HISCOX
ASSURANCES

Rapport Hiscox 2021 sur la gestion des cyber-risques

Cyber-résilience: Ne jouez pas l'avenir de votre entreprise aux dés !

Les cyber-risques sont trop importants pour être laissés au hasard.

Parmi les entreprises attaquées l'an dernier, une sur six a déclaré avoir risqué de peu la faillite. La menace est complexe. Mais, comme tous les autres risques de l'entreprise, elle peut être gérée. La clé est de renforcer la cyber-résilience.

Évaluez la résilience de votre entreprise grâce à notre modélisation de la maturité accessible à l'adresse hiscoxgroup.com/cyber-maturity.

Gérer la cyber-menace

Les entreprises consacrent toujours plus de ressources à la lutte contre la cyber-menace.

Gareth Wharton
Cyber CEO, Hiscox

Davantage d'entreprises ciblées, souvent à plusieurs reprises.

Le rapport de cette année met en lumière l'ampleur de la cyber-menace. Mais il apporte également son lot de bonnes nouvelles. Malgré les difficultés liées à la pandémie de Covid-19, les entreprises ont intensifié leur riposte en mobilisant plus de ressources et d'attention que jamais en faveur de la cyber-résilience. Au début de la pandémie, la poursuite de l'activité était la priorité n° 1 pour la majorité des entreprises. En raison du resserrement des budgets informatiques, on craignait que les dépenses de cybersécurité ne s'en trouvent réduites. Notre rapport montre qu'il n'en a pas été ainsi. Les dépenses liées à cybersécurité ont augmenté.

La prévalence croissante des ransomwares devrait faire prendre conscience de la pertinence d'une bonne gestion de la cybersécurité au niveau commercial. Les attaques par ransomware ne sont pas simplement des événements informatiques, ils impactent l'entreprise à plusieurs niveaux. La cybersécurité constitue sans aucun doute un problème complexe, mais cela ne signifie pas que ce problème n'est pas maitrisable. Aujourd'hui, le risque est tellement élevé et palpable que les entreprises et les particuliers ne peuvent plus l'ignorer en se retranchant derrière la difficulté. Le risque qu'une seule attaque puisse mettre en danger l'ensemble de l'entreprise est réel. Parmi les entreprises ciblées l'année dernière, une sur six a déclaré qu'une attaque avait menacé la viabilité de ses activités. Des mesures simples et concrètes peuvent permettre d'atteindre un niveau de cyber-résilience diminuant le risque d'attaques. Si une attaque se produit, votre entreprise disposera alors de la formation, des outils et de la protection financière pour y parer.

En tant qu'ancien directeur de la technologie, je me suis toujours demandé « comment font nos concurrents ? » et « comment pouvons-nous nous comparer à eux ? ». L'innovation cette année est d'avoir centré le rapport autour d'une nouvelle modélisation des capacités de gestion des cyber-risques qui évalue les forces des participants de l'étude dans six domaines clés de la cybersécurité axés sur les personnes, processus et technologies. Elle est conçue comme une modélisation interactive vous permettant d'évaluer et de comparer la maturité de votre entreprise à celle d'autres entreprises implantées dans votre pays, exerçant dans votre secteur d'activité et réalisant un chiffre d'affaires semblable. La modélisation de la maturité illustre ce que les experts de la cybersécurité font dans chaque domaine pour vous aider à planifier et à renforcer votre cyber-résilience.

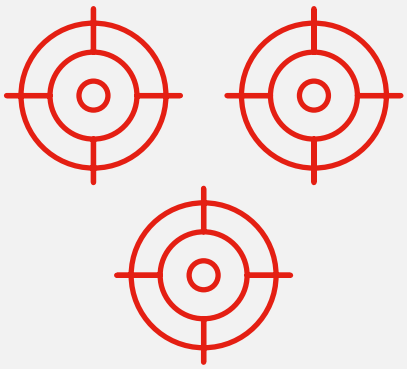
Notre expérience en tant qu'assureur a montré qu'il est essentiel de respecter des normes cohérentes dans tous les domaines de la sécurité pour éviter que les pirates ne trouvent un moyen de s'introduire. Nous espérons que cette modélisation vous apportera un regard neuf sur vos mesures en place et qu'elle mettra en lumière d'éventuels axes d'amélioration.La cyber-menace ne va pas disparaitre, mais grâce à une bonne gestion des risques, complétée par une police de cyber-assurance adaptée, les entreprises peuvent contenir son impact et minimiser les dommages. Notre objectif est que ce rapport permette aux entreprises de mieux comprendre la cyber-menace, qu'il leur fournisse un modèle de bonnes pratiques et qu'il les aide à se préparer et à faire face aux défis auxquels elles seront confrontées.

Résumé

Les entreprises concentrent leurs dépenses informatiques sur la cyber-résilience pour faire face à la hausse des attaques.

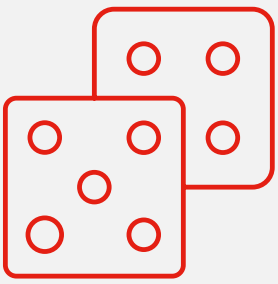
Davantage d'entreprises ciblées

La proportion d'entreprises attaquées est passée de 38% à 43%. Beaucoup ont subi de multiples attaques.



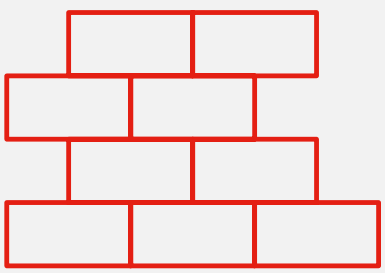
L'éventail inquiétant des conséquences

Le coût des attaques varie nettement. Parmi les entreprises victimes d'une attaque, une sur six a déclaré que sa survie était menacée.



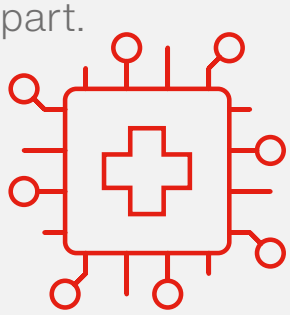
Les budgets informatiques se réorientent vers la cybersécurité

En moyenne, les entreprises consacrent désormais plus d'un cinquième (21%) de leur budget informatique à la cybersécurité, ce qui représente un bond de 63%.



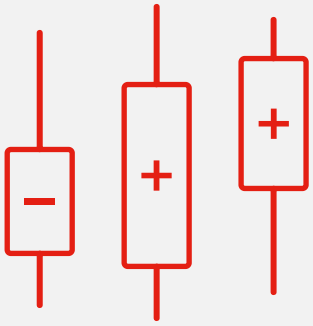
Les ransomwares sont désormais monnaie courante

Près d'un sixième des entreprises victimes d'une attaque ont reçu une demande de rançon et plus de la moitié l'ont versée. Les emails de phishing ont constitué le principal point de départ.



Personnes, processus et technologies

Notre modélisation des capacités de gestion des cyber-risques montre que les scores relatifs aux personnes sont plus faibles que ceux des deux autres catégories.

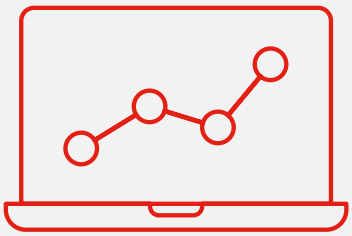


Les entreprises « expertes » s'en sont mieux sorties

Les entreprises classées expertes ont subi moins d'attaques par ransomware, elles ont été moins nombreuses à verser des rançons et se sont rétablies plus rapidement.

Lente progression des souscriptions d'assurance

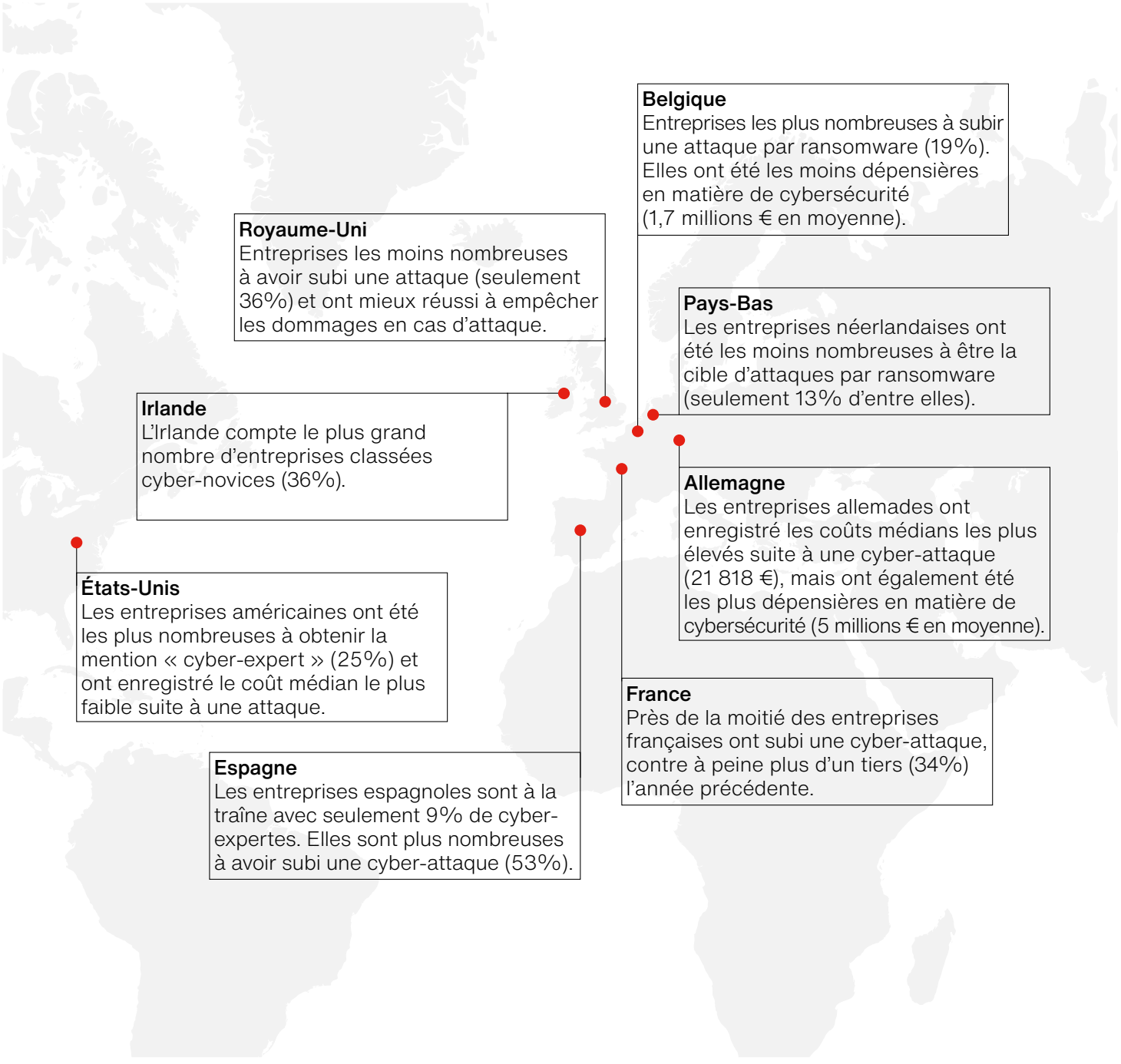
La souscription d'une garantie des cyber-risques dédiée progresse à peine, de 26% à 27%. La souscription de ce type de garanties est plus importante parmi les expertes et les grandes entreprises.



Grande disparité entre les pays

Les entreprises américaines sont les plus représentées parmi les expertes, les entreprises espagnoles sont les plus fortement ciblées et les allemandes paient le plus lourd tribut.

Comparaison par pays



Belgique
Entreprises les plus nombreuses à subir une attaque par ransomware (19%). Elles ont été les moins dépensières en matière de cybersécurité (1,7 millions € en moyenne).

Royaume-Uni
Entreprises les moins nombreuses à avoir subi une attaque (seulement 36%) et ont mieux réussi à empêcher les dommages en cas d'attaque.

Pays-Bas
Les entreprises néerlandaises ont été les moins nombreuses à être la cible d'attaques par ransomware (seulement 13% d'entre elles).

Irlande
L'Irlande compte le plus grand nombre d'entreprises classées cyber-novices (36%).

Allemagne
Les entreprises allemades ont enregistré les coûts médians les plus élevés suite à une cyber-attaque (21 818 €), mais ont également été les plus dépensières en matière de cybersécurité (5 millions € en moyenne).

États-Unis
Les entreprises américaines ont été les plus nombreuses à obtenir la mention « cyber-expert » (25%) et ont enregistré le coût médian le plus faible suite à une attaque.

France
Près de la moitié des entreprises françaises ont subi une cyber-attaque, contre à peine plus d'un tiers (34%) l'année précédente.

Espagne
Les entreprises espagnoles sont à la traîne avec seulement 9% de cyber-expertes. Elles sont plus nombreuses à avoir subi une cyber-attaque (53%).

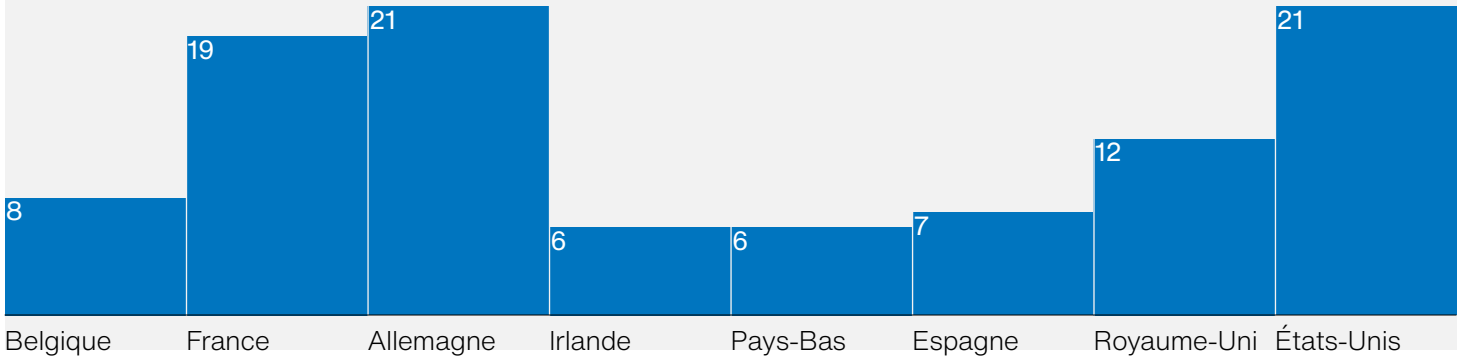
En chiffres

Pourcentage des dépenses informatiques alloué à la cybersécurité

(%)

Ont versé une rançon

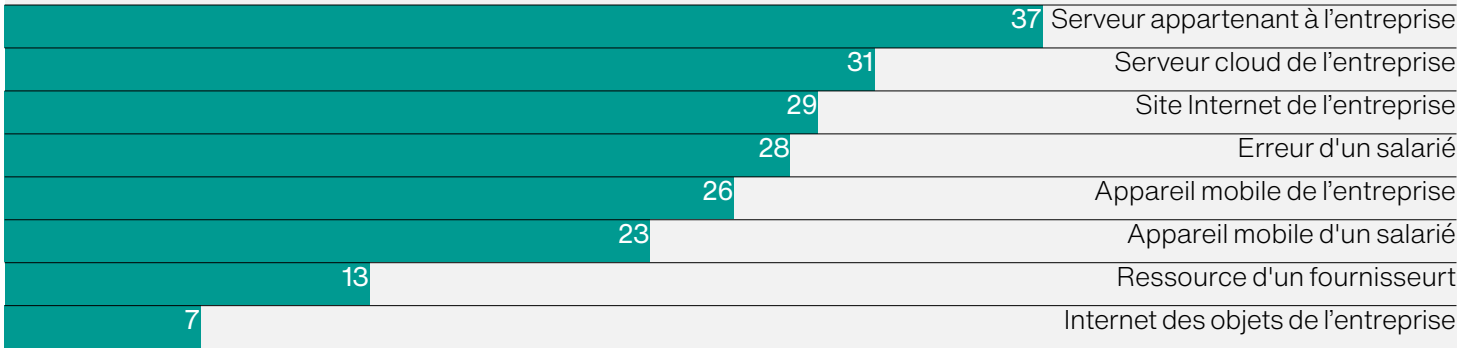
(%)



Premier point d'entrée en cas de cyber-attaque

Réponse à choix multiples

(%)



Étendue du problème

Les entreprises sont beaucoup plus nombreuses à rapporter des cyber-attaques, alors que la menace s'intensifie dans les principaux secteurs cibles.

Nous avons enregistré une nette augmentation du nombre d'entreprises ayant signalé une ou plusieurs cyber-attaques cette année, les pirates concentrant leurs efforts sur trois ou quatre secteurs en particulier et ciblant beaucoup plus largement les grandes entreprises.

Qui a été le plus attaqué ?
Le nombre de participants ayant rapporté des attaques a bondi de 38% en 2020 à 43% cette année. Les technologies, médias et télécommunications (TMT) ; les services financiers et les secteurs de l'énergie ont constitué les cibles privilégiées des pirates. Le nombre d'entreprises touchées dans ces secteurs, qui s'étalait entre 40% et 44% l'an passé, se situe désormais autour de 55% (voir Fig. 1).

Cette année encore, de nombreuses grandes entreprises ont été ciblées. Comme les rapports précédents l'ont relevé, la probabilité de subir une attaque augmente fortement en fonction de la taille des entreprises. Cette année, la tendance a été encore plus marquée : de 23% pour les plus petites entreprises à 61% pour les très grandes entreprises (1 000 salariés et plus). L'an dernier, les chiffres correspondants étaient de 31% pour les petites entreprises contre 51% pour les très grandes entreprises.

Dans l'ensemble, les entreprises espagnoles ont été les plus nombreuses à rapporter une cyber-attaque (53%). Près de la moitié des participants français (49%) ont signalé une attaque, contre 34% l'année précédente. À titre de comparaison, seules 36% des entreprises britanniques ont indiqué avoir été ciblées.

Les entreprises sont nombreuses à avoir subi plusieurs attaques
Plus d'un quart (28%) des entreprises victimes de cyber-attaques ont été ciblées plus de cinq fois au cours de l'année passée. Près de la moitié (47%) des très grandes entreprises attaquées ont dû lutter contre des pirates six fois ou plus. Un tiers d'entre elles (33%) ont subi plus de 25 attaques. Plus d'un cinquième (22%) des entreprises françaises et allemandes ciblées ont subi plus de 25 attaques.

Fig. 1. Top cinq des secteurs ayant signalé au moins une cyber-attaque
(%)

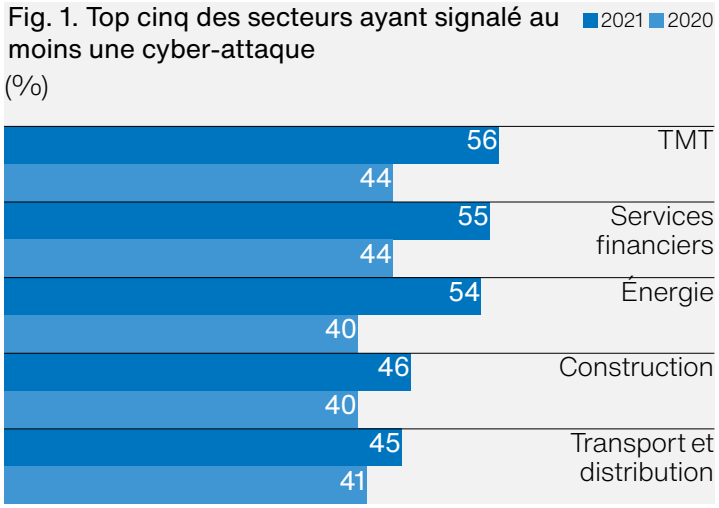


Fig. 2. Nombre d'attaques l'an dernier (parmi les entreprises ayant rapporté au moins une attaque)
(%)

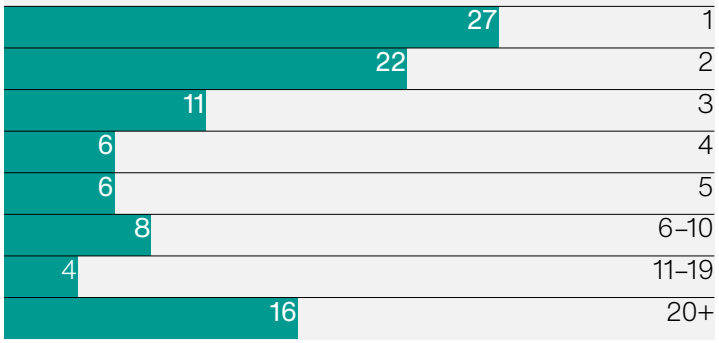
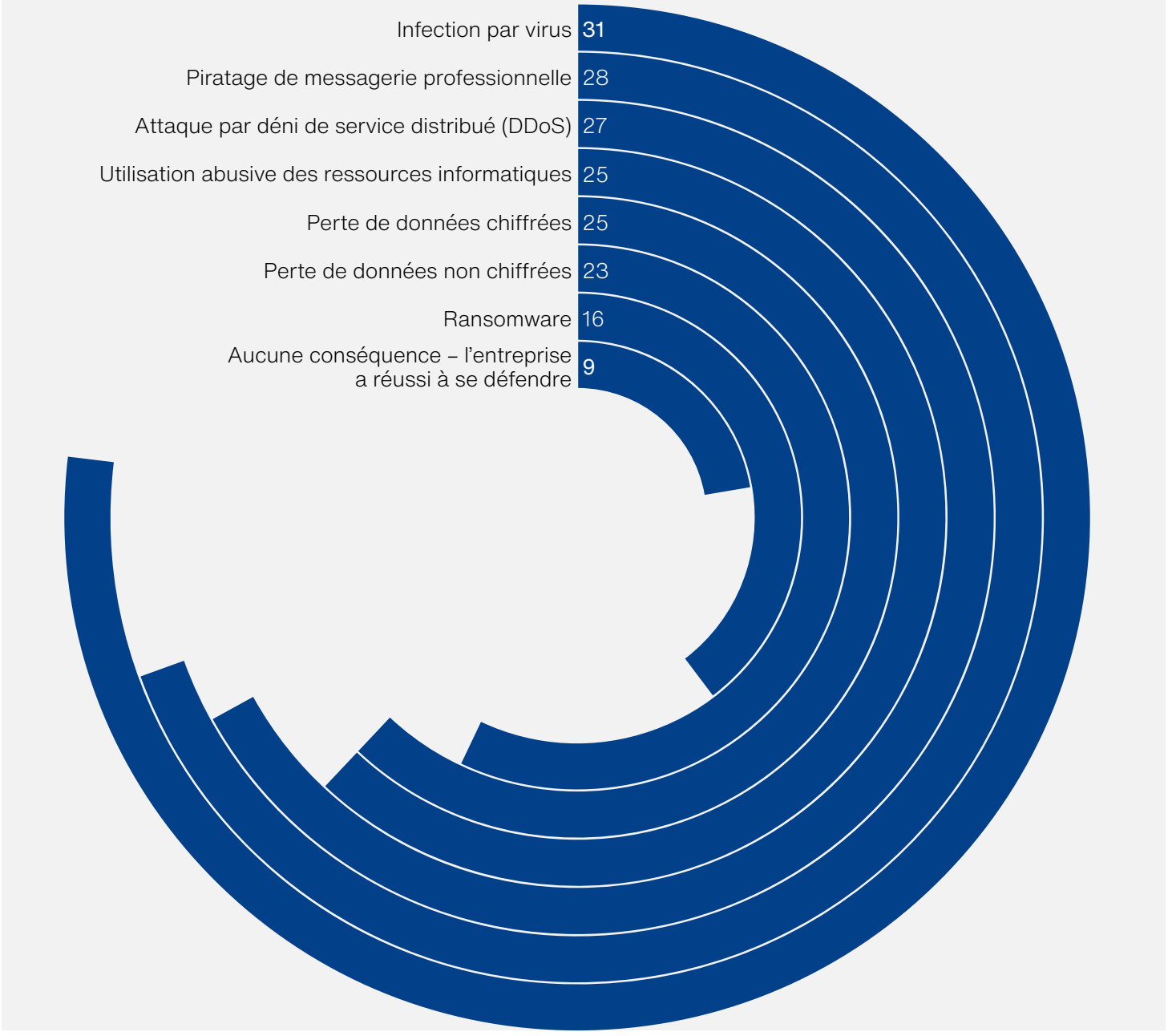


Fig. 3. Conséquences des cyber-attaques

Réponse à choix multiples

(%)



Le point de vue d'Hiscox

Les grandes entreprises sont-elles simplement meilleures pour détecter les attaques ? Il convient en d'observer que les entreprises ayant obtenu la mention « cyber-intermédiaire » ou « cyber-expert » dans notre modélisation des capacités de gestion des cyber-risques ont été plus nombreuses à signaler de multiples attaques. En 2020, des entreprises de toutes tailles ont développé leur activité en ligne en ligne et développé le télétravail pour leurs salariés. Les ports RDP ouverts ont constitué 61% des déclarations de sinistre auprès d'Hiscox concernant des attaques par ransomware en 2020. Il s'agit en partie des causes des multiples attaques.

Les entreprises ont eu à faire face à une grande variété d'attaques.

Trois entreprises ciblées sur dix (31%) ont du faire face à un infection par virus (hors ransomware), 28% à un piratage de messagerie professionnelle et 27% à une attaque par déni de service distribué ou DDoS - Distributed Denial of Service (voir Fig. 3.). Les entreprises allemandes, françaises et américaines ont été les plus susceptibles de subir ces attaques.

A noter que, 39% des entreprises américaines – contre 25% au global – ont eu à faire à un détournement d'usage de ressources IT, comme l'hébergement d'un malware ou le piratage de l'infrastructure pour développer de la cryptomonnaie.

Chercher la faille

Si vous oubliez de verrouiller une porte ou une fenêtre, les cambrioleurs la trouveront. À la question de savoir quel est le premier point d'entrée des pirates, 37% des personnes interrogées ont mentionné leur propre serveur d'entreprise. Les serveurs situés sur le cloud ont été cités en deuxième position (par 31% des participants), suivent les sites Internet des entreprises (29%) et les erreurs des salariés découlant d'une attaque par phishing ou d'une usurpation d'adresse email (28%). L'année précédente, le phishing était clairement le problème n°1, cité par 45% des participants. L'étude de cette année a offert aux participants la possibilité de choisir parmi un éventail plus large de réponses.

Il existe néanmoins de grandes disparités selon les secteurs : si les entreprises des secteurs des services professionnels, de la construction et des services financiers ont été nombreuses à citer le serveur d'entreprise comme point d'entrée, les entreprises en relation avec le public, notamment dans les secteurs de la vente au détail et en gros et de l'énergie, ont pour beaucoup subi une faille via leur site Internet. Les appareils mobiles appartenant à l'entreprise, mentionnés par à peine plus d'un quart des entreprises attaquées (26%), semblent constituer des points de vulnérabilité particuliers pour de plus en plus d'entreprises des secteurs mobiles tels que les transports/la distribution et les voyages/loisirs (mentionnés respectivement par 32% et 30% des entreprises de ces secteurs).

Les petites entreprises de 10 à 49 salariés semblent particulièrement sensibles à la vulnérabilité des serveurs ou au piratage d'identifiants (mentionnés par 41% de ces entreprises contre 37% en moyenne), mais il est étonnant de constater que les très grandes entreprises ont également massivement mentionné ces deux points d'entrée. Les données suggèrent que l'investissement dans un site Internet sophistiqué peut être contre-productif : les plus grandes entreprises de notre panel d'étude sont beaucoup plus nombreuses à avoir subi une attaque via leur site Internet (comme une attaque par déni de service distribué).

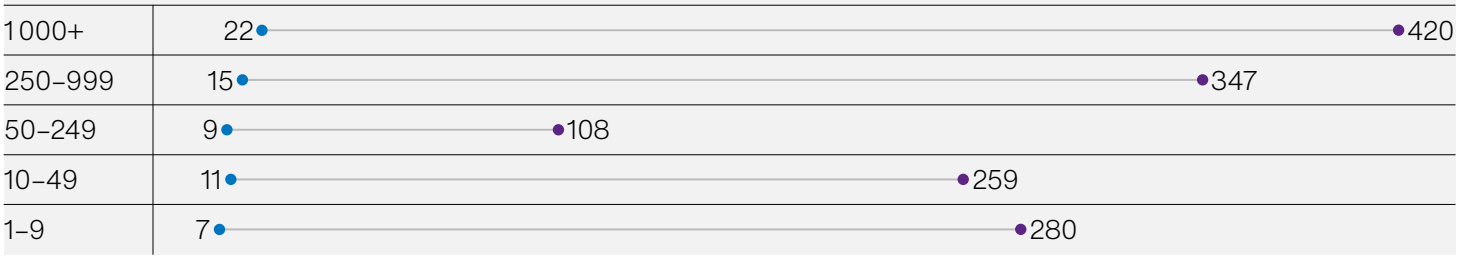
Les entreprises classées expertes semblent avoir connu les mêmes vulnérabilités que les autres. Il convient de relever que 44% des expertes ont mentionné leur propre serveur d'entreprise comme premier point d'entrée des pirates, contre 37% de l'ensemble du panel d'étude. Le site Internet de l'entreprise est également mentionné par 36% des expertes.

Les entreprises allemandes doivent s'améliorer dans presque tous ces domaines. Par exemple, elles sont respectivement 44% et 41% à avoir répondu qu'un serveur appartenant à l'entreprise ou un serveur cloud (impliquant soit une vulnérabilité directe du serveur soit un piratage d'identifiants) avait constitué le premier point d'entrée des pirates. Les entreprises américaines semblent avoir été particulièrement vulnérables face à la plupart de ces problématiques.

Coûts financiers

Le large éventail de conséquences accentue la cyber-menace.Il est facile de négliger la portée complète des données relatives aux coûts des cyber-attaques. Si l'on regarde seulement les chiffres moyens ou médians, l'impact financier peut sembler maitrisable. Mais derrière ces chiffres, il y a toute une série de conséquences qui devraient donner des sueurs froides à tout chef d'entreprise.

Fig. 4. Étendue des coûts des cyber-attaques
Taille de l'entreprise
(000 €)



Ce qui interpelle le plus en observant le graphique (voir Fig. 4.), c'est la diversité et l'imprévisibilité des conséquences liées à un incident pour chacune des catégories de taille d'entreprise de notre panel. Tenant compte de l'ensemble des cyber-attaques subies au cours des 12 derniers mois, le graphique montre à la fois le coût médian et le coût au 95è percentile de chaque catégorie de taille.

Si les coûts médians peuvent sembler maitrisables, il n'est pas inutile de rappeler ce que la médiane représente. Il s'agit du point central. Tandis que la moitié des entreprises ciblées auront enregistré des coûts inférieurs ou égaux à ce chiffre, l'autre moitié aura subi des pertes plus importantes. Ce que le graphique montre, c'est que l'ordre de grandeur de ces coûts peut être deux, trois ou même quatre fois supérieur.

Les petites entreprises souffrent

Les petites entreprises sont les plus touchées, en ce qui concerne le montant des pertes proportionnellement à la taille de l'entreprise. Pour les micro-entreprises de moins de 10 salariés, le coût médian de l'ensemble des attaques cette année était tout juste supérieur à 7 273 €. Mais au 95ème percentile et au-delà, certaines entreprises ont essuyé des pertes de 280 000 €. Parfois, les conséquences sont encore pires. Une entreprise de services allemande a subi des failles représentant un coût de 430 909 € par salarié.

À l'opposé, la moitié des très grandes entreprises ont réussi à contenir le coût des cyber-attaques à moins de 21 818 €. Mais au 95è percentile, elles ont enregistré des pertes presque 40 fois supérieures. L'impact de telles pertes ne saurait être sous-estimé. Sur l'ensemble des entreprises attaquées cette année, un sixième (17%) ont déclaré que l'impact était suffisamment grave pour « menacer sérieusement la solvabilité/viabilité de l'entreprise ».

Là encore, les entreprises allemandes se distinguent par la gravité des attaques subies. Elles totalisent en effet plus d'un tiers de l'impact financier total, soit 43,5 millions €, dont la moitié pour seulement deux secteurs : le commerce de gros et de détail et la pharmacie/santé. Les entreprises allemandes figurent également dans le haut du tableau pour ce qui concerne le coût médian de l'ensemble des cyber-attaques (21 545 €) et le coût unique de l'attaque la plus importante (4,6 millions €). À l'opposé du spectre, les entreprises irlandaises ont enregistré des coûts médians de seulement 7 545 €.

Les données sur les coûts proviennent de 1 709 entreprises qui ont évalué les coûts des cyber-attaques. Il est encourageant de constater que les entreprises qui mesurent l'impact sont de plus en plus nombreuses. Davantage d'entreprises déclarent qu'elles peuvent désormais « mesurer clairement l'impact sur l'entreprise des incidents de sécurité qui ont perturbé leurs activités » (62% contre 60% l'an dernier et 57% l'année précédente).

Heureusement, les pirates informatiques ne font pas toujours les choses comme ils l'entendent. 9% des entreprises participantes (et 11% des expertes) ont déclaré qu'elles étaient parvenues à repousser ou contrer toutes les attaques dirigées contre elles avant qu'elles ne causent des dommages. Les entreprises britanniques ont été les meilleures dans ce domaine (13%) et les entreprises américaines les moins performantes (à peine 6%). Il est néanmoins utile de préciser que la défense contre les cyber-attaques ou la rectification des problèmes engendrent toujours des coûts très importants. Dans l'ensemble, le coût médian n'a été que marginalement inférieur au coût subi du fait d'une attaque réussie. Rien n'est gratuit !

La réputation de la marque est en jeu

L'effet d'une faille importante va bien au-delà des coûts financiers immédiats. Près d'un quart des entreprises attaquées (23%) ont mentionné la mauvaise publicité et son impact sur l'image de marque et la réputation de la société. Ce chiffre est en forte augmentation par rapport à l'année dernière (14%). Sans surprise, les très grandes entreprises, qui pour beaucoup d'entre elles ont des marques internationales, ont été plus nombreuses à signaler un impact sur leur réputation.

Les entreprises en relation avec le public ont été les plus touchées (28% des entreprises de voyages et loisirs et 25% des entreprises du secteur de l'agro-alimentaire). 23% des personnes interrogées ont en outre pointé l'augmentation des coûts liés à la notification des clients.

€6,6m

Somme totale versée par les 241 entreprises ayant payé une rançon.

Il semble donc pertinent que l'une des principales mesures que les entreprises expertes se sont imposées cette année soit « l'amélioration de la sécurité des services et applications destinés aux clients ».

Plus d'un dixième des entreprises ciblées (11%) ont dû s'acquitter d'une « amende conséquente ayant eu un impact important sur la santé financière de l'entreprise ». Aux États-Unis, ce chiffre était de 18%, laissant penser que les réglementations strictes des principaux États impliquant des pénalités en cas de violation de données, comme le California Consumer Privacy Act (Loi californienne sur la protection des données des clients, CCPA) ont eu un impact. Le nombre d'entreprises ayant perdu des clients a bondi de 11% à 19%. Elles sont presque aussi nombreuses (18%) à avoir fait mention de difficultés accrues pour attirer de nouveaux clients, contre 15% l'année précédente.

Ransomware : un peu plus de la moitié des entreprises ciblés ont versé des rançons

Près d'un sixième (16%) des entreprises ayant fait état de cyber-attaques ont été confrontées à un ransomware. Les entreprises belges et allemandes ont été les plus ciblées (19%) les entreprises néerlandaises les moins ciblées (13%).

Un peu plus de la moitié des entreprises ciblées 58%) ont versé une rançon, soit pour récupérer des données, soit pour empêcher la publication d'informations sensibles. Le pays le plus bénéfique pour les demandeurs de rançon a été les États-Unis, 71% des entreprises américaines ciblées ayant versé une rançon (ce chiffre était encore plus élevé en Irlande, à savoir 75%, mais l'échantillon ne représentait que 20 entreprises et n'était pas statistiquement pertinent). Les entreprises espagnoles ont été les moins enclines à verser une rançon, seules 44% d'entre elles l'ont fait.

Les 241 sociétés qui ont payé une rançon ont versé au total la somme de 6,6 millions €. Le montant médian versé à titre de rançon s'élève à 10 818 € et la rançon la plus importante a été versée par une entreprise allemande (86 273 €). Une entreprise française a versé quasiment la même somme, à quelques dollars près.

Fig. 5. Méthodes de pénétration en cas d'attaque par ransomware
(%)

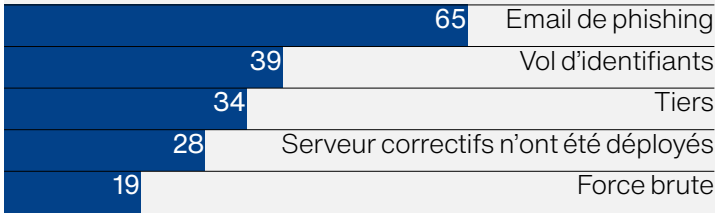
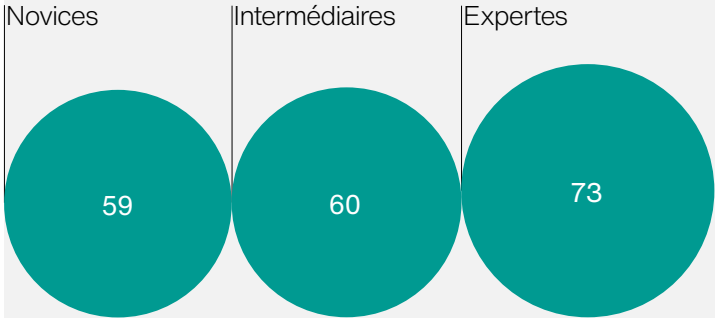


Fig. 6. Retour à la normale en une semaine
(%)



Le point de vue d'Hiscox

Les ransomwares sont sans aucun doute le fléau des activités commerciales en ligne. Des entreprises de toutes tailles sont régulièrement victimes de pirates diffusant des ransomwares. Toutefois, comme notre étude le montre, Les entreprises expertes s'en sortent mieux en cas d'attaque. Elles ont subi moins d'attaques par ransomware, elles ont été moins victimes d'emails de phishing, et lorsqu'elles ont été touchées, elles se sont rétablies plus rapidement. Chez Hiscox, nous prenons les ransomwares très au sérieux. Nos offres sont tout particulièrement conçues pour encourager une bonne protection contre les ransomwares, en encourageant ainsi nos clients à améliorer et préserver leur cyber-résilience.

Un quart des entreprises ayant versé une rançon sont des sociétés du secteur des Technologies – Médias – Télécommunication.

Le montant de la rançon versée n'est qu'une partie du problème. Pour la première fois, nous avons demandé aux participants d'évaluer les coûts de rétablissement induits suite à la plus importante attaque par ransomware et suite à l'ensemble des attaques par ransomware au cours des 12 derniers mois. Les résultats sont particulièrement édifiants : globalement, les frais de rétablissement ont quasiment doublé l'impact financier, représentant 45% du coût total (rançon et rétablissement compris).

Plus de 60% des entreprises ayant versé une rançon sont regroupées dans trois pays : États-Unis (21%), Allemagne (21%) et France (19%). L'Allemagne est à égalité avec la Belgique le pays dans lequel les entreprises rapportant une ou plusieurs attaques par ransomware sont les plus nombreuses (19%).

Les petites entreprises en proie au phishing

Les emails de phishing ont constitué le principal point d'entrée des pirates. Près de deux tiers des victimes de ransomware (65%) ont fait état de ce moyen d'entrée, et encore davantage aux Pays-Bas et en Allemagne (respectivement 76% et 74%). Les petites entreprises ont été en proie au phishing plus souvent que les autres. 74% des entreprises de moins de dix salariés ciblées par un ransomware ont mentionné ce point d'entrée. En comparaison, seules 65% des plus grandes entreprises de notre panel ont cité ce point d'entrée. Le vol d'identifiants et une intrusion du fait d'un fournisseur tiers (ou un prestataire de services d'infogérance) ont été les deux biais suivants les plus cités (mentionnés par 39% et 34% des victimes) (voir Fig. 5).

Les entreprises américaines semblent avoir été particulièrement vulnérables à une pénétration du fait d'un fournisseur tiers/prestataire de services d'infogérance, d'un serveur sur lesquels les correctifs n'ont pas été déployés ou d'un vol d'identifiants.

Lorsqu'ils ont trouvé une cible lucrative, les pirates informatiques reviennent souvent à la charge. Presque 200 entreprises ont ainsi dû verser une rançon aux pirates plus d'une fois. 76 entreprises ont versé entre trois et cinq rançons et 14 entreprises en ont versé cinq ou plus. Un quart des entreprises (27%) ont versé trois rançons ou plus pour récupérer des données et un cinquième (22%) ont versé trois rançons ou plus pour empêcher la publication de données sensibles.

Comment les entreprises expertes s'en sont-elles sorties ?

Dans l'ensemble, très bien. Les entreprises expertes sont moins nombreuses à avoir reçu des demandes de rançon (13% contre 16% pour les novices et 17% pour les intermédiaires) ou à avoir été victimes d'emails de phishing (56% contre 65% en moyenne parmi l'ensemble des entreprises ciblées).

Elles sont également moins nombreuses à avoir versé une rançon, ce qui laisse penser qu'elles ont souvent disposé de l'expertise suffisante pour repousser une attaque par ransomware ou pour y remédier après coup. Un peu plus de la moitié des entreprises expertes ciblées (54%) ont versé une rançon, contre deux tiers (68%) des novices. De façon générale, les expertes se sont rétablies plus rapidement (voir Fig. 6).

Toutefois, si l'on tient compte de l'ensemble des cyber-attaques, les entreprises expertes ont subi des coûts aussi élevés que l'ensemble des novices et des intermédiaires, malgré le fait qu'elles ne représentent que 20% de notre panel d'étude. Ce phénomène est corrélé à la taille des entreprises expertes. Un peu plus de la moitié d'entre-elles sont de très grandes entreprises et constituent les principales cibles, subissant ainsi les failles les plus importantes.

Néanmoins, les entreprises n'ont pas toujours été à la hauteur : elles ont été plus nombreuses à laisser des pirates s'introduire via un serveur sur lequel les correctifs n'ont pas été déployés (raison mentionnée par 38% des expertes, contre 28% en moyenne) ou via une attaque de serveur par force brute par laquelle les pirates cherchent à saisir des identifiants en utilisant des séquences de chiffres ou des mots de passe populaires (25% contre 19% en moyenne).

Modélisation des capacités de gestion des cyber-risques

Les entreprises sont fortes dans un certain nombre de domaines technologiques mais présentent des faiblesses en ce qui concerne leur personnel.

Avec l'évolution des cyber risques, il faut aussi adapter la façon de mesurer la préparation et la résilience. Pour la première fois depuis le lancement de ce rapport, nous avons revu ce qui signifie, pour une entreprise, d'être un expert en cyber sécurité. Notre nouveau modèle d'évaluation de la maturité n'est pas qu'un modèle d'évaluation du niveau de préparation, mais aussi de la résilience d'une entreprise face à des tentatives d'attaques et des attaques.

Notre modélisation des capacités de gestion des cyber-risques a deux dimensions. Elle quantifie les capacités des entreprises selon six axes opérationnels de la cybersécurité (désignés « domaines ») et affine son analyse au moyen de questions conçues pour évaluer l'efficacité des personnes, processus et technologies (« fonctions ») Elle combine les deux notes pour obtenir une photographie de la cyber-maturité (voir Fig. 7).

Dans le cadre de ce processus, elle met en lumière les points de force ou de faiblesse. Beaucoup sont étonnamment cohérents d'un pays à l'autre et d'un secteur à l'autre, soulignant les leçons que beaucoup d'entreprises doivent tirer.

Seule une entreprise sur cinq (20%) se qualifie d'experte (bien que cela constitue une légère amélioration par rapport à la modélisation des années précédentes). La moitié des entreprises se situe dans la tranche des intermédiaires. Les novices constituent les 30% restants.

Les États-Unis dominent le classement

Les entreprises américaines réalisent le meilleur score avec la plus grande proportion d'expertes (25%) et la plus faible proportion de novices (27%), bien qu'elles soient derrière les entreprises allemandes et françaises au niveau du score moyen global. Il est intéressant de noter que la bonne performance des entreprises américaines se reflète également par le coût médian subi suite à une attaque, qui est le plus faible de tout notre panel. Les entreprises espagnoles sont à la traine : seules 9% d'entre elles se classent expertes et 35% se classent novices. Elles figurent en bas du classement dans toutes les catégories de taille d'entreprise.

Le Royaume-Uni fait figure d'énigme. Alors qu'il se classe deuxième derrière les États-Unis en ce qui concerne la proportion d'expertes (23%), ses micro-entreprises (1-9 salariés) sont le mauvais élève de l'ensemble des huit pays, 62% d'entre elles obtenant la mention « novice ». Les petites entreprises espagnoles et irlandaises ont également obtenu de mauvais scores, avec 58% de novices.

En ce qui concerne les secteurs d'activité, les secteurs des métiers technologies, médias et télécommunications (TMT) comptent la plus forte proportion d'expertes (25%), devançant les services financiers et la fabrication qui étaient en tête l'année dernière (voir Fig. 8). Ce n'est pas une coïncidence si les trois secteurs en tête (TMT, énergie et services financiers) sont également les trois secteurs les plus ciblés. À l'opposé, les secteurs des services professionnels, des voyages/loisirs et des services aux entreprises comptent la plus forte proportion de novices (respectivement 41%, 41% et 39%).

Sans surprise, les expertes sont majoritairement les plus grandes entreprises, bien qu'il y ait peu de différence dans les notes d'évaluation des capacités des grandes entreprises (250-999 salariés) et des très grandes entreprises (1 000 salariés et plus). La plus forte proportion d'expertes se trouve parmi les grandes et les très grandes entreprises américaines (respectivement 35% et 36%). Viennent ensuite les très grandes entreprises britanniques (33%). Dans l'ensemble, plus de la moitié (53%) des entreprises de moins de dix salariés se classent novices, tout comme un tiers des entreprises de 10 à 49 salariés.

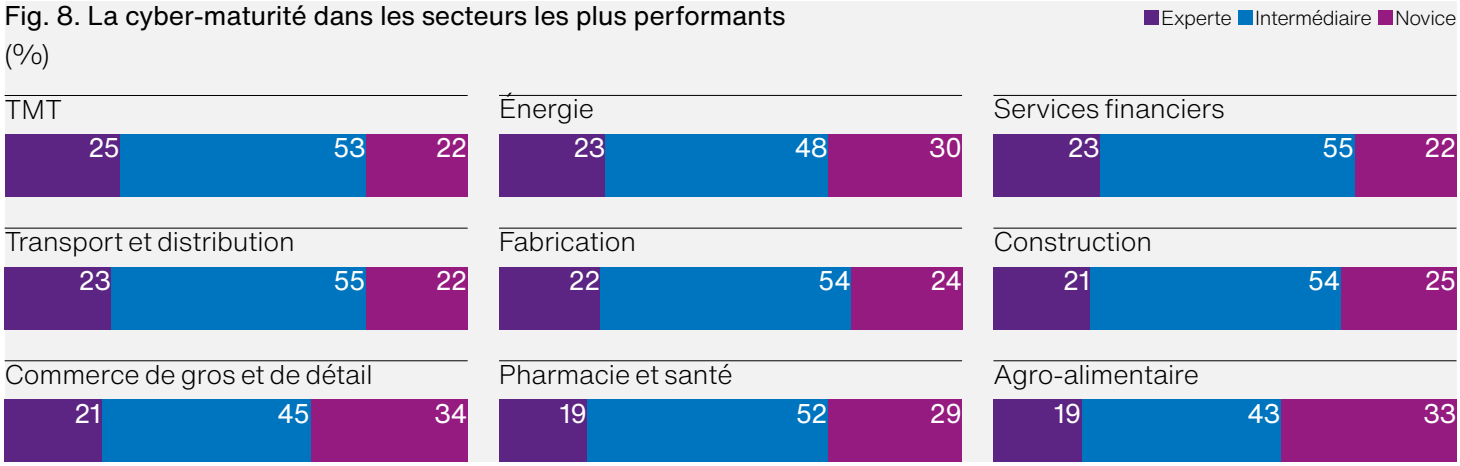
Fig. 7. Modèle de maturité

Notre modélisation repose sur une architecture axée sur les capacités, comprenant les personnes, processus et technologies nécessaires pour créer un système de gestion de la cybersécurité efficace. Elle évalue le niveau de maturité des entreprises à travers six différents axes de capacité (domaines), en utilisant le référentiel COBIT® (Control Objectives for Information and related Technology [objectifs de contrôle de l'information et des technologies associées]). Les six domaines (voir le tableau ci-dessous) couvrent l'ensemble des éléments nécessaires pour installer, exploiter, gérer et contrôler un système de sécurité efficace. Chaque domaine est mesuré au regard de six différents facteurs correspondant aux fonctions « personnes », « processus » et « technologies ». Comme les années précédentes, les entreprises sont notées sur cinq. Une note supérieure à quatre qualifie l'entreprise de « cyber-experte ». À 2,5 et plus, elle qualifie l'entreprise de « cyber-intermédiaire ». En dessous de 2,5, les entreprises sont considérées comme « cyber-novices ».

	Personnes	Processus	Technologies	Moyenne totale
Gestion de la résilience de l'entreprise	3.12	3.13	3.10	3.12
Cryptographie et gestion des clés	2.93	2.90	2.94	2.93
Gestion des identifiants et des accès	3.05	2.95	2.94	2.97
Gestion des informations et événements en matière de sécurité	2.93	3.10	2.99	2.99
Gestion des menaces et vulnérabilités	3.00	3.12	3.28	3.13
Gestion de la confiance	3.07	3.05	3.09	3.07
Moyenne totale	3.02	3.04	3.06	3.03

Fig. 8. La cyber-maturité dans les secteurs les plus performants

(%)



64%

des participants sont « très confiants » dans leurs capacités de gestion des cyber-risques.

Ce que la modélisation nous enseigne

Si l'on observe les notes d'évaluation des capacités de gestion des cyber-risques, la modélisation révèle un énorme fossé entre les expertes et les autres avec une note moyenne de 4,38 pour les expertes et de seulement 1,69 pour les novices (voir Fig. 10). Lorsqu'il s'agit d'analyser où résident les forces et les faiblesses des entreprises, la répartition entre domaines et fonctions est instructive.

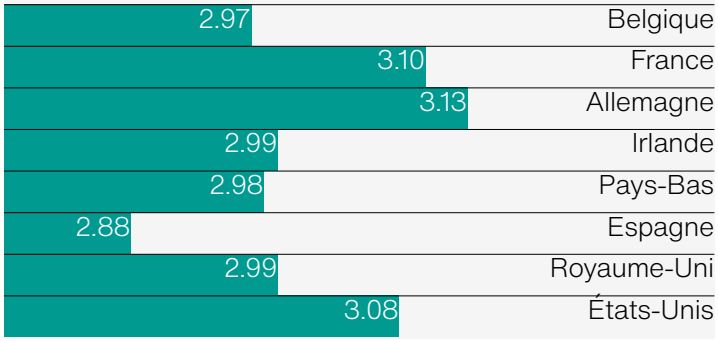
Domaines

Deux domaines se détachent comme des relatifs points de force : la gestion des menaces et vulnérabilités et la gestion de la résilience de l'entreprise (dans lesquels les entreprises ont respectivement obtenu en moyenne 3,13 et 3,12). Les entreprises allemandes ont obtenu les meilleures notes, juste devant les entreprises françaises et américaines. Les entreprises espagnoles ont obtenu les moins bonnes notes, comme dans les autres domaines. Les notes vont néanmoins de pair avec la taille des entreprises et se nivellent pour les entreprises de 250 salariés et plus.

Si l'on considère l'ensemble des six domaines, trois secteurs se sont distingués. Les TMT ont obtenu la meilleure note, comme on pouvait s'y attendre, mais les services financiers et le secteur des transports/distribution se placent juste derrière. Les services professionnels ont été les mauvais élèves.

De nombreuses entreprises ont été pénalisées par de mauvaises notes en matière de cryptographie et de gestion des clés (voyages et loisirs, services aux entreprises et services professionnels en particulier), et dans une moindre mesure en matière de gestion des identités et des accès. Cela représente un problème. La cryptographie est à la base de tout système informatique moderne et au centre de tout autre contrôle. Il convient de souligner que le rapport montre une forte corrélation entre l'incidence des piratages de messagerie professionnelle et la faiblesse des notes en matière de configuration et de gestion des contrôles cryptographiques.

Fig. 9. Note globale d'évaluation des capacités de gestion des cyber-risques



Fonctions

En ce qui concerne les fonctions, la modélisation évalue les opérations de cybersécurité des entreprises selon trois axes : personnes, processus et technologies. Globalement, les notes les plus faibles sont obtenues dans le premier de ces trois axes, ce qui laisse penser que beaucoup d'entreprises doivent s'améliorer dans le recrutement et la formation de personnes convenablement qualifiées et expérimentées. De façon logique, le niveau d'expertise augmente généralement avec la taille de l'entreprise. Les petites entreprises de moins de dix salariés sont très loin derrière mais beaucoup d'entre elles n'ont pas la possibilité d'embaucher un spécialiste de ce domaine.

Une fois de plus, ce sont les entreprises allemandes et françaises qui sont les plus performantes, talonnées de près par les entreprises américaines. Les entreprises espagnoles ferment la marche avec une note particulièrement faible en matière de technologies. Comme pour ce qui concerne les domaines, le secteur des TMT obtient les meilleures notes, même si les services financiers et le secteur des transports/distribution obtiennent une meilleure note en matière de processus (voir Fig. 9.).

Le point de vue d'Hiscox

Sans surprise, certaines pratiques de cybersécurité plus établies ont obtenu de meilleures notes. À titre d'exemple, les sauvegardes et reprises d'activité après catastrophe au sein de la « gestion de la résilience de l'entreprise » et les pratiques comme la mises en place de pares-feux et d'antivirus au sein de la « gestion des menaces et vulnérabilités ». Les scores révèlent également une faiblesse générale dans le domaine de la « cryptographie et de la gestion des clés », dans lequel même les expertes sont en difficulté. C'est un problème général. Parmi les domaines les plus compliqués à maîtriser, la cryptographie souffre d'une pénurie de compétences notoire.

Fig. 10. Score de maitrise du risque cyber

Cyber novices	Personnes	Processus	Technologies	Moyenne totale
Gestion de la résilience de l'entreprise	1.83	1.86	1.75	1.81
Cryptographie et gestion des clés	1.58	1.54	1.52	1.55
Gestion des identifiants et des accès	1.80	1.71	1.63	1.69
Gestion des informations et événements en matière de sécurité	1.57	1.90	1.61	1.65
Gestion des menaces et vulnérabilités	1.65	1.85	2.24	1.91
Gestion de la confiance	1.76	1.71	1.72	1.73
Moyenne totale	1.70	1.76	1.74	1.72

Cyber expertes	Personnes	Processus	Technologies	Moyenne totale
Gestion de la résilience de l'entreprise	4.44	4.43	4.43	4.43
Cryptographie et gestion des clés	4.29	4.25	4.34	4.29
Gestion des identifiants et des accès	4.37	4.29	4.38	4.34
Gestion des informations et événements en matière de sécurité	4.32	4.34	4.38	4.35
Gestion des menaces et vulnérabilités	4.34	4.36	4.29	4.33
Gestion de la confiance	4.37	4.37	4.46	4.41
Moyenne totale	4.35	4.34	4.38	4.36

Ce que les entreprises cyber-expertes peuvent nous enseigner

Gérer les risques

Il est impossible de garantir une sécurité totale. Mais la capacité à réagir rapidement et efficacement et à faire appel à une expertise extérieure dans les moments critiques, garantit la résilience. C'est ce que font les expertes. Près de la moitié d'entre elles (47%) indiquent avoir souscrit une police de cyber-assurance dédiée, contre 45% l'an dernier. Mais le fossé entre elles et les autres continue de se creuser. Seules 11% des novices sont dans ce cas-là (contre 18% l'an dernier).

Désigner un responsable

Beaucoup d'entreprises sont trop petites pour être en mesure d'embaucher un cyber-spécialiste interne, mais ce n'est pas une raison pour ne pas désigner une personne en charge de la cybersécurité ou mandater un prestataire de services externe. Près de la moitié (48%) des entreprises de moins de 10 salariés et 45% des novices ont déclaré qu'elles n'avaient désigné aucun responsable de la cybersécurité.

Traiter les principales vulnérabilités

Sept entreprises cyber-expertes sur dix considèrent que le télétravail augmente leur vulnérabilité aux attaques. Seules 40% des novices partagent cet avis. La priorité numéro un pour les entreprises cyber-expertes dans l'année à venir est de traiter les « menaces et vulnérabilités existantes ». Près de trois quarts d'entre elles la mentionnent. Les entreprises cyber-expertes sont deux fois plus nombreuses que les novices à envisager de renforcer la sécurité des services et applications destinés aux clients. Il faut y voir un message.

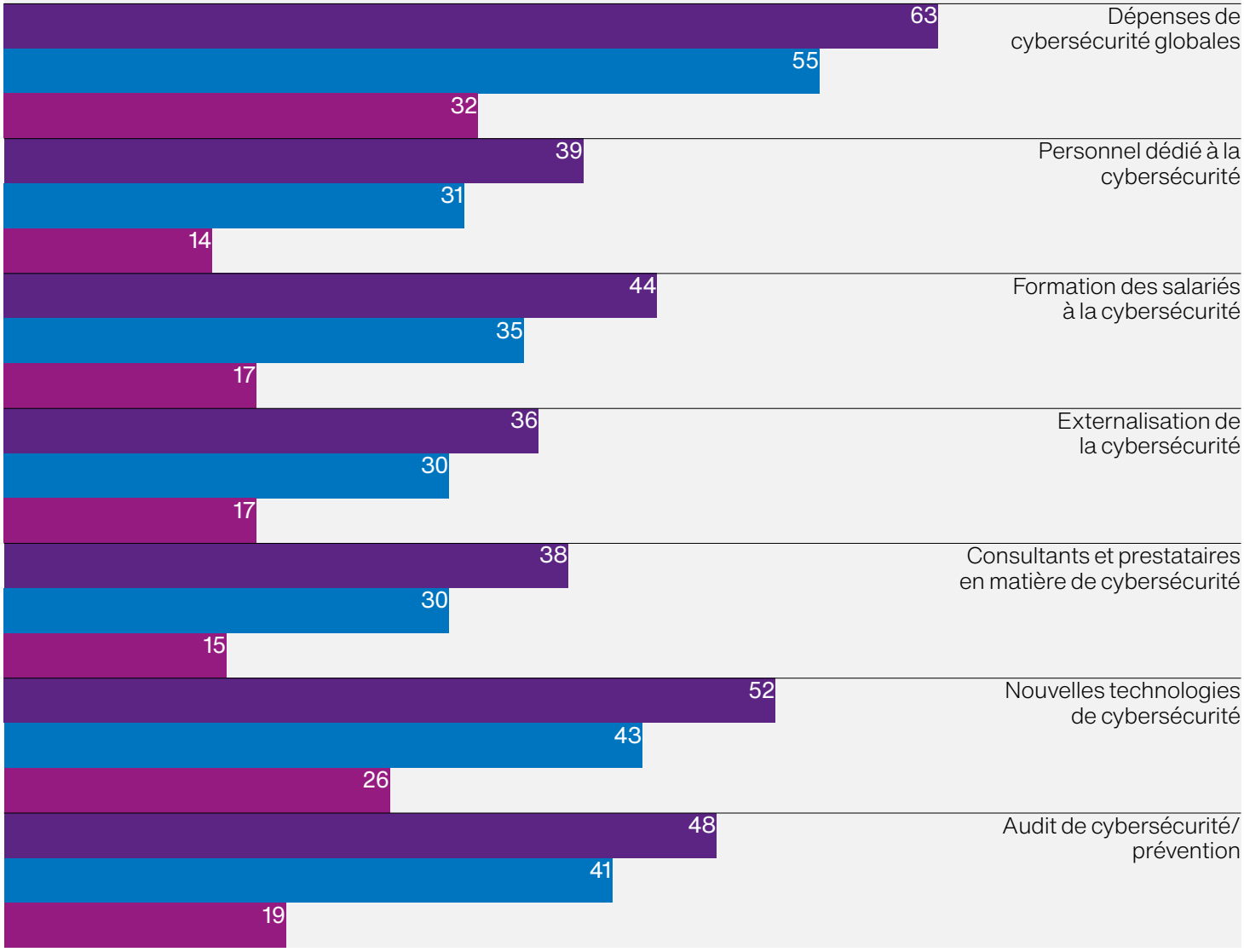
Sauvegarder les données, de préférence en dehors des locaux de l'entreprise

Les entreprises cyber-expertes ont mieux réussi à repousser les attaques avant qu'elles ne causent de dommages. Un septième d'entre elles (14%) ont déclaré que les attaques par déni de service distribué/ransomware n'avaient eu aucun impact financier. L'une des raisons à cela est qu'elles étaient mieux préparées à récupérer leurs données. Près de deux-cinquième d'entre elles (39%) l'ont fait trois fois ou plus l'an dernier. Il est donc crucial de respecter les règles fondamentales, comme celle d'effectuer une sauvegarde de toutes les données, de préférence en dehors des locaux de l'entreprise.

Fig. 11. Dépenses

(%)

Les entreprises cyber-expertes consacrent près d'un quart (24%) de leur budget informatique à la cybersécurité. Ce chiffre est de 17% pour les novices. Celles-ci sont presque deux fois plus nombreuses que les novices à prévoir une augmentation de leurs dépenses au cours des 12 prochains mois (63% contre 32% des novices). Les principaux postes de dépense ciblés sont les nouvelles technologies, l'audit et la prévention, et la formation.



Développer la résilience

Les dépenses de cybersécurité représentent désormais une part beaucoup plus importante des dépenses informatiques globales, car les entreprises intensifient leurs mesures de lutte contre la cybercriminalité.

Les entreprises ont radicalement réorienté leur budget informatique l'année dernière. Si les dépenses informatiques ont globalement peu évolué, la part dédiée à la cybersécurité a connu une nette augmentation de 63%. En moyenne, les entreprises consacrent désormais plus d'un cinquième (21%) de leur budget informatique à la cybersécurité, contre un peu moins de 13% l'année précédente. Cela révèle un changement d'attitude important.

En raison de la présence majoritaire de petites entreprises dans notre étude, l'augmentation globale des dépenses de cybersécurité dans notre panel s'élève modestement à 25% (13,0 milliards € contre 10,4 milliards € l'an passé), ou 23% après ajustement lié à l'augmentation du nombre de participant de 4 313 à 4 412.

En moyenne, les entreprises allemandes ont consacré le budget le plus important à la cybersécurité, soit 5,0 millions €, en augmentation de 155% par rapport à l'année précédente, ce qui peut constituer un signe de leur apparente vulnérabilité évoquée par ailleurs dans ce rapport. Les entreprises belges ont le moins dépensé (1,6 millions €).

S'agissant des différents secteurs, les entreprises dans le secteur de l'énergie ont consacré le plus gros budget à la cybersécurité (12.2 millions € en moyenne). Les services financières arrivent en second (5,1 millions €) devant le secteur de la fabrication (4,9 millions €). Les entreprises du secteur des voyages ont le moins dépensé (646 364 €), mais cela peut être la conséquence du gel de leurs activités depuis le début de la pandémie.

La croissance la plus rapide s'observe aux deux extrémités du spectre d'entreprises, à savoir les très petites et les très grandes entreprises (voir Fig. 13). Concernant les plus petites entreprises, les chiffres sont gonflés puisqu'une entreprise de services financiers de moins de 10 salariés a dépensé 'équivalent de 4 millions € par tête. Mais les entreprises de 10 à 49 salariés ont également multiplié leurs dépenses par plus de dix, soit 359 091 €. De leur côté, les très grandes

Fig. 12. Les dépenses de cybersécurité moyennes par entreprise

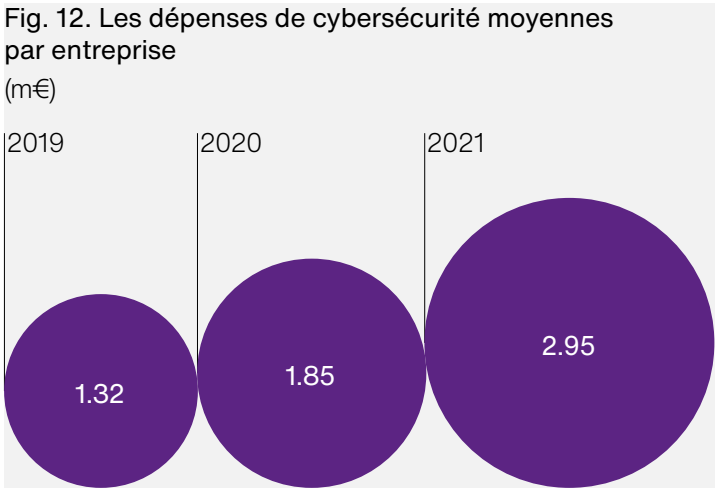


Fig. 13. Dépenses de cybersécurité
Nombre d'employés
(€)

	2021	2020
1–9	112 455	12 090
10–49	359 159	72 202
50–249	289 399	255 884
250–999	1 751 905	784 380
1 000+	11 876 082	7 299 115

entreprises dépensent désormais en moyenne 11,8 millions € contre 3,8 millions € il y a deux ans. Du point de vue des dépenses par salarié, elles restent loin derrière les autres, ce qui laisse penser qu'elles ont encore la capacité d'accroitre davantage leurs dépenses.

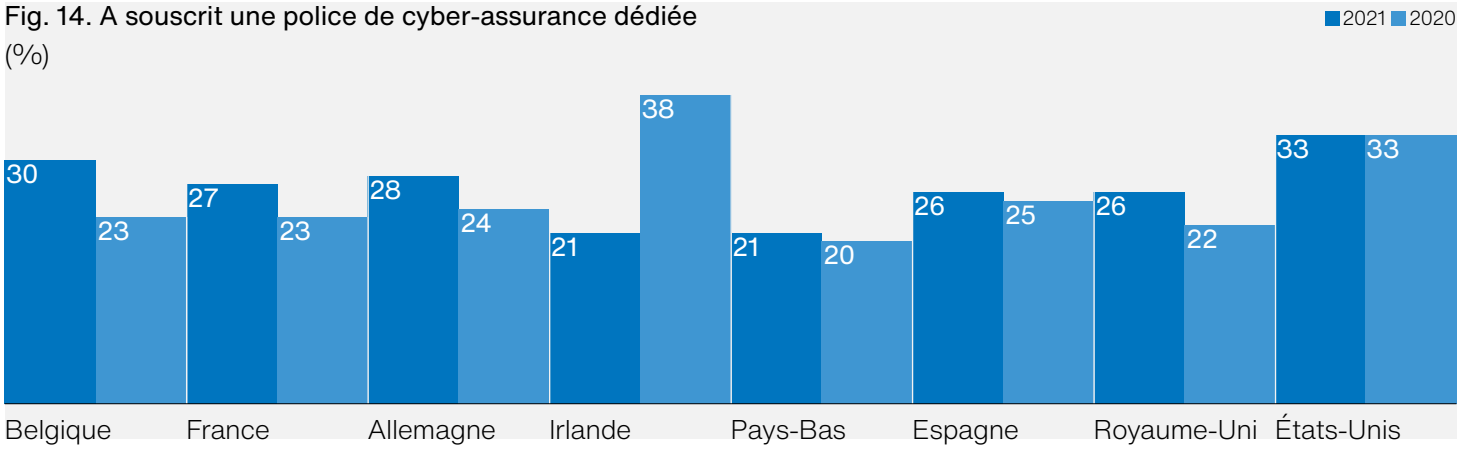
La hausse des dépenses devrait se poursuivre mais à un rythme moins effréné. Si l'on considère chaque entreprise individuellement, les prévisions d'augmentation des dépenses pour l'année à venir s'élèvent à 51%. À titre de comparaison, ce chiffre était de 72% l'an dernier et s'est révélé plutôt juste.

Où vont les dépenses ?
Deux entreprises sur cinq (40%) prévoient d'augmenter de 5 à 10% leurs dépenses en technologie tandis que

Le point de vue d'Hiscox

En 2020, les entreprises ont été contraintes du jour au lendemain de se mettre au télétravail, de développer leur activité en ligne en ligne et de s'engager auprès de leurs clients via des canaux totalement différents. Un des bénéfices de cette migration soudaine en ligne a été la reconnaissance de l'importance de renforcer la cyber-résilience et donc d'augmenter les dépenses de cybersécurité. Les attaques, leurs conséquences et l'attention portée à la cybersécurité diffèrent néanmoins d'un secteur à l'autre, certaines entreprises seront donc mieux préparés que d'autres à gérer les changements critiques à l'avenir.

Fig. 14. A souscrit une police de cyber-assurance dédiée
(%)



36% des entreprises indiquent la même dynamique concernant les audits de cybersécurité et la prévention. Pour autant, le nombre d'entreprises mentionnant une augmentation des dépenses de personnel et de formation est en baisse (de 35% à 27% s'agissant du personnel et de 40% à 32% s'agissant de la formation), ce que nous déplorons compte tenu de la faiblesse du segment « personnes » de notre modélisation des capacités de gestion des cyber-risques.

On constate également que moins d'entreprises prennent des mesures déterminantes à la suite d'une faille subie cette année. Parmi les entreprises attaquées, la part de celles qui déclarent que la sécurité et/ou la protection des données sont régulièrement évaluées chute de 32% à 19%, tandis que le nombre d'entreprises prévoyant d'accroitre les exigences en matière de cybersécurité/ d'audit régresse de 26% à 20%. Dans la lignée des observations ci-dessus, seules 16% des entreprises évoquent des dépenses supplémentaires en matière de formation des salariés et de changement de culture d'entreprise, contre 25% l'an passé.

Un panorama disparate concernant la cyber-assurance

La souscription de polices de cyber-assurance progresse, que ce soit par le biais de polices dédiées (27% des entreprises en possèdent désormais une, contre 26% l'an passé) ou de garanties ajoutées à un autre contrat (34% contre 32% l'an dernier). Le nombre d'entreprises prévoyant de souscrire une police dédiée a augmenté marginalement, de 11% à 12%, tandis que la proportion du nombre d'entreprises à ajouter une couverture cyber à leur police d'assurance existante est resté fixe à 7%, le nombre d'entreprises indiquant qu'elles ne disposent pas de telles garanties et qu'elles ne prévoient pas d'en souscrire, est en hausse (18% contre 21% l'an dernier).

L'adoption d'une police dédiée au cyber est plus importante parmi les entreprises de 250 salariés et plus (36% pour les entreprises de 250 à 999 salariés et 38% pour les très grandes entreprises). Il demeure difficile de faire évoluer les petites entreprises, près de la moitié des entreprises de moins de 10 salariés déclarant en effet qu'elles n'ont pas l'intention de souscrire une assurance. Compte tenu des autres éléments de cette étude qui montrent que les petites entreprises sont vulnérables aux attaques par phishing et au vol d'identifiants, et du potentiel de pertes majeures bien au-delà du chiffre médian, c'est un constat inquiétant.

Les entreprises américaines sont toujours en tête dans ce domaine (voir Fig. 14.). Un tiers d'entre elles (33%) disposent d'une police dédiée. Les entreprises belges sont en deuxième position de notre tableau à 30%. Les entreprises irlandaises, espagnoles et allemandes sont les plus nombreuses à déclarer qu'elles sont couvertes par un autre contrat (respectivement 43%, 37% et 36%).

46%

Augmentation moyenne des salariés en télétravail en raison du Covid-19.

Deux secteurs se démarquent : les services financiers et les TMT. Dans le secteur des services financiers, 39% des entreprises disposent d'une police de cyber-assurance dédiée et 37% d'une garantie des cyber-risques dans le cadre d'un autre contrat. Dans le secteur des TMT, ces chiffres sont respectivement de 34% et 37%. Les entreprises du secteur de la fabrication sont les plus nombreuses à se reposer sur un autre contrat (42%).

Des écarts de perception de l'impact Covid-19

Malgré la multiplication des cas de phishing liés au Covid et l'explosion du travail à domicile, il est surprenant de constater que la prise en compte de la menace accrue résultant de la pandémie est disparate. Moins de la moitié des participants (47%) ont déclaré que leur entreprise « est plus vulnérable aux cyber-attaques depuis le début de la pandémie », ce pourcentage s'élevant aux alentours de 59% pour les entreprises de 250 salariés ou plus. Il y a un problème évident de perception au sein des petites entreprises qui sont moins d'un tiers (31%) à reconnaitre qu'elles sont plus vulnérables.

Dans l'ensemble, le télétravail a très fortement progressé. En moyenne, les entreprises de notre panel d'étude ont augmenté le nombre de leurs salariés en télétravail de 14% à 60%. Mais le changement se concentre sur une minorité d'entreprises. Deux entreprises sur cinq (41%) indiquent qu'elles ont favorisé le télétravail, tandis que 29% ont davantage utilisé les technologies basées sur le cloud et 32% ont recours à des technologies plus collaboratives. Dans chacun des cas, le pourcentage augmente en fonction de la taille de l'entreprise.

La question spécifique du travail à domicile est plus préoccupante. Près de trois entreprises sur cinq (58%) conviennent qu'« en raison du fait que davantage de salariés travaillent à domicile, mon entreprise est plus vulnérable aux cyber-attaques ». À nouveau, cette perception est plus répandue parmi les grandes entreprises (environ 69% des entreprises de 250 salariés ou plus).

Fig. 15. Durcissement de la cybersécurité en raison du Covid-19

Nombre de salariés
(%)

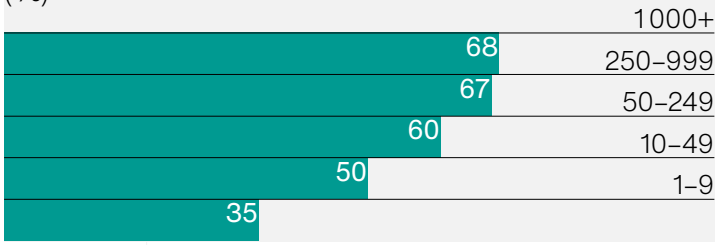


Fig. 16. Changements dus au Covid-19

(%)

Augmentation du nombre de salariés en télétravail	41
Gel des embauches	33
Augmentation de l'utilisation des technologies collaboratives	32
Diminution des coûts d'exploitation	31
Augmentation de l'utilisation des technologies basées sur le cloud	29
Élargissement des paiements en ligne	27
Accélération des plans de transformation numérique	27
Élargissement des canaux de e-commerce existants	20
Réduction du nombre de modifications informatiques	18
Ajouts de nouveaux canaux de e-commerce	18
Consolidation ou réduction du nombre de fournisseurs	15

Les grandes entreprises sont également plus nombreuses à avoir pris des mesures pour limiter leur vulnérabilité : plus de deux tiers des très grandes entreprises et des entreprises de plus de 250 salariés ont indiqué avoir renforcé leurs cyber-défenses (respectivement 68% et 67%). Pour les petites entreprises de moins de dix salariés, le chiffre correspondant est d'à peine 35%. Les chiffres suggèrent qu'un grand nombre d'entreprises, et pas seulement les plus petites, n'ont pas encore pris conscience de la vulnérabilité accrue liée au télétravail.

Le cinquième Rapport annuel d'Hiscox sur la gestion des cyber-risques a été élaboré en collaboration avec Forrester Consulting. Le rapport offre un aperçu rapide des capacités de gestion des cyber-risques des entreprises et propose également un tableau des meilleures pratiques pour lutter contre une menace en perpétuelle évolution. Il est élaboré à partir d'une étude réalisée auprès de dirigeants, directeurs de service, responsables informatiques et autres professionnels clés. Sélectionnés à partir d'un échantillon représentatif de 6 042 entreprises issues de huit pays, classées par taille et par secteur (plus de 1 000 personnes par pays pour le Royaume-Uni, les États-Unis et l'Allemagne, plus de 500 pour la Belgique, la France, l'Espagne et les Pays-Bas et plus de 300 pour la République d'Irlande), ce sont les personnes qui sont en première ligne dans la lutte contre la cybercriminalité. Les participants ont rempli le questionnaire en ligne entre le jeudi 5 novembre 2020 et le vendredi 8 janvier 2021.

Niveau (%)	
Fondateur/Cadre de niveau	50
Vice-président	13
Administrateur	22
Directeur	16

Secteur (%)	
Services aux entreprises	8
Énergie	4
Construction	8
Services financiers	8
Agro-alimentaire	4
Administration et organismes à but non lucratif	5
Fabrication	8
Pharmacie et santé	8
Services professionnels	8
Immobilier	4
Commerce de gros et de détail	9
TMT	16
Transport et distribution	5
Voyages et loisirs	4

Nombre de salariés (%)	
1 000+	25
250–999	15
50–249	15
10–49	16
1–9	29

Service (%)	
Haute direction	14
e-Commerce	2
Finance	9
Direction juridique	2
Ressources humaines	6
Informatique et technologie	21
Marketing et communications	3
Opérations	11
Propriétaire	21
Achats	2
Gestion de produit	3
Gestion des risques	3
Ventes	5

Hiscox Assurances

38 avenue de l'Opéra
75002 Paris France

+33 (0)1 53 21 82 82
info.france@hiscox.com
hiscox.fr/courtage/toutes-assurances-hiscox/cyberclear

21486 04/21