous êtes d'accord avec les affirmations suivantes : (N=125)

66,4% ont répondu « oui » à la question de savoir s'il y avait des aides psychosociales pour les collaborateurs victimes d'actes criminels. L'on relève un pourcentage identique de répondants (à savoir 65,6%) ayant indiqué qu'il y avait une personne de confiance en charge de cette matière au sein de l'entreprise. Un peu plus de la moitié des répondants (56,8%) ont déclaré qu'il existait un point de contact externe (aide à la victime, idewe) dans ce domaine et 54,4% ont indiqué qu'il existait au sein de l'entreprise une procédure pour signaler les agissements suspects sur le lieu du travail et en dehors. La moitié des répondants ont indiqué qu'il existait suffisamment d'aides psychosociales au sein de l'entreprise au cas où quelqu'un serait victime d'actes criminels. Enfin, 65,6% ont indiqué ne pas avoir fait appel à une organisation qui aide et soutient les entreprises qui subissent des actes criminels.

Nous avons relevé plusieurs liens (modérément) significatifs d'un point de vue statistique en croisant ces affirmations avec le nombre de collaborateurs dans l'entreprise :

- Pour les deux premières affirmations, concernant l'appel aux organisations qui aident et soutiennent les entreprises subissant des actes criminels, nous notons que les petites entreprises ont plus souvent répondu « non ».
- À la question de savoir s'il existait des aides psychosociales, ce sont surtout les entreprises de grande taille qui y ont répondu positivement.
- « Il existe suffisamment d'aides au sein de l'entreprise pour aider les personnes ayant subi des actes criminels » : plus l'entreprise est grande, plus la réponse est positive.
- « Il y a une personne de confiance en charge de cette matière au sein de notre entreprise » et « Il existe un point de contact anonyme au sein de notre entreprise » : les entreprises employant jusqu'à 50 collaborateurs ont plus souvent répondu non.
- « Il existe au sein de notre entreprise une procédure pour signaler les agissements suspects sur le lieu de travail et en dehors » : les entreprises employant plus de 251 collaborateurs ont répondu plus positivement de manière générale.
- « Il existe un point de contact externe » : les entreprises employant plus de 51 collaborateurs ont répondu plus positivement.
- « Il existe un point de contact interne » : les entreprises employant plus de 1001 collaborateurs ont répondu plus positivement.

4. Avis sur la session de travail interactive

Au cours d'une session de travail interactive (SI), les résultats d'étude dudit baromètre ont été commentés avec les organisations partenaires. Dans les lignes qui suivent, nous allons discuter de plusieurs considérations.

4.1 Employeur versus travailleur

Les affirmations issues du premier tableau ont indiqué entre autres choses que les travailleurs accorderaient moins d'attention à la sûreté dans une entreprise que les employeurs. Quand ce résultat a été abordé lors de la SI, il a été avancé que tant les employeurs que les travailleurs ont un rôle crucial à jouer au niveau de la sûreté dans l'entreprise. Le pourcentage élevé de répondants d'accord avec l'affirmation « Notre direction accorde de l'attention à la sûreté », peut éventuellement s'expliquer par le fait que beaucoup de dirigeants ont complété ce questionnaire, et que le cadre dirigeant s'estime responsable de la sûreté dans l'entreprise. « *La sécurité au plus haut niveau occupe une place plus importante dans notre agenda* », selon un participant. Enfin, quelqu'un a ajouté que les messages de prévention sur le plan de la sûreté ne font pas toujours mouche.

Près de 30% des répondants ont également indiqué ne pas être d'accord avec l'affirmation selon laquelle des activités de sensibilisation sont organisées dans le cadre de la sûreté. Il a été avancé durant la session de travail interactive que ces résultats coïncident avec les chiffres obtenus pour l'affirmation « nos collaborateurs accordent de l'attention à la sûreté ». Les collaborateurs sont moins conscients de l'importance de la sûreté dans l'entreprise, ce qui explique pourquoi ils y accordent moins d'attention. De surcroît, selon un participant à la SI, il manque souvent de temps pour conscientiser suffisamment les travailleurs : « *Dans beaucoup de nos secteurs, la charge de travail est telle qu'on n'a pas le temps d'organiser des activités de ce genre* ». Néanmoins, il importe de libérer du temps pour ce genre d'activité.

Il est frappant de constater que près de 47,34% ont indiqué que peu voire pas de tests ou contrôles sont organisés au niveau de la sûreté dans l'entreprise, ce qui est perçu comme problématique durant la SI.

Enfin, il est important de souligner que certaines entreprises agissent avec précaution quand il s'agit de communiquer en matière de sûreté. Ces informations ne sont par conséquent pas toujours relayées.

4.2 Cybercriminalité comme risque

Les faits dont les gens pensent qu'ils pourraient devenir victimes semblaient plausibles aux participants à la SI. La cybercriminalité est un risque réel et les gens en sont conscients. D'un autre côté, il a été signalé qu'il est inquiétant de constater que deux tiers des personnes interrogées ne l'évaluent pas comme un risque, sachant que la cybercriminalité est en hausse. Une organisation a mentionné que certains secteurs sont plus exposés à la cybercriminalité que d'autres. La criminalité ICT touche à peine le secteur de l'agriculture, de la sylviculture et de la pêche.

Le fait que la violence et l'agressivité constituent souvent un risque a été confirmé, en particulier par un participant représentant les services sociaux et de santé humaine. Les ambulanciers, le personnel d'accueil au service des urgences, le personnel soignant dans les maisons de repos, le personnel infirmier dans les hôpitaux et/ou les établissements psychiatriques, etc. sont souvent confrontés à de l'agression et à de la violence. Cette agression est parfois aussi commise par le patient. En outre, les hôpitaux, les maisons de repos et les institutions sont généralement des lieux accessibles au public, ce qui signifie qu'ils sont fréquemment exposés au public et courent donc un risque plus élevé de devenir victimes d'une certaine forme de menace, de violence et d'agression.

Le fait que l'on sous-estime les risques de manière générale est considéré comme un résultat de recherche « logique » par les participants à la session de travail interactive. Les entreprises de petite taille ne se sentent absolument pas concernées par certaines formes de criminalité telles que la traite/le trafic d'êtres humains ou le blanchiment d'argent et ne s'attendent donc pas à en être victimes.

4.3 Culture de la sécurité, gestion et politique en matière de sûreté dans votre entreprise

À la question de savoir s'ils ont connaissance des modifications au niveau des prescriptions et des dispositions légales relatives à la sûreté dans leur entreprise, 68,94% ont répondu « oui » et 31,06% « non ». En outre, 56,6% des répondants ont indiqué qu'il existait une politique de sûreté contre la criminalité et 43,4% ont répondu que ce n'était pas le cas. Plusieurs répondants travaillant dans une petite entreprise ont répondu « non » à la question de savoir s'il y avait dans leur entreprise une politique de sûreté contre la criminalité. Ce lien a été contextualisé pendant la SI : « *S'il n'y a que 5 personnes dans une entreprise, il n'y aura pas forcément de politique de sécurité à proprement parler mais un accord oral sera établi ou certaines règles seront fixées entre les différents travailleurs* ». Un participant à la SI a indiqué que ça ne signifiait pas pour autant que les petites entreprises étaient plus vulnérables : « *Elles sont de plus petite taille et elles ont peut-être moins besoin de sécuriser les choses, d'une politique de sûreté ou d'une fonction spécifique dans le cadre de la sûreté ».*

67,3% des entreprises ont indiqué prendre des mesures dans la lutte contre la criminalité. Parmi les entreprises qui ont répondu « oui », 75% trouvaient qu'il s'agissait de mesures adaptées ou correctes. Ces résultats ont été expliqués durant la SI par le fait que la plupart des dirigeants interrogés développement ou mettent sur pied lesdites mesures, ils les considèrent donc comme « adaptées ».

Les principales raisons avancées pour investir dans la sécurité (cf. figure 4) :

1. La protection de personnes
2. La protection de l'infrastructure
3. La protection des informations
4. La protection du produit ou du service

La protection de l'image fait l'objet d'une brève discussion. Dans la SI, cela a été considéré comme un résultat frappant. Il a été indiqué que ce pourcentage est très faible à un moment où les médias et la publicité jouent un rôle central. Les répondants ont probablement fait une distinction entre les raisons principales et secondaires, les raisons principales étant plutôt la protection des personnes, de l'infrastructure, de l'information, des produits ou des services, et l'image n'est prise en compte que dans un second temps. Un participant a estimé que la protection des personnes était logique en raison de la finalité de son secteur, à savoir les soins de santé humaine et les services sociaux. Dans la SI, un partenaire impliqué a déclaré : « *Il est bon que l'on pense davantage aux personnes et à l'information et seulement en dernier lieu à l'image* ».

Les répondants s'accordent à dire que le principal responsable de la sécurité dans l'entreprise est l'employeur. Il a été commenté lors de la SI que ce constat coïncide avec les résultats des premières affirmations (tableau 1), et démontre que le travailleur est de nouveau d'une importance mineure. La fonction occupée par la personne qui répond au questionnaire est tout aussi importante : s'agit-il d'un directeur ou d'un travailleur ? Les questions de base nous apprennent qu'il s'agit dans une large mesure de fonctions dirigeantes.

Un participant a indiqué que les instances publiques jouaient un rôle de premier plan : « *Le gouvernement a donc un rôle important à jouer en matière de sécurité ; il doit accorder une attention suffisante à la sécurité et y consacrer des ressources afin qu'une culture de la sécurité puisse être inculquée à l'organisation, à l'employeur et aux employés. »*. Concernant la police, il a été indiqué que l'on collaborait fréquemment avec les services de police.

« *Le fait que la sécurité privée n'occupe que la sixième place n'est pas si surprenant,* » selon un participant à la SI, « *Le secteur privé est toujours considéré comme le partenaire junior, c'est la mentalité qui prévaut.* ».

4.4 Sûreté IT

93,94% des personnes interrogées ont indiqué que la sûreté IT était importante dans une entreprise. Il a été déclaré durant la session de travail interactive que les petites entreprises étaient plus vulnérables. La raison pour laquelle la sûreté IT est moins prise en considération dans les entreprises de plus petite taille s'explique par :

- Un manque de temps
- Un manque de connaissances
- L'âge : la génération peut jouer un rôle dans l'attention accordée à la sûreté IT.

Au cours de la SI, le pourcentage élevé de répondants indiquant que l'organisation effectue régulièrement des back-ups s'explique par le fait que la plupart des systèmes effectuent automatiquement des sauvegardes. Les participants à la SI ont se sont indignés du fait que 30 % des répondants ont indiqué qu'ils n'étaient pas sensibilisés. Cela est conforme aux réponses aux affirmations précédentes, selon lesquelles il a été indiqué que la sensibilisation était limitée. Cependant, il est crucial que ces 10 mesures s'appliquent à tous les employés et, par conséquent, que l'employé soit également responsabilisé dans ce domaine. Il a été avancé dans la SI qu'il fallait établir une distinction claire entre les grandes et les petites entreprises en termes de sûreté IT.

Enfin, un participant a déclaré que la réglementation GDPR peut expliquer pourquoi plus d'entreprises sont concernées par la sûreté IT.

4.5 Sûreté physique et organisationnelle

Les formes de sûreté physique et organisationnelle ont été discutées au cours de la SI, lors de laquelle il a été indiqué que les formes de sûreté les plus courantes sont aussi celles qui peuvent le mieux être mises en œuvre. Cependant, il est également possible que ces formes soient faciles à manipuler. En ce sens, il faudrait investir davantage dans une sûreté plus difficile à manipuler ou opter pour une combinaison de plusieurs techniques. L'importance de la sensibilisation et de l'implication de tous les employés dans la sûreté a été une fois de plus soulignée.

Les chiffres sur le contrôle préalable à l'emploi ont également fait l'objet d'une discussion lors de la SI. Par exemple, il a été avancé que de tels contrôles préalables sont obligatoires dans certains secteurs, par exemple pour obtenir un permis, et qu'il faut parfois un certificat de bonne vie et mœurs pour pouvoir commencer à travailler. Cependant, les employeurs privés n'ont pas toujours accès à toutes les bases de données. L'intensité du contrôle est également mentionnée : s'agit-il d'une sorte de curiosité de la part de l'employeur ou d'un dépistage approfondi ? Certains participants à la SI ont déclaré que de tels examens préalables sont souvent confiés à un organisme privé.

Le pourcentage de contrôle à l'emploi a été considéré comme une suite logique : « *Si l'on effectue un contrôle préalable à l'emploi, l'on réalise également un contrôle à l'emploi ».* La criminalité des travailleurs comme le vol commis par le personnel propre est un réel problème, il est donc logique que de tels contrôles aient lieu.

4.6 Victimisation

4.6.1 **Au cours des 12 derniers mois, les entreprises ont le plus souvent été victimes de cybercriminalité**

Les participants à la SI ont perçu le taux de victimisation de « dommages » comme élevé. L'une des explications possibles était que, dans les grandes entreprises, les différentes formes de dommages devraient être signalées plus souvent. Les grandes entreprises rapportent davantage les dommages encourus, notamment parce qu'elles fonctionnent avec des véhicules de société.

En ce qui concerne la victimisation de « l'agression et de la violence », les internes (leur propre personnel) et les externes (autres) ont été qualifiés d'auteurs. Le nombre d'actes criminels est fonction de la taille de l'entreprise : « *Plus l'entreprise est grande, plus les risques de conflits mutuels sont élevés* ».

Au cours de la SI, une distinction a été établie entre les infractions de « détérioration » et « d'agression, violence » : les dommages peuvent se produire inconsciemment (par exemple, une personne percutant un poteau ou une voiture sans qu'elle ne s'en rende compte), tandis que la violence et l'agression sont des actes conscients commis par leur auteur. En ce sens, ce pourcentage élevé a été considéré comme plus problématique.

Le pourcentage élevé d'agression et de violence a été reconnu par le représentant du secteur de la santé humaine et du travail social. De telles formes de criminalité sont souvent rencontrées dans ce secteur. D'une part, de nombreux endroits de ce secteur sont accessibles au public, ce qui signifie qu'ils sont fréquemment exposés à la violence, aux agressions, aux dommages et à l'accès interdit par des externes. D'autre part, il a été fait mention de violences et d'agressions commises par des patients (voir hôpitaux, maisons de repos, établissements psychiatriques, soins à domicile, aide à domicile, autres organisations du secteur des soins, etc.)

Le pourcentage de victimisation de la criminalité IT était également perçu comme élevé. En associant « l'accès illégal aux systèmes IT » à l' « ingérence dans les données ou systèmes », nous remarquons qu'une entreprise

interroge sur trois en a été victime au cours des 12 derniers mois. De plus, ces chiffres montrent qu'il ne s'agit pas d'une tentative, mais bien un accès effectif : « *On sait que cela s'est effectivement produit dans l'entreprise* ».

Un participant à la SI avance comme explication au pourcentage élevé de victimisation le fait que ce sont principalement des entreprises qui ont été victimes d'actes criminels dans le passé qui remplissent ce type d'enquêtes : « Ces baromètres sont plus susceptibles d'être remplis par des personnes impliquées ou concernées par ce problème ».

Dans la SI, les pourcentages de trafic et de traite des êtres humains étaient considérés comme faibles, bien que l'on ait enregistré un certain nombre de cas ces dernières années/mois. Cela peut s'expliquer par le fait que l'accent a été mis principalement sur les affaires internationales, qui ne concernent que des activités à l'étranger et non en Belgique.

D'éventuelles divergences d'interprétation ont été évoquées dans le cas des dommages causés aux véhicules. Par exemple, la question a été posée de savoir si nous pouvions également parler de dommages dans le contexte de la circulation (accident par exemple).

Durant la SI, la définition du caractère « marquant » des actes criminels a été évoquée : « Est-ce marquant pour l'entreprise ou pour le répondant qui remplit le baromètre ? » Dans ce contexte, il est important de quantifier les faits : « Plus il y a de cas personnels, plus ils sont marquants pour l'entreprise ».

Au cours de la SI, des questions se sont également posées sur le nombre de cas d'accès interdit : s'agit-il systématiquement d'un accès interdit à l'entreprise, est-ce organisé ou s'agit-il plutôt d'une disparition accidentelle ? Enfin, l'impact de la cybercriminalité a également été considéré comme frappant, quoique pas illogique.

4.6.2 Un tiers des répondants ne portent pas plainte à la police

La propension des entreprises à porter plainte a également fait l'objet de discussions. Le fait d'éviter les faits à l'avenir est la principale raison pour laquelle il faut les signaler, et le fait de les signaler a également un caractère symbolique important, comme dans le cas de l'agression et de la violence : « *Nous indiquons à la victime que nous prenons ce fait au sérieux* ». Plusieurs participants à la SI établissent un lien entre les chiffres au niveau la plainte et la compagnie d'assurance : la compagnie d'assurances n'intervient que si la plainte est déposée.

Le baromètre montre qu'environ 30% n'ont pas déclaré l'incident à la police. Au cours de la séance de travail interactive, il a été suggéré que le rapport soit présenté à d'autres secteurs, tels que le secteur privé. D'autres facteurs expliquent également pourquoi les victimes ne signalent pas les faits : cela crée une charge administrative supplémentaire, le cas est résolu en interne ou, si le patient est l'auteur du crime, il n'est pas toujours considéré comme l'auteur du crime. La relation patient-infirmier peut être un facteur explicatif pour ne pas indiquer certains faits. Certains soignants y voient une partie de leur travail (voir établissement psychiatrique, service de démence dans la maison de repos...) dans laquelle l'expérience personnelle de l'aidant joue un rôle important : ai-je été victime ou non de menaces, de violence, d'agression ? Le secteur des soins de santé humaine et des services sociaux peut être considéré comme un secteur dans lequel les fournisseurs de services sont exposés à de nombreuses vulnérabilités. Cela exige une attention particulière.

De plus, il a été mentionné qu'il est important d'avoir un aperçu des faits et de faire ensuite le lien avec la question de savoir s'il faut ou non signaler ces faits. Il a également été indiqué qu'il faudrait encourager et simplifier le signalement des infractions, car la police n'accorde pas suffisamment d'attention à la criminalité des entreprises.

Un participant à la SI déclare que les résultats de la plainte doivent être examinés au cas par cas : « Est-il vrai que la violence et l'agression sont déclarées plus que le vol de marchandises ? »

4.6.3 Caractéristiques de l'acte criminel

La question a été posée de savoir quelles étaient les autres conséquences du procès-verbal du fait « le plus marquant ». 38,57 % ont déclaré que l'affaire était toujours en cours de traitement et 30 % ont dit qu'ils ne savaient pas. Le pourcentage de « toujours en cours de traitement » a été considéré comme un résultat

logique au sein de la SI, car ce baromètre a été utilisé pour sonder des faits qui avaient eu lieu au cours des 12 derniers mois. Certains ont répondu « je ne sais pas », ce qui peut également indiquer que l'affaire est toujours en cours de traitement et que l'issue n'est pas encore connue. La réponse « Je ne sais pas » était également considérée comme allant de soi dans le contexte des grandes entreprises, car elles ne sont pas toujours informées. Le pourcentage de condamnations a été considéré comme faible et, selon certains, confirme le stéréotype de l'impunité : « Ce que les gens pensent est donc vrai ».

Enfin, la question des dommages a été abordée lors de la SI. Il a été souligné que les dommages mentaux peuvent être importants mais pas toujours faciles à exprimer. L'impact sur l'activité opérationnelle peut être important parce que les employés peuvent devenir inaptes. De plus, il peut y avoir des dommages indirects, ce qui signifie que quelqu'un doit être réembauché.

5. Quelques considérations critiques et recommandations

Ce rapport présente un certain nombre de tendances en matière de sécurité dans les entreprises. Le baromètre, qui génère également des données chiffrées sur l'évaluation des risques et la victimisation des entreprises baromètre, permet d'objectiver certaines hypothèses.

Le fait que de nombreuses entreprises, y compris les PME, soient concernées par la sûreté, est considéré comme une tendance positive. Néanmoins, elles restent nombreuses à être encore insuffisamment préparées à la criminalité : absence de politique ou de mesures, peu de tests ou de contrôles, sentiment d'être insuffisamment préparé à d'éventuels incidents de sécurité... Dans ce contexte, quelques considérations et recommandations critiques sont formulées. Nous concluons en énonçant un programme en 20 points.

Tout d'abord, la responsabilité de chacun est mise en avant : chacun est responsable de la sécurité dans l'entreprise. La responsabilité de la sécurité incombe donc à la fois à l'employeur et à l'employé.

La cybercriminalité est et demeure un sujet d'une importance capitale. Dans le baromètre, elle n'est pas seulement perçue comme un risque majeur, mais 42,6% des entreprises ont également été effectivement victimes, au cours des 12 derniers mois, de l'une des cinq formes de cybercriminalité étudiées. Il faut accorder plus d'attention à la sensibilisation et à la prévention. En outre, les petites entreprises doivent prêter une attention particulière à cette forme de criminalité. Les règles empiriques - comme le changement rapide de mots de passe - doivent être davantage diffusées. S'il s'avère qu'un tiers d'entre elles ont été victimes de phishing au cours des 12 derniers mois, il est essentiel de réagir promptement et que de mener des campagnes de prévention en conséquence.

Outre la cybercriminalité, les dommages causés à un véhicule ou à des propriétés, la violence et les agressions apparaissent également comme des faits qui ont touché environ 40 % des entreprises interrogées au cours des 12 derniers mois. De tels faits peuvent avoir un impact particulièrement significatif sur une entreprise ou un employé de l'entreprise. Les crimes de violence et d'agression sont considérés comme les plus marquants : ils peuvent causer une grande blessure sur le plan personnel, mais n'ont pas nécessairement d'impact majeur sur l'entreprise. Néanmoins, il convient d'y veiller en créant un point de contact au sein de l'entreprise, en reconnaissant les victimes et en offrant un soutien en cas de victimisation, en encourageant et en supervisant la plainte...

Près d'un quart des entreprises victimes d'une forme de criminalité ont porté plainte à la police. Les raisons avancées pour ne pas avoir porté plainte étaient : « parce que cela ne donne de toute façon aucun résultat » et « parce que nous connaissons l'auteur ». Le dépôt de plainte doit être encouragé. Un investissement supplémentaire est nécessaire pour donner des conseils sur ce qui peut être dénoncé et ce qui ne peut pas, sur comment dénoncer un fait et où le faire.

Une politique de sécurité adéquate et une bonne sécurité dans une entreprise ont une fonction externe et interne importante. Cela montre au monde extérieur comment une entreprise traite les facteurs potentiellement menaçants d'une manière professionnelle. Cela montre aussi qu'en tant qu'entreprise, l'on assume sa responsabilité sociale. Cela protège et améliore l'image de l'entreprise et encourage le personnel à continuer à travailler pour l'entreprise plus longtemps. (Agence européenne pour la sécurité et la santé au travail, 2008). Il s'agit d'une donnée capitale dans une société où le « *job hopping* » gagne en importance (LiveCareer, 2018).

Enfin, voici quelques conseils pour se protéger en tant qu'entreprise (Tolsma, 2011 ; Korthals Altes & Armstrong, 2017 ; SPF Economie, 2017).

Vaut mieux prévenir que guérir…

1. Tout le monde (aussi bien l'employeur que le travailleur) est responsable de la sécurité.
2. Conscientiser tous les acteurs au sein de l'entreprise aux dangers et aux procédures de sûreté. Beaucoup d'incidents peuvent être évités si l'on sait comment traiter les informations en toute sécurité.
3. Désigner un responsable : une personne chargée en interne de la sécurité dans l'entreprise et qui y veille de manière continue.
4. Identifier et sécuriser les informations capitales.
5. Accorder l'accès aux secrets d'entreprise uniquement à un groupe restreint de collaborateurs.
6. Protéger l'accès aux endroits et données critiques pour l'entreprise.
7. Des exigences en matière de sécurité doivent être définies à l'égard des fournisseurs et des clients importants.
8. Outre une cybersécurité optimale, veiller à une sûreté physique.
9. Utiliser un système de réseau professionnel et moderne.
10. Mettre le logiciel à jour.
11. Choisir des mots de passe très sécurisés.
12. La gestion de l'accès aux ordinateurs est capitale, accorder uniquement l'accès à quelques spécialistes IT.
13. Investir dans des formations, des campagnes de sensibilisation sur la sûreté IT.
14. Surfer sur Internet en toute sécurité.
15. Ne pas accorder une confiance aveugle aux services de stockage ou d'envoi de données, tels que Dropbox ou WeTransfer.
16. Il est primordial de faire des back-ups afin d'éviter de perdre certains programmes ou applications.
17. Penser aussi aux dangers en dehors du réseau de l'entreprise comme les clés USB, les portails USB, les tablettes, les, smartphones et les laptops. Sécuriser donc les appareils mobiles.

Et pour les victimes d'actes criminels…

18. Veiller à un accompagnement interne professionnel de la victime.
19. Prendre la victime au sérieux, avoir une oreille attentive et éviter une victimisation secondaire.
20. Déposer plainte à la police.

6. Bibliographie

Algemeen Dagblad (2019). *Weinig zicht op slachtoffers van mensenhandel en uitbuiting.* Retrieved from https://www.ad.nl/binnenland/rapport-weinig-zicht-op-slachtoffers-van-mensenhandel-en-uitbuiting~a5e40067/

Allianz Risk Barometer (2018). Retrieved from https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2018.html [Mei 2018]

Bafort, T. (2016). *Screening van werknemers*. Retrieved from https://lib.ugent.be/fulltxt/RUG01/002/304/239/RUG01-002304239_2016_0001_AC.pdf [Maart 2019]

Belga (2016). *Banden tussen drugshandel en terrorisme worden steeds sterker*. Retrieved from https://www.hln.be/nieuws/buitenland/banden-tussen-drugshandel-en-terrorisme-worden-steeds-sterker~a76e99d2/ [Maart 2019]

Belga (2018). *België en Nederland vormen één drugsmarkt: dus nood aan één aanpak*. Retrieved from https://www.hln.be/nieuws/binnenland/-belgie-en-nederland-vormen-een-drugsmarkt-dus-nood-aan-een-aanpak~a0445397/ [Maart 2019]

Cybersecurity strategy research: Common tactics, issues with implementation, and effectiveness. Tech Pro Research. Retrieved from http://www.techproresearch.com/downloads/cybersecurity-strategy-research-common-tactics-issues-with-implementation-and-effectiveness/ [April 2018]

De Tijd (2018). *Ruim derde van bedrijfsfraude gepleegd door eigen personeel*. Retrieved from https://www.tijd.be/ondernemen/algemeen/ruim-derde-van-bedrijfsfraude-gepleegd-door-eigen-personeel/10068628.html [Maart 2019]

Europees Agentschap voor veiligheid en gezondheid op het werk (2008). *De voordelen van goede veiligheid en gezondheid op het werk voor bedrijven*. Retrieved from https://osha.europa.eu/sites/default/files/publications/documents/nl/publications/factsheets/77/Factsheet_77_-_De_voordelen_van_goede_veiligheid_en_gezondheid_op_het_werk_voor_bedrijven.pdf [Maart 2019]

Europees Parlement (2018). *Terrorisme in de EU : terreuraanslagen, sterfgevallen en arrestaties*. Retrieved from http://www.europarl.europa.eu/news/nl/headlines/security/20180703STO07125/terrorisme-in-de-eu-terreuraanslagen-sterfgevallen-en-arrestaties [Maart 2019]

Federale overheidsdienst (2017). *Maak uw bedrijf cyberveilig in 10 stappen*. Retrieved from https://news.economie.fgov.be/163055-een-cyberveilig-bedrijf-in-10-stappen [April 2018]

Federale Politie (2018). *Tendensen 2016-2017. Politiële criminaliteitsstatistieken*. http://www.stat.policefederale.be/assets/pdf/notas/tendensen_2016_2017_PCS.pdf [Oktober 2018]

Guinevere, J. (2010). *Een kwantitatieve analyse van werknemerscriminaliteit in de bedrijfswereld*. Retrieved from https://lib.ugent.be/nl/catalog/rug01:002049471 [Maart 2019]

Hoeffnagel, W. (2016). *Inzetten op IT-beveiliging is nodig om boetes en reputatieschade te voorkomen*. https://dutchitchannel.nl/546429/managers-vinden-it-afdeling-verantwoordelijk-voor-it-beveiliging.html [Maart 2019]

ICT Security in enterprises. Eurostat: Security policy: risks addressed and staff awareness. Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises^ [April 2018]

Korthals Altes, J. & Armstrong, T (2017). *Tien tips om je onderneming beter te beveiligen tegen cybercriminaliteit*. Retrieved from https://mkbgroeit.nl/10-tips-om-onderneming-beter-beveiligen-cybercriminaliteit/ [Maart 2019]

LiveCareer (2018). *Job hopping analysis: trends by generation & education level.* Retrieved from https://www.livecareer.com/wp-content/uploads/2018/05/2018-Job-Hopping-Report.pdf [Maart 2019]

Smets, L., De Kinder, J., & Moor, L. G. (2011). *Proces-verbaal, aangifte en forensisch onderzoek*. Cahiers Politiestudies, 4, Nr. 21.

Techzine (2018). *Middelgrote bedrijven moeten anticiperen op toenemende risico's Industrie 4.0*. Retrieved from https://www.techzine.be/blogs/22957/middelgrote-bedrijven-moeten-anticiperen-op-toenemende-risicos-industrie-4-0.html [Maart 2019]

Tolsma, J. (2011). *Aangiftebereidheid: Welke overwegingen spelen een rol bij de beslissing om wel of niet aangifte te doen*. Proces-verbaal, aangifte en forensisch onderzoek. Cahiers Politiestudies, 21, 11-32.

UNIZO (2016).UNIZO KMO cijfers, September 2016.

van Dijk, JJM, Tseloni, A. & Farrell, G. (Eds.) (2012). *The International Crime Drop: New Directions in Research. Basingstoke: Palgrave Macmillan; Farrell: Five tests for a theory on the crime drop*. Crime Science 2013 2:5

Veilige buurt (2017). *Lage aangiftebereidheid in 2017*. Retrieved from https://veiligebuurt-.nl/nieuws/aangiftebereidheid-erg-laag/ [Maart 2019]

Veiligheidsladder. Retrieved from http://www.veiligheidsladder.org/wp-content/uploads/2016/06/Certificatieschema_Veiligheidsladder_4.0-final.pdf) [April 2018]

Veiligheidsklimaat. Retrieved from (https://blog.sbo.nl/veiligheid/de-menselijke-factor-praktijkervaring-met-de-barometer-veiligheidsklimaat/) [April 2018]

Versteegh, P. (2007). *Haaldelicten en brengdelicten*. Secondant, 3, 68-71.

World Economic Forum (2018). *The global risks Report 2018. 13the Edition*.

Vias institute cvba - vso • Institut Vias scrl - fs
Haachtsesteenweg 1405, 1130 Brussel • Chaussée de Haecht 1405, 1130 Bruxelles • +32 2 244 15 11 • info@vias.be • www.vias.be • BE 0432.570.411