

Rapport Hiscox
sur la gestion des
cyber-risques
2019



Hiscox, assureur spécialiste international, est une société cotée au London Stock Exchange (LSE:HSX), dont le siège social est situé aux Bermudes. Notre ambition est d'être un assureur spécialiste reconnu, disposant d'un portefeuille diversifié par produit et zone géographique. Dans le cadre de notre activité de retail au Royaume-Uni, en Europe, en Asie et aux États-Unis, nous proposons une gamme d'assurances spécialisées pour les professionnels, entreprises et particuliers. Les activités relatives aux contrats internationaux, grands comptes et à la réassurance sont gérées par nos divisions Hiscox Marché de Londres et Hiscox Re & ILS. Nos valeurs définissent notre entreprise, qui attache la plus grande importance aux personnes, à la qualité, au courage et à l'excellence dans la réalisation. Nous sommes fidèles à nos engagements et notre service de gestion de sinistres plusieurs fois récompensé en est la preuve. Pour de plus amples informations, rendez-vous sur www.hiscoxgroup.com.

Répondre aux cyber-menaces

Notre troisième Rapport Hiscox sur la gestion des cyber-risques vous propose un aperçu rapide du niveau de capacité de gestion des cyber-risques des entreprises, ainsi qu'un tableau des meilleures pratiques pour lutter contre la cyber-menace en perpétuelle évolution.



Gareth Wharton
Cyber CEO, Hiscox

Le nombre d'entreprises ayant fait état de cyber-incidents est passé de 45% en 2018 à 61% cette année.

Quasiment toutes les semaines, des cyber-incidents majeurs sont rapportés, et les enjeux n'ont jamais été aussi importants. Le vol de données est devenu quotidien, le niveau des demandes de rançon a considérablement augmenté et, en parallèle, l'environnement dans lequel les entreprises doivent évoluer est de plus en plus hostile. La cyber-menace est devenue une source de coûts inévitable pour les entreprises aujourd'hui.

Il s'agit de notre troisième Rapport Hiscox sur la gestion des cyber-risques et, pour la première fois, une grande majorité des entreprises interrogées ont déclaré avoir subi une ou plusieurs cyber-attaques au cours des 12 derniers mois. Le coût et la fréquence des attaques ont augmenté de façon significative par rapport à l'année dernière. Alors que les pirates s'attaquaient auparavant principalement aux grandes entreprises, on constate aujourd'hui que les petites et moyennes entreprises sont tout aussi vulnérables.

La réglementation vise à sensibiliser davantage et à imposer un socle de rigueur en matière de cybersécurité. En 2018, le Règlement général sur la protection des données de l'Union européenne (RGPD) est entré en vigueur et les entreprises ont dû s'y conformer. Celui-ci a eu pour conséquence d'accroître les demandes de cyber-assurance. Dans les pages qui suivent, nous observons que les entreprises sont plus nombreuses à adopter une démarche structurée face au problème, en désignant des personnes en charge de la cyberstratégie, et nous constatons également une volonté plus appuyée de transférer tout ou partie des risques à un assureur en souscrivant une police de cyber-assurance.

Le vieil adage « mieux vaut prévenir que guérir » est plus que jamais d'actualité, et le fait d'être conscient de ces menaces constitue déjà une moitié du chemin à parcourir pour s'en prémunir. Selon notre expérience d'assureur de cyber-risques, le piratage des comptes de messagerie électronique professionnelle est actuellement la principale cause de cyber-sinistres, suivie des ransomware.

Il y a un an, nous avons lancé notre plateforme de formation en ligne, la CyberClear Academy, dans le but de mieux préparer nos clients à faire face à ces dangers, et plus de 2 500 entreprises en ont déjà bénéficié. Nous ne nous reposons toutefois pas sur nos lauriers et nous continuerons d'élaborer d'autres mesures de prévention qui protégeront nos clients et ce qui a de la valeur à leurs yeux.

Les cyber-risques peuvent évoluer rapidement mais les moyens de les atténuer et de les gérer progressent également. J'espère que ce rapport saura vous aider à mieux comprendre les problématiques et qu'il vous encouragera à prendre des mesures rigoureuses et efficaces pour minimiser la cyber-menace.

Résumé

Le niveau des capacités de gestion des cyber-risques ne progresse plus, alors que les attaques se font plus intenses, tant par leur fréquence, que par les coûts qu'elles engendrent.

Principales conclusions

Des motifs d'optimisme malgré une stagnation des notes d'évaluation des capacités de gestion des cyber-risques.

Au vu des résultats de notre test d'évaluation des capacités de gestion des cyber-risques, davantage d'entreprises montre un niveau de préparation insuffisant

Notre modélisation quantitative des capacités de gestion des cyber-risques montre un léger déclin cette année du nombre d'entreprises ayant obtenu la mention « expert » suite à l'évaluation de leur cyberstratégie et son exécution (le pourcentage de ces entreprises passe de 11% à 10%).

Augmentation des pertes liées aux cyber-incidents

Le montant moyen des pertes liées à l'ensemble des cyber-incidents parmi les entreprises ayant fait état d'une attaque, a augmenté pour atteindre 369 000 € cette année contre 229 000 € en 2018, soit une hausse de 61%, les entreprises de moyenne et grande taille supportant un niveau de coût proportionnellement supérieur aux autres.

Le montant des pertes est impacté par les incidents importants

Le montant indiqué ci-dessus est largement impacté par la forte hausse du coût du pire incident rapporté. Le coût moyen a fait un bon pour passer de 34 000 € il y a un an à près de 200 000 €. Pour les grandes entreprises, ce coût a été multiplié par 18 et s'établit à 395 000 €. A titre de comparaison, le coût moyen pour les petites entreprises ne représente que 9 000 € cette année contre 3 000 € l'an dernier.

Deux facteurs expliquent la chute des notes d'évaluation des capacités de gestion des cyber-risques

L'inclusion des entreprises françaises pour la première fois a abaissé le niveau global des notes. On observe également une baisse importante du nombre d'entreprises américaines et allemandes de grande taille (entre 250 et 999 salariés) et de très grande taille (1 000 salariés et plus) ayant obtenu les meilleures notes.

Les incidents dans la chaîne logistique sont désormais monnaie courante

Près de deux tiers des entreprises (65%) ont subi des cyber-incidents dans leur chaîne logistique l'an dernier. Trois quarts des entreprises de technologie, média et télécommunications (TMT) et de transport ont été impactées.

Les entreprises allemandes ont été les plus touchées, pour la deuxième année consécutive

Le coût moyen des incidents rencontrés en Allemagne cette année par les moyennes et grandes entreprises a dépassé 1 millions €, voire même 1,5 millions € pour les très grandes entreprises.

Les cyber-attaques s'intensifient

Plus de trois entreprises sur cinq (61%) ont indiqué avoir subi une attaque l'an dernier, contre 45% dans le précédent rapport. La fréquence des attaques a également augmenté. Parmi les sept pays de notre étude, les entreprises belges sont celles qui ont subi le plus d'attaques, et les entreprises américaines celles qui en ont subi le moins.

Les petites entreprises ont davantage été attaquées cette année

Alors que les grandes entreprises sont toujours les plus ciblées par les cyber-attaques, la proportion de petites entreprises (moins de 50 salariés) ayant signalé un ou plusieurs incidents progresse, passant de 33% à 47%. En ce qui concerne les entreprises de taille moyenne (entre 50 et 249 salariés), ce chiffre s'est accru de façon très significative et représente 63% contre 36% l'an dernier.

Les dépenses de cybersécurité augmentent de 24%

La dépense moyenne en matière de cybersécurité s'établit désormais à 1,45 millions € et le rythme des dépenses s'accélère. Le total des dépenses des 5 400 entreprises sondées pour notre rapport atteint pas moins de 7,9 milliards €. Deux tiers des répondants prévoient d'augmenter leurs dépenses de cybersécurité de 5% ou plus dans l'année à venir.

Comparaison par pays

Bien que l'on constate des différences en ce qui concerne les pertes liées à des cyber-incidents dans les sept pays considérés, il existe néanmoins des points de comparaison, tels que la fréquence des cyber-attaques et les coûts de rétablissement.

Belgique



- Pays le plus attaqué (71% des entreprises ont signalé un cyber-incident) et le plus impacté par les incidents liés à la chaîne logistique.
- Première place du classement en nombre d'attaques : plus d'un tiers des entreprises ciblées ont été attaquées quatre fois ou plus.
- 16% des grandes et très grandes entreprises ont obtenu la mention « expert » dans notre modélisation des capacités de gestion des cyber-risques, ce qui les place en tête du classement.

Allemagne



- Les grandes et très grandes entreprises sont moins nombreuses à avoir obtenu la mention « expert » dans notre modélisation des capacités de gestion des cyber-risques (20% en 2018 contre 14% cette année).
- Les entreprises allemandes ont été les plus impactées au cours des 12 derniers mois, avec un coût moyen de l'ensemble des incidents supérieur à 900 000 €, plus du double du coût moyen établi pour les sept pays.
- Une entreprise allemande a déclaré que le coût de l'ensemble des incidents représentait 48 millions €, soit la somme la plus importante parmi toutes les entreprises de notre panel.

Espagne



- Les entreprises ont pris des mesures fortes en cas d'incident, 18% d'entre elles ayant augmenté leurs dépenses dans les technologies de détection et 22% dans les technologies de prévention.
- Malgré une démarche plus rigoureuse d'évaluation des risques liés à leur chaîne logistique, 72% ont rapporté une attaque dans ce secteur.
- Les entreprises espagnoles sont les plus nombreuses à avoir souscrit une police de cyber-assurance dédiée : 49% alors que la moyenne du panel de l'étude est de 41%.

États-Unis



- Le coût moyen des incidents rencontrés par les entreprises américaines est le plus faible – 119 000 € contre 369 000 € pour l'ensemble du panel.
- Les grandes et très grandes entreprises sont plus de deux fois moins nombreuses à avoir obtenu la mention « expert » dans notre modélisation des capacités de gestion des cyber-risques (26% en 2018 contre 11% cette année).
- 72% des entreprises américaines prévoient d'augmenter leurs dépenses de sécurité, soit la plus grande proportion parmi les sept pays.

France



- 81% des entreprises françaises ont obtenu la plus mauvaise note dans notre modélisation des capacités de gestion des cyber-risques, seules 6% d'entre elles ont obtenu la mention « expert ».
- Les dépenses de cybersécurité des entreprises françaises ont été les plus importantes (coût moyen de 2,1 millions €) et elles ont subi moins de cyber-incidents que les autres.
- Les entreprises françaises sont les moins nombreuses à disposer d'une couverture de cyber-risques, à égalité avec les entreprises allemandes.

Pays-Bas



- Meilleure progression dans notre modélisation 2019 des capacités de gestion des cyber-risques – le pourcentage d'entreprises ayant obtenu la plus faible note est passé de 82% à 76%.
- 19% des entreprises ont fait état d'une attaque par déni de service distribué (DDoS), en comparaison de la moyenne de 15% relevée dans le panel de l'étude.
- Les entreprises néerlandaises sont les plus nombreuses à avoir subi des ruptures de service, 27% d'entre elles ayant signalé un problème.

Royaume-Uni



- Les entreprises britanniques consacrent le budget moyen le plus faible à la cybersécurité : 900 000 € contre 1,46 millions € en moyenne dans le panel de l'étude.
- Le coût moyen des incidents subis par les entreprises britanniques est inférieur à la moyenne de l'étude : 243 000 € contre 369 000 €.
- Elles sont les plus nombreuses à prétendre être capables de mesurer clairement les impacts commerciaux des cyber-incidents.

L'étendue du problème

Année après année, davantage d'entreprises déclarent être touchées par un cyber-incident. Le risque semble être aussi important quelle que soit la dimension de l'entreprise ou du secteur d'activités.

Les cyber-attaques s'intensifient

Le pourcentage de répondants ayant signalé un cyber-incident a augmenté pour passer de 45% l'an dernier à 61% cette année, et les chiffres sont encore plus importants dans chacune des catégories de taille. Près d'un quart des entreprises interrogées (24%) rapportent avoir été infectées par un virus ou un ver et 17% avoir subi une attaque par ransomware. Le nombre d'entreprises ayant subi une attaque par déni de service distribué (DDoS) est passé de 10% à 15%.

La fréquence des attaques a également augmenté considérablement. Parmi les entreprises ayant subi des cyber-attaques 30% ont rapporté quatre incidents ou plus, contre 20% l'an dernier.

Les petites entreprises ont davantage été ciblées cette année

Un nombre croissant de petites entreprises est désormais la cible des pirates informatiques. Les entreprises de petite et moyenne taille sont plus nombreuses à avoir subi plusieurs attaques cette année, et en moyenne, le pourcentage de ces entreprises à avoir subi une attaque a augmenté de 59%.

Les grandes entreprises sont plus nombreuses à avoir subi des incidents répétés. Plus d'un cinquième d'entre elles (21%) ont subi cinq attaques ou plus cette année, contre 16% en moyenne parmi l'ensemble des répondants.

Il est bien entendu possible que les grandes entreprises soient simplement meilleures pour détecter des failles de données que les petites entreprises. Néanmoins, la mise en œuvre du RGPD l'an dernier a obligé les grandes entreprises, qui risquent de lourdes sanctions en cas de faille importante ou de non-signalement d'un incident dans les délais impartis, à être plus vigilantes et promptes à signaler des incidents.

Pourcentage d'entreprises ciblées dans l'année (%)

Petites entreprises (1–49 salariés)



Moyennes entreprises (50–249 salariés)



Grandes entreprises (250–999 salariés)



Très grandes entreprises (1 000 salariés et plus)



Pourcentage d'entreprises ayant rapporté une attaque (%)

	2019	2018
Belgique	71	–
France	67	–
Allemagne	61	48
Pays-Bas	68	50
Espagne	66	57
Royaume-Uni	55	40
États-Unis	53	38

Les données 2018 ne sont pas disponibles pour la Belgique ou la France.

Aucun secteur n'est épargné

Dans chacun des 15 secteurs observés pour élaborer ce rapport, le pourcentage d'entreprises à avoir déclaré une ou plusieurs attaques a nettement augmenté. Dans l'ensemble des sept pays, le secteur le plus lourdement ciblé était les TMT, où 72% des répondants ont rapporté une ou plusieurs attaques, contre 53% l'an dernier. Viennent ensuite les organismes publics (71% ayant rapporté une attaque, contre 55% en 2018), suivis des services financiers (67% contre 57% en 2018).

La chaîne logistique est-elle un maillon faible ?

Pour la première fois, nous avons posé une série de questions concernant la sécurité des réseaux de fournisseurs des entreprises participantes. Près de deux tiers des répondants (65%) ont indiqué avoir subi une ou plusieurs cyber-attaques l'an dernier en raison d'une faiblesse dans leur chaîne logistique. Les pourcentages étaient encore plus élevés en Belgique et en Espagne (respectivement 73% et 72%). Dans l'ensemble, trois quarts des entreprises de TMT et de transport ont été ciblées. Un peu plus de la moitié de l'ensemble des entreprises interrogées prévoient des indicateurs clés de performance (KPI) dans les contrats avec leurs fournisseurs. Ce pourcentage est de 65% parmi les très grandes entreprises mais de seulement 39% parmi les petites entreprises.

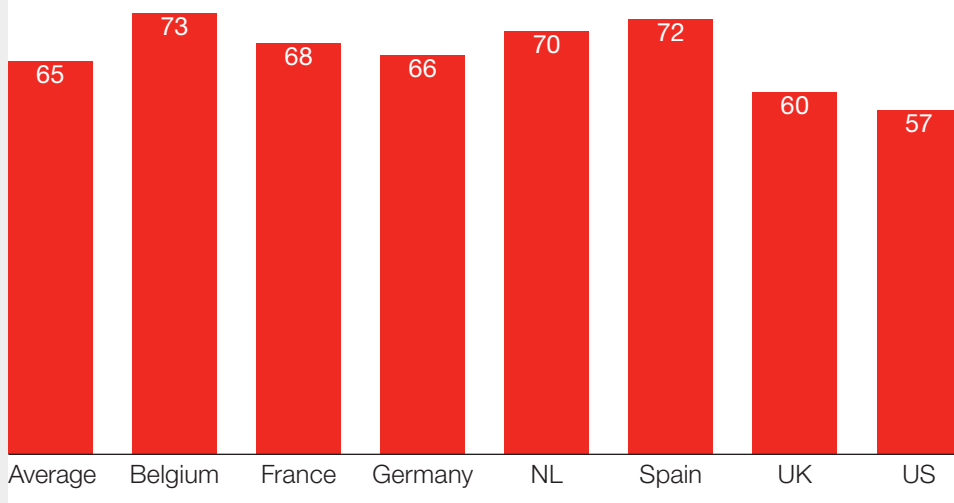
A la question de savoir à quelle fréquence ils évaluent la sécurité de leurs réseaux de fournisseurs, près de trois quarts des entreprises (74%) ont répondu qu'elles le faisaient au moins tous les trimestres ou de façon ponctuelle. Les entreprises espagnoles semblent les plus prudentes sur cette question : près de la moitié d'entre elles (47%) ont déclaré évaluer la cybersécurité de leurs fournisseurs une fois par mois, contre 32% en moyenne pour l'ensemble des répondants.

8% des entreprises ont indiqué avoir accru l'évaluation de leur chaîne logistique en conséquence d'un incident l'an dernier, ce pourcentage étant le plus important dans le secteur des services financiers (12%).

Les entreprises dépendantes du cloud courent davantage de risques

Beaucoup de répondants ont signalé cette année des problèmes de ruptures de service de leurs prestataires de services cloud (22% contre 13% en 2018). Les entreprises néerlandaises ont été les plus touchées, 27% de celles qui ont subi des cyber-incidents ont signalé des ruptures de service, tandis que dans le panel d'entreprises interrogées, les grandes entreprises et les très grandes entreprises sont les plus nombreuses à avoir subi un incident lié au cloud: respectivement 27% et 22%. Cela révèle la tendance des entreprises à transférer leur données dans le cloud au fur et à mesure qu'elles grandissent.

Pourcentage d'entreprises ayant subi une cyber-attaque liée à leur chaîne logistique (%)



Impact financier

Le coût de la cybercriminalité pour les entreprises semble augmenter de façon exponentielle, plus 61% en moyenne cette année.

Augmentation des pertes liées aux cyber-incidents

Les entreprises dans le monde subissent de plus en plus de pertes liées à la cybercriminalité. Sur les 3 300 entreprises de notre panel qui ont subi une attaque, environ 2 250 ont évalué les coûts correspondants pour leur entreprise.

En considérant l'ensemble des incidents rencontrés sur l'année, on observe que le coût moyen pour les entreprises est passé de 229 000 € à 369 000 €, soit une augmentation de 61%. Si l'on applique cette moyenne aux entreprises qui n'ont pas suivi ni quantifié l'impact des cyber-attaques, le coût total pour les 3 300 entreprises ciblées s'élève à environ 1,2 milliards €. En ajustant ce chiffre en fonction de l'augmentation du panel d'entreprises sondées cette année et du nombre d'entreprises ciblées, on constate que le coût est plus de deux fois supérieur à celui observé dans le rapport précédent.

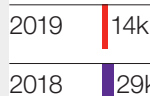
Les moyennes n'expliquent toutefois qu'une partie du tableau. Alors que près de la moitié (47%) des petites entreprises ont subi une cyber-attaque au cours des 12 derniers mois (contre 33% en 2018), le coût moyen de l'ensemble des incidents subis a en réalité diminué de moitié, passant de 29 000 € à 14 000 €. Toutefois, ces données ne concernent pas les entreprises de moyenne et grande taille qui ont supporté une part disproportionnée de ce coût cette année, exposant souvent des montants bien plus élevés que l'année précédente. C'est le cas du Royaume-Uni, de la France, de l'Espagne et des Pays-Bas en particulier.

L'une des données les plus frappantes cette année est le coût moyen du pire incident rapporté. L'an dernier, il était de 34 000 €. Cette année, il a presque été multiplié par six, pour atteindre près de 200 000 €. Toutes entreprises confondues, le coût des pires incidents est désormais

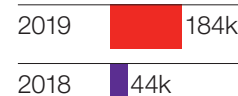
susceptible de représenter de trois à dix-huit fois le budget qu'il représentait il y a seulement un an. Ces chiffres concordent avec les données sectorielles de grande échelle qui révèlent une nette augmentation des demandes de rançon, par exemple, sur l'année 2018.

Coût moyen de tous les incidents (€)

Petites entreprises (1–49 salariés)



Moyennes entreprises (50–249 salariés)



Grandes entreprises (250–999 salariés)

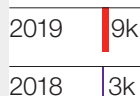


Très grandes entreprises (1 000 salariés et plus)

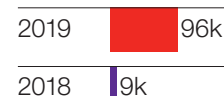


Coût moyen du pire incident (€)

Petites entreprises (1–49 salariés)



Moyennes entreprises (50–249 salariés)



Grandes entreprises (250–999 salariés)



Très grandes entreprises (1 000 salariés et plus)



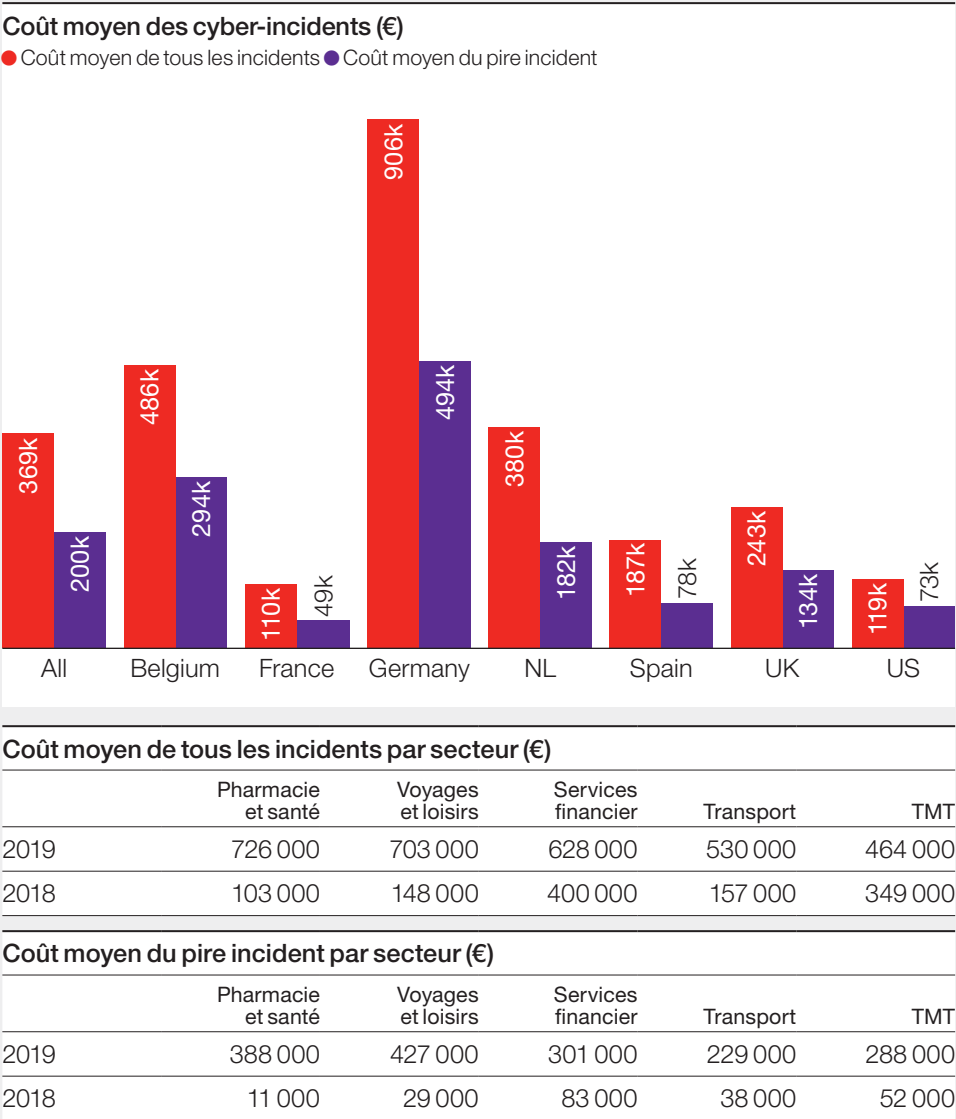
L'Allemagne lourdement touchée

Dans l'ensemble, les entreprises allemandes sont celles qui ont subi le plus de pertes, avec un coût moyen des incidents rencontrés sur l'année de plus d'1 million € pour les moyennes et grandes entreprises et de plus d'1,5 million € pour les très grandes entreprises. C'est également une entreprise allemande qui a rapporté le coût lié aux cyber-incidents le plus élevé : 48 millions €. De même, si l'on regarde le coût du pire incident subi, il est près de dix fois supérieur pour les entreprises allemandes par rapport aux entreprises françaises et espagnoles : 776 000 € contre respectivement 78 000 € et 82 000 €.

A l'opposé, les entreprises américaines semblent s'en être correctement sorties. Pour les moyennes et grandes entreprises, le coût moyen de l'ensemble des incidents est d'à peine 100 000 € ; pour les très grandes entreprises il s'élève à 213 000 €. Et cela, malgré une nette diminution (de 26% à 11%) du nombre de grandes entreprises américaines figurant dans le haut du classement de notre modélisation des capacités de gestion des cyber-risques. Une explication peut être que les entreprises américaines ont été beaucoup moins touchées par la perte des données de leurs clients ou salariés, ou le vol de propriété intellectuelle (PI), de secrets commerciaux ou de résultats de recherche et développement (R&D) sur les 12 mois considérés. Par exemple, les entreprises françaises sont deux fois plus nombreuses (16%) que les entreprises américaines (8%) à avoir signalé une faille de données ayant entraîné la perte de données de salariés.

Tous les secteurs sont impactés

Le coût moyen des incidents s'est réduit en 2018 dans seulement cinq des secteurs observés (services professionnels, énergie, commerce de gros et de détail, agro-alimentaire et organismes publics) et même dans ces secteurs, le coût moyen du pire incident a très nettement augmenté.



Modélisation des capacités de gestion des cyber-risques

En mesurant précisément l'écart entre les pratiques d'une société et ce qu'on peut considérer comme les meilleures pratiques, il apparaît que la plupart des entreprises sont encore loin d'être adéquatement préparées à faire face aux cyber-risques.

Pas de nouveaux progrès constatés

Malgré les nouvelles réglementations et le nombre de failles révélées publiquement, les entreprises ont obtenu de moins bonnes notes dans notre modélisation des capacités de gestion des cyber-risques cette année : près de trois quarts des entreprises (74%) n'ont obtenu la mention « expert » dans aucun des domaines.

La modélisation des capacités de gestion des cyber-risques mesure précisément l'écart entre les pratiques d'une société et ce qu'on peut considérer comme les meilleures pratiques. Les personnes interrogées doivent répondre à une série de question couvrant leur approche dans cinq domaines : stratégie, contrôle et ressources d'un côté et technologie et procédures de l'autre. Les répondants sont invités à nous dire à quel point leurs pratiques relèvent d'une approche bien structurée, rigoureuse et efficace.

Les répondants sont notés sur chacune de leurs réponses et classés ensuite selon une échelle allant de « cyber novice » et « cyber intermédiaire » à « cyber expert ». Les entreprises qui obtiennent quatre ou plus (sur cinq) sur les deux axes sont « expertes ». Celles qui obtiennent cette note sur un axe mais pas sur l'autre sont « intermédiaires ». Celles qui obtiennent une note inférieure à quatre dans les deux catégories sont « novices ».

Notre diagramme de corrélation des capacités à gérer les cyber-risques montre les résultats de l'ensemble des entreprises du panel de l'étude. Dans l'ensemble, le pourcentage d'entreprises ayant obtenu la mention « expert » cette année est légèrement inférieur, passant de 11% à 10%. Les intermédiaires représentent 16% (même pourcentage que l'an dernier) et les novices 74%.

Modélisation des capacités de gestion des cyber-risques

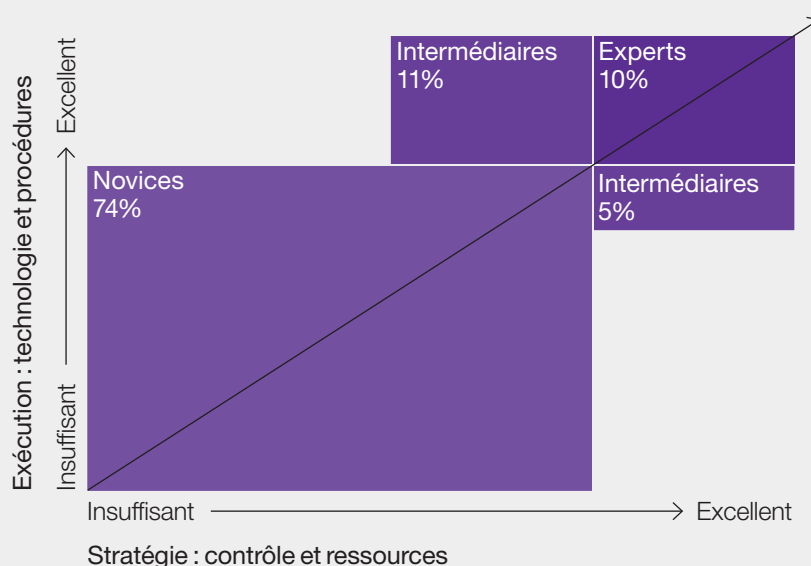
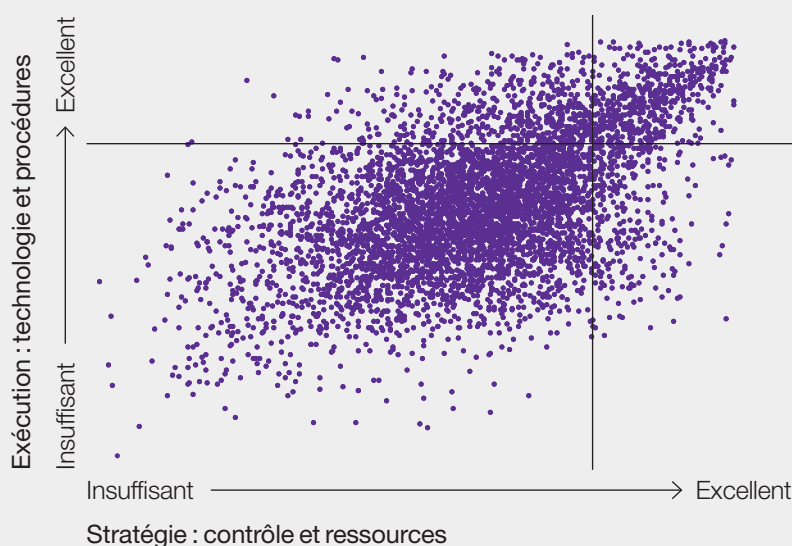


Diagramme de corrélation des capacités de gestion des cyber-risques



Les entreprises prennent des mesures

Les entreprises sont concernées par la cyber-menace et prennent des mesures pour y faire face, on constate notamment une amélioration du processus décisionnel par rapport aux années précédentes.

Davantage d'entreprises désignent désormais un responsable de la cybersécurité

Le pourcentage d'entreprises n'ayant défini aucun rôle en matière de cybersécurité a été divisé par deux (de 32% à 16%). Les 84% restantes ne disposent pas toutes d'un responsable de la cybersécurité ni d'une équipe dédiée à cette question. 19% des entreprises ont recours à un prestataire extérieur pour gérer leur cybersécurité. Trois quarts des petites entreprises ont désormais au moins une personne ou un prestataire en charge de la cybersécurité (contre 56% l'an dernier). Elles sont encore loin des grandes entreprises qui sont 95% à avoir désigné des personnes en charge de la cybersécurité, mais cela reste un indicateur de progrès encourageant.

Davantage d'entreprises prennent des mesures adéquates en cas d'incident

Davantage d'entreprises répondent aux incidents de sécurité en prenant des mesures concrètes. L'année dernière, près de la moitié des répondants (47%) ont indiqué n'avoir rien changé après des incidents de cybersécurité. Cette année, ce pourcentage a diminué de près d'un tiers pour s'établir à 32%. Parmi les novices, ce pourcentage est passé de 51% à 33% et parmi les intermédiaires, de 42% à 31%.

Moins de laxisme, plus de réalisme

Les entreprises sont moins confiantes quant à l'efficacité des mesures de sécurité qu'elles ont mises en place et, dans de nombreux domaines, la confiance décline depuis notre premier rapport en 2017. Cela est sans doute la conséquence non seulement de l'intensification de la cyber-menace, mais également de l'augmentation des règles auxquelles les entreprises sont soumises, comme le RGPD et le Règlement sur la cybersécurité du département des services financiers de l'État de New York (qui impose des obligations aux entreprises offrant leurs services dans l'État de New York semblables à celles que le RGPD impose en Europe). L'immobilisme ne fait qu'aggraver la situation.

Les mesures réglementaires stimulent l'action

Lorsque nous avons demandé aux entreprises quels changements elles avaient éventuellement apportés en conséquence des nouvelles réglementations telles que le RGPD, la grande majorité des entreprises d'Europe continentale (à savoir environ 84%) ont indiqué qu'elles avaient effectivement mis en œuvre quelques changements. Les entreprises britanniques sont un peu moins nombreuses dans ce cas-là (80%). Aux États-Unis, où le RGPD peut être considéré comme une problématique accessoire pour les entreprises qui se s'orientent sur le marché intérieur, cette donnée est très inférieure : près d'un tiers (32%) des entreprises américaines ont indiqué qu'elles n'avaient effectué aucun changement.

L'expertise permet-elle de diminuer les coûts ?

Le coût moyen des incidents subis par les entreprises « expertes » est de 456 000 €, contre 558 000 € pour celles qui ont été jugées « intermédiaires ». Ces montants sont sensiblement plus élevés que le coût moyen des incidents subis par les « novices », mais cela s'explique par le nombre plus important de petites entreprises parmi les novices. Le coût lié aux failles exposé par les petites entreprises est généralement très inférieur à celui subi par les grandes entreprises : 612 000 € en moyenne pour les grandes et très grandes entreprises contre 77 000 € pour les petites et moyennes entreprises.

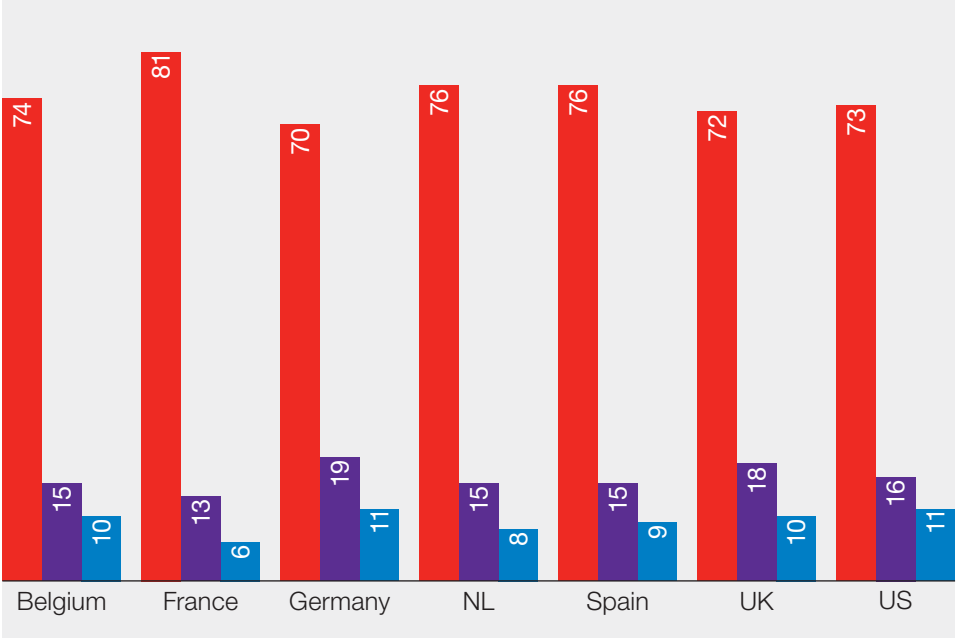
Capacités de gestion des cyber-risques par pays

Plus de quatre cinquième des entreprises françaises (81%) figurent dans la catégorie « novices ». S'agissant du nombre de grandes et très grandes entreprises ayant obtenu la mention « expert », les Pays-Bas et la France ferment la marche (9%). Dans l'ensemble, les entreprises américaines, allemandes et belges ont obtenu les meilleures notes, 10% d'entre elles se classant dans la catégorie « expert ».

Toutefois, on observe une chute drastique du nombre de grandes et très grandes entreprises américaines et allemandes qui obtiennent la mention « expert ». En Allemagne, leur proportion est passée de 20% à 10% et aux États-Unis, de 26% à 11%.

Les données concernant les entreprises américaines et allemandes sont la principale raison expliquant une régression générale du nombre d' « experts » parmi les grandes et très grandes entreprises cette année (21% en 2018 contre 12% cette année). Près de trois-quart d'entre elles (73%) se classent désormais dans la catégorie « novices ». Elles étaient 61% l'an dernier. Étant donné les ressources dont elles disposent et les budgets bien plus importants qu'elles consacrent à la sécurité, ce chiffre a de quoi surprendre.

La grande majorité des pays ne sont pas préparés (%) ● Novices ● Intermédiaires ● Experts



Pourcentage d'entreprises n'ayant assigné aucun rôle en matière de cybersécurité (%)

	2019	2018
Tous pays	16	32
Belgique	12	–
France	12	–
Allemagne	15	31
Pays-Bas	12	36
Espagne	14	26
Royaume-Uni	20	33
États-Unis	20	32

Les données 2018 ne sont pas disponibles pour la Belgique ou la France.

En tant qu'assureur spécialiste, nous assurons nos clients contre les cyber-risques depuis plus de 20 ans, ce qui nous donne une expertise unique pour apprécier les bons et les mauvais usages lorsqu'il s'agit de détecter une cyber-menace et d'y répondre. Cette expérience, associée aux informations que cette étude nous permet de rassembler, nous donne une idée claire des mauvais usages des entreprises et de ce qu'elles pourraient faire pour les améliorer.

Quels sont les bons et les mauvais usages ?

- ✓ Implication de la direction – la cybersécurité est une priorité pour le conseil d'administration ou le propriétaire
 - ✓ Stratégie claire élaborée par plusieurs parties prenantes au sein de l'entreprise
 - ✓ Responsable de la cybersécurité ou équipe dédiée à la cybersécurité
 - ✓ Budget cybersécurité adéquat – en moyenne, les experts dépensent plus d'1 million de dollars de plus que les novices
 - ✓ Évaluation régulière de la chaîne logistique, KPI de sécurité dans les contrats conclus avec les fournisseurs
 - ✓ Procédure – capacité de suivre, documenter, mesurer l'impact
 - ✓ Formation de sensibilisation à la cybersécurité dispensée à l'ensemble du personnel
 - ✓ Tests proactifs – simulations d'attaque
 - ✓ Tests anti-phishing réguliers
 - ✓ Aptitude à apprendre, prendre des mesures et effectuer des changements après un incident
 - ✓ Souscription d'une police de cyber-assurance
-
- ✗ Gestion ad hoc de la cybersécurité – absence de définition claire des responsabilités
 - ✗ Pas de cyberstratégie formelle, pas de budget dédié à la cybersécurité
 - ✗ Dépendance excessive aux technologies, manque de ressources humaines dédiées
 - ✗ Lenteur des mesures en cas d'incident
 - ✗ Formations de sensibilisation du personnel occasionnelles, voire sporadiques
 - ✗ Pas d'évaluation des vulnérabilités de la chaîne logistique
 - ✗ Pas de simulation de cyber-attaques ni de test des réactions des salariés
 - ✗ Simple assurance générale des biens de l'entreprise

Dépenses de cybersécurité

Mieux vaut prévenir que guérir : cette année, nous avons relevé une augmentation significative des dépenses liées aux mesures de cybersécurité, beaucoup anticipant une poursuite de cette tendance cette année.

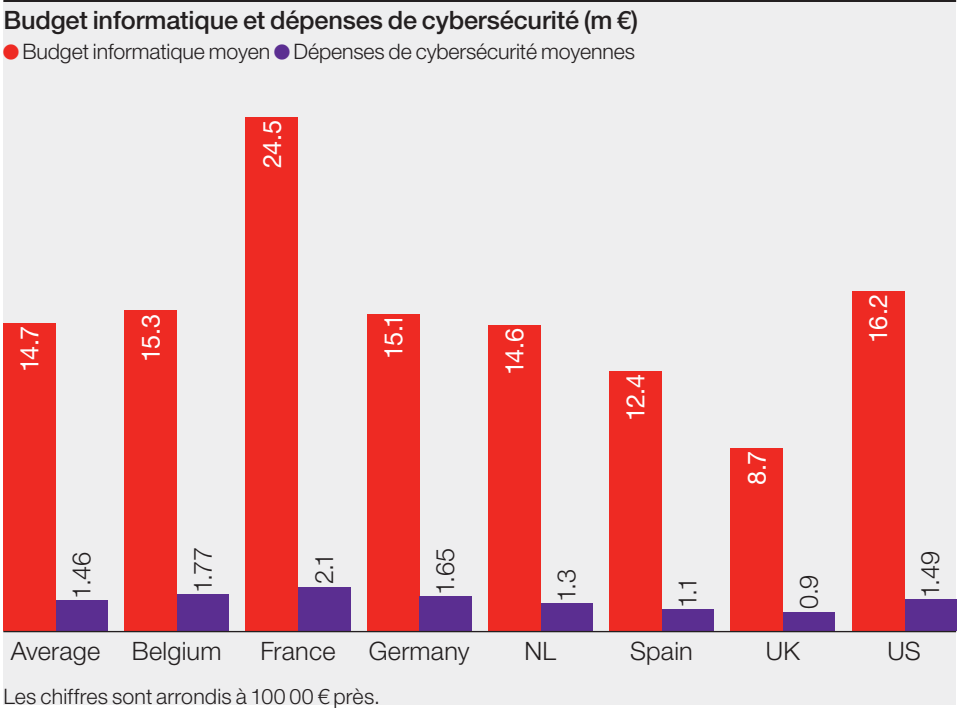
Le rythme s'accélère

Sur l'ensemble du panel d'entreprises de l'étude, nous avons constaté une augmentation marquée des dépenses informatiques générales, qui sont passées en moyenne de 11,2 millions € l'an dernier à 14,7 millions € cette année. Cela s'explique largement par la prise en compte dans cette enquête de la France, où le budget informatique moyen est de 24,5 millions €.

La part des budgets informatiques consacrée à la cybersécurité est à peine plus faible qu'avant (9,9 % des dépenses informatiques totales contre 10,5 % l'an dernier), mais en valeur, elle progresse de près d'un quart (24%) pour atteindre 1,46 millions €.

La prise en compte de la Belgique et de la France cette année a également faussé les données à la hausse. Les dépenses moyennes de cybersécurité des entreprises belges est d'1,77 million € et de 2,1 millions € pour les entreprises françaises. Ces deux montants sont bien au-delà de la moyenne des sept pays considérés :

Si l'on tient compte de l'ensemble des 5 400 entreprises du panel de l'étude, les dépenses de cybersécurité s'élèvent à non moins de 7,9 milliards € sur l'année. En ajustant ce résultat en fonction de l'augmentation de la taille du panel de l'étude cette année, cela représente une hausse de près de 20% par rapport aux données équivalentes de 2018, les grandes entreprises représentant une partie importante de ces dépenses.



Dépenses annuelles moyennes de cybersécurité (€)	
Nombre de salariés	Dépenses annuelles moyennes
1–9	7 000
20–49	37 000
50–99	115 000
100–249	436 000
250–499	930 000
500–999	1 018 000
1 000–4 999	2 336 000
5 000–19 999	4 009 000
20 000+	10 643 000

Réorientation des dépenses pour l'année à venir

Environ deux tiers des répondants (67%) ont indiqué que leurs dépenses de cybersécurité allaient augmenter cette année, contre 59% l'an dernier. Si l'augmentation des dépenses de technologie est toujours un objectif pour 50% des répondants, le nombre d'entreprises prévoyant de consacrer davantage de fonds à la formation des salariés, au personnel dédié à la cybersécurité et aux services de consultants et de tiers est sensiblement en hausse, ce qui laisse penser que les entreprises réorientent leurs priorités sur les ressources humaines et les procédures.

Cela est confirmé par les priorités que les entreprises se sont elles-mêmes fixées pour l'année à venir. Si l'on regarde les domaines d'action auxquels les répondants ont le plus fréquemment attribué un niveau de priorité « élevé » ou « critique », on obtient une bonne indication de l'orientation des dépenses cette année. Une grande partie de cette action s'oriente sur les procédures.

Les entreprises américaines sont les plus nombreuses à prévoir une augmentation de leur budget de cybersécurité, 72% d'entre elles ayant fait état d'une hausse des dépenses en ce sens. Curieusement, ce sont les entreprises qui dépensent déjà le plus d'argent, principalement les grandes entreprises dans l'étude, qui prévoient les plus grandes augmentations budgétaires.

Entreprises prévoyant une augmentation des dépenses de cybersécurité (%)	
Petites entreprises (1–49 salariés)	60
Moyennes entreprises (50–249 salariés)	67
Grandes entreprises (250–999 salariés)	73
Très grandes entreprises (1 000 salariés et plus)	75

Orientation des dépenses de technologie et de ressources humaines pour l'année à venir (%)

Nouvelle technologie de sécurité

2019	50
2018	57

Formation des salariés à la cybersécurité

2019	39
2018	34

Consultants en sécurité et tiers prestataires

2019	31
2018	25

Personnel dédié à la cybersécurité

2019	31
2018	25

Externalisation de la sécurité

2019	30
2018	24

Cyber-assurance

La prise en compte croissante des cyber-risques contribue à susciter l'intérêt des entreprises pour la cyber-assurance, de plus en plus d'entreprises ayant déclaré qu'elles avaient investi ou qu'elles prévoyaient d'investir dans la cyber-assurance.

Qu'est-ce qu'une cyber-assurance ?

Une cyber-attaque peut nécessiter l'implication d'un ensemble experts, tels que des avocats pour effectuer les notifications aux autorités en charge de la protection des données et gérer les contentieux, des informaticiens pour évaluer les failles et restaurer les systèmes informatiques, et des consultants en relations publiques pour gérer la communication avec les médias et le grand public. La cyber-assurance couvre tous ces coûts ainsi que les pertes financières subies, que ce soit en raison d'une perte d'activités ou de plaintes de tiers.

Hausse des souscriptions de polices de cyber-assurance

Nous avons pu observer cette année davantage de souscriptions et une meilleure compréhension de l'intérêt de souscrire une police de cyber-assurance : 41% des répondants ont indiqué que leur entreprise avait souscrit une cyber-assurance, contre 33% il y a un an. De même, 30% des entreprises ont déclaré qu'elles prévoyaient d'adopter une cyber-assurance dans les 12 prochains mois, contre 25% l'an dernier.

Le pourcentage de ceux ayant répondu « pas certain de savoir ce qu'est une cyber-assurance ? » a diminué de moitié depuis notre rapport de 2017, passant de 6% à 3%. Néanmoins, une certaine confusion subsiste parmi les petites entreprises car 6% d'entre elles continuent de dire qu'elles ne sont pas certaines de savoir ce qu'est une cyber-assurance.

Sans surprise, les entreprises qui obtiennent la mention « expert » dans notre modélisation des capacités de gestion des cyber-risques, sont les plus nombreuses à avoir souscrit une cyber-assurance (59%), et les grandes entreprises sont beaucoup plus nombreuses à avoir souscrit une cyber-assurance que les petites entreprises.

Plus de la moitié des très grandes entreprises indiquent avoir souscrit une police de cyber-assurance, contre 27% des petites entreprises de moins de 50 salariés.

Souscription d'une police de cyber-assurance (%)

Nous disposons déjà d'une cyber-assurance



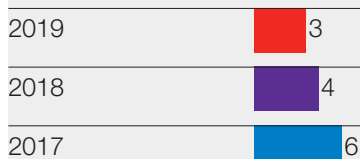
Nous prévoyons de souscrire une police de cyber-assurance dans les 12 prochains mois



Nous ne prévoyons pas de souscrire une police de cyber-assurance



Pas certain de savoir ce qu'est une cyber-assurance



Méthodologie de recherche

Les conclusions présentées dans ce rapport sont établies à partir d'un échantillon représentatif d'entreprises par taille et par secteur, qui comprend notamment celles qui sont en première ligne dans la lutte contre la cybercriminalité.

Niveau hiérarchique des répondants (%)	
Administrateur	51
Vice-président	24
Directeur	13
Cadre de niveau C	12

Si l'ensemble des personnes interrogées sont engagées dans les efforts de cybersécurité de leur entreprise, 70% d'entre elles sont les décideurs finaux ou font partie de l'équipe décisionnaire.

Périmètre du rapport

Hiscox a sollicité Forrester Consulting pour évaluer les capacités de gestion des cyber-risques des entreprises. Au total, 5 392 professionnels impliqués dans la stratégie de cybersécurité de leur entreprise ont été contactés (plus de 1 000 personnes par pays pour le Royaume-Uni, les États-Unis et l'Allemagne et 500 pour la Belgique, la France, l'Espagne et les Pays-Bas). 39% des répondants représentaient des entreprises de moins de 50 salariés (petites entreprises), 16% des entreprises de taille moyenne (entre 50 et 250 salariés), 16% des grandes entreprises (entre 250 et 999 salariés) et les 28% restants, des très grandes entreprises (1 000 salariés ou plus). Les répondants ont rempli le questionnaire en ligne entre le 22 octobre et le 7 décembre 2018.

Changements dans cette édition

Un certain nombre de changements ont été effectués pour étendre le périmètre du rapport cette année et le rendre plus pertinent d'un point de vue statistique, notamment pour les petites entreprises. Les entreprises du panel de l'étude représentent désormais sept pays, avec l'ajout cette année de la Belgique et de la France. Le nombre de répondants est passé de 4 100 à environ 5 400, ce qui fait du rapport Hiscox sur la gestion des cyber-risques l'un des plus complets dans sa catégorie.

La répartition au sein du panel entre les petites entreprises (moins de 50 salariés), moyennes entreprises (50 –249), grandes entreprises (250–999) et très grandes entreprises (plus de 1 000) a également été modifiée. Les petites entreprises représentent désormais 40% du panel, contre 33% l'an dernier. Les entreprises de cinq salariés ou moins représentent quant à elles 5% du panel. Le nombre de très grandes entreprises a également augmenté, passant de 17% à 27%. Le groupe intermédiaire des moyennes et grandes entreprises représente désormais 33% du total contre 50% l'an dernier. Il y a un dernier changement. Les questions relatives au budget informatique, aux dépenses et ressources dédiées à la cybersécurité ont été posées cette année uniquement aux décideurs finaux ou aux membres de l'équipe décisionnaire sur ces sujets.

02 Résumé	03 Comparaison par pays	04 L'étendue du problème	06 Impact financier
08 Modélisation des capacités de gestion des cyber-risques	12 Dépenses de cybersécurité	14 Cyber-assurance	15 Méthodologie de recherche

Répartition des répondants par taille d'entreprise

Petites entreprises (1–49 salariés)

15%

2–510%

6–94%

10–197%

20–4913%

39%

Moyennes entreprises (50–249 salariés)

50–997%

100–2499%

16%

Grandes entreprises (250–999 salariés)

250–4997%

500–9999%

16%

Très grandes entreprises (1 000 salariés et plus)

1 000–4 99916%

5 000–19 9998%

20 000+4%

28%

Secteur d'activité des répondants (%)	
Technologie, média et communications	16
Services professionnels	11
Fabrication	9
Commerce de gros et de détail	8
Services aux entreprises	8
Services financier	8
Construction	7
Pharmacie et santé	7
Transport et distribution	5
Voyages et loisirs	5
Agro-alimentaire	5
Énergie	3
Immobilier	3
Organismes publics	3
Organismes sans but lucratif	2

Service auquel appartiennent les répondants (%)	
Informatique et technologie	22
Opérations	11
Finance	10
Marketing et communications	8
Commercial	7
Gestion des risques	6
Gestion de produit	6
Ressources humaines	6
Achats	5
Direction juridique	5
e-commerce	5
Haute direction	4
Propriétaire	3

Hiscox Ltd
4th Floor
Wessex House
45 Reid Street
Hamilton HM 12
Bermudes
T +44 (0)20 7448 6000
E enquiries@hiscox.com
hiscoxgroup.com

19882 07/19

