HISCOX
ASSURANCES

Rapport Hiscox 2020 sur la gestion des cyber-risques

Le quatrième rapport annuel Hiscox sur la gestion des cyber-risques a été élaboré en collaboration avec l'entreprise de recherche Forrester. Le rapport n'offre pas simplement un aperçu rapide des capacités de gestion des cyber-risques des entreprises, il propose également un tableau des meilleures pratiques pour lutter contre une menace en perpétuelle évolution. Ce rapport est élaboré à partir d'une étude réalisée auprès de dirigeants, directeurs de service, responsables informatiques et autres professionnels clés. Sélectionnés au sein d'un échantillon représentatif d'entreprises de huit pays classées par taille et par secteur, ce sont les personnes en première ligne dans la lutte contre la cybercriminalité.

Relever le défi de la cyber-menace

Un changement radical dans la préparation à la gestion du risque cyber est clairement observable.

Gareth Wharton
Cyber CEO, Hiscox

Le rapport de cette année nous permet de tirer une conclusion très positive. Après deux années où les progrès semblaient stagner, on assiste clairement à un changement radical des capacités de gestion des cyber-risques. Cela ressort non seulement des indicateurs composant notre modélisation des capacités de gestion des cyber-risques, mais s'observe également par la hausse des activités et dépenses réalisées pour répondre à cette menace.

Ce n'est pas trop tôt. Si les entreprises sont moins nombreuses à avoir signalé une faille, le coût et l'intensité des actes de cybercriminalité semblent nettement plus importants. Le nombre d'entreprises ayant versé une rançon à la suite d'une infection par un malware fait froid dans le dos. Personne n'oserait remettre en cause l'étendue du problème.

Les entreprises sondées pour notre rapport ont été interrogées avant l'épidémie de coronavirus, leurs conclusions reflètent donc leurs perspectives dans des temps de plus grande quiétude. L'augmentation du nombre d'entreprises classées comme expertes cette année est indubitablement un signe encourageant en vue de la protection des entreprises dans un paysage de cyber-menace en perpétuelle évolution.

Si un haut niveau de capacité de gestion des cyber-risques ne peut pas constituer une garantie de sécurité, il existe des mesures crédibles, dont un bon nombre sont détaillées dans ce rapport, que les entreprises peuvent prendre pour minimiser leur vulnérabilité, apporter une réponse adéquate et se remettre en ordre de marche. Il est ici question de défense en profondeur et de développement de la résilience.

De notre point de vue d'assureur de cyber-risques, nous estimons que, lorsqu'elle se produit, une faille ne doit pas être la fin du processus. Il est intéressant de constater le nombre de «cyber-experts» de ce rapport à avoir souscrit une police de cyber-assurance dédiée, non seulement pour se protéger financièrement, mais également pour pouvoir s'appuyer sur l'expertise spécialisée qu'elle apporte dans les moments cruciaux. De même, il est primordial de tirer les leçons d'un incident et de s'assurer de mettre en œuvre ces enseignements et d'améliorer la planification et la résilience aux incidents ultérieurs. Comme le rapport l'illustre, c'est précisément ce qu'un grand nombre d'experts font.

La souscription d'une police de cyber-assurance dédiée demeure néanmoins minoritaire avec plus de la moitié des entreprises de notre rapport qui s'appuient encore sur une assurance plus générale. On peut se demander pourquoi. Ces entreprises ont presque systématiquement des garanties couvrant les incendies et les vols, pourtant, le rapport indique qu'elles ont près de 20 fois plus de risques de subir un cyber-incident, à savoir 30% contre environ 2% pour les incendies et vols cumulés au Royaume-Uni.

Le rapport de cette année souligne l'importance de faire évoluer le comportement des salariés. Cette démarche prend souvent la forme d'une formation de sensibilisation à la cybersécurité dans l'entreprise. Il s'agit d'un autre domaine dans lequel un assureur a un rôle important à jouer. Notre plateforme de formation en ligne, HiscoxCyberClear Academy, offre une formation de sensibilisation à la cybersécurité aux employés de nos clients, et plus de 12,000 personnes ont à ce jour suivi la formation. Nous remarquons que ceux qui ont suivi cette formation sont souvent plus prompts à signaler une faille, ce qui nous permet de les aider à remettre leur entreprise en ordre de marche plus rapidement et avec de meilleurs résultats.

La capacité de gestion des cyber-risques s'apprécie à plusieurs niveaux. Nous espérons que ce rapport, avec ses nombreux exemples de bonnes pratiques, aidera les lecteurs à mieux comprendre le défi de la cyber-menace et à y répondre.

Résumé

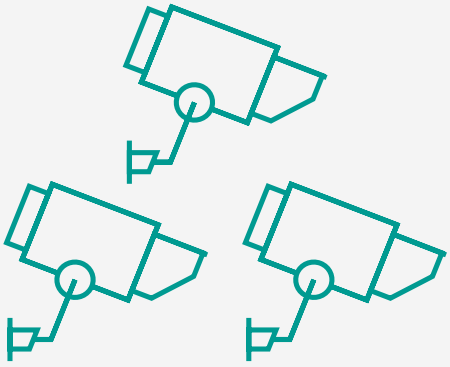
Un changement radical dans la préparation à la gestion du risque cyber est clairement observable.

Soyons clairs

Le nombre d'entreprise ayant obtenu la mention «expert» suite à notre modélisation des capacités de gestion des cyber-risques a presque doublé cette année, passant de 10% à 18%.

Les dépenses de sécurité augmentent

Les entreprises ont augmenté leurs dépenses de cybersécurité de 39%. Les entreprises expertes ont dépensé davantage et prévoient de poursuivre cette tendance.



Les entreprises perdent plus

Le total des pertes par les entreprises touchées s'èléve à 1,6 milliards €. En comparaison, l'an dernier ce chiffre s'établissait à 1,1 milliards €.

Augmentation des pertes liées aux cyber-incidents

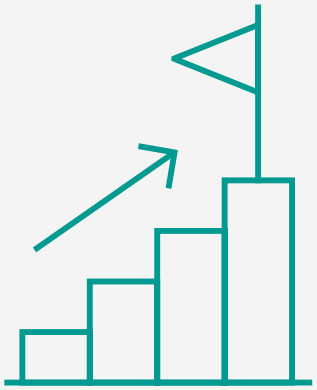
L'impact financier pour les entreprises ciblées a presque été multiplié par six, pour s'établir à un coût médian de 50,000€.

Baisse du nombre de cyber-événements

Le nombre d'entreprises touchées par un cyber-événement a chuté, passant de 61% à 39% du panel.

Des pertes record liées aux cyber-événements

Les pertes les plus importantes liées aux cyber-événements ont été rapportées par une entreprise britannique de services financiers: 79,9 millions €.



Paiement de rançon

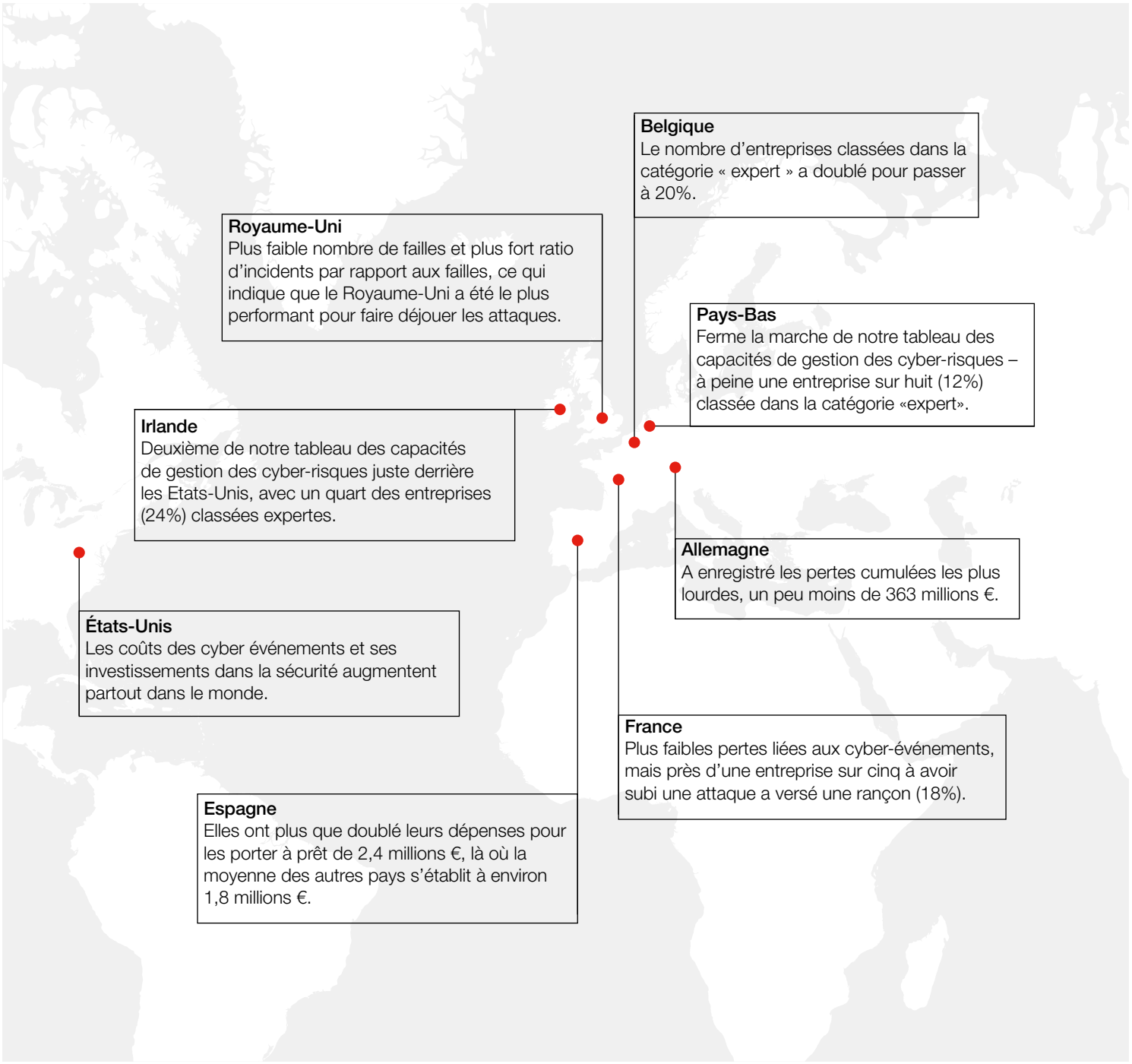
Plus de 6% des entreprises du panel ont versé une rançon. Leur somme cumulée était de 335 millions €.

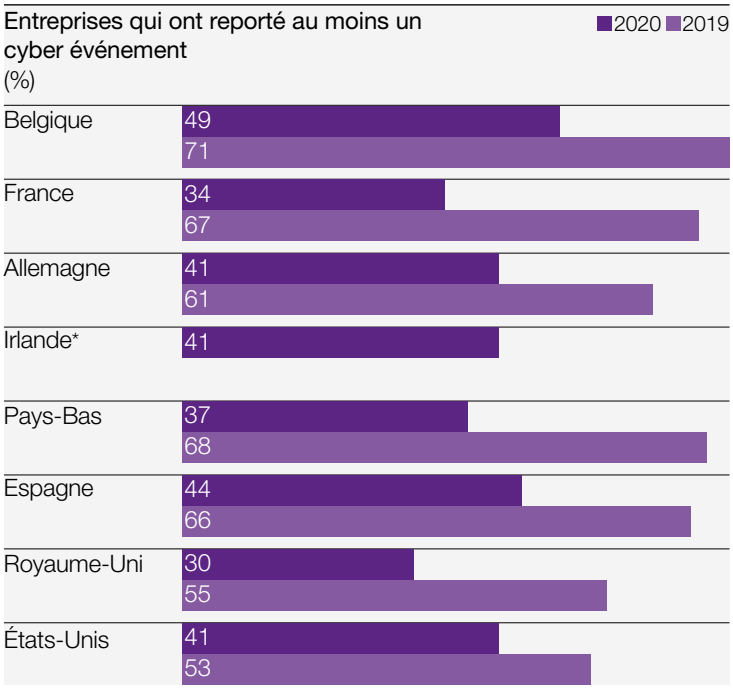
Signes positifs

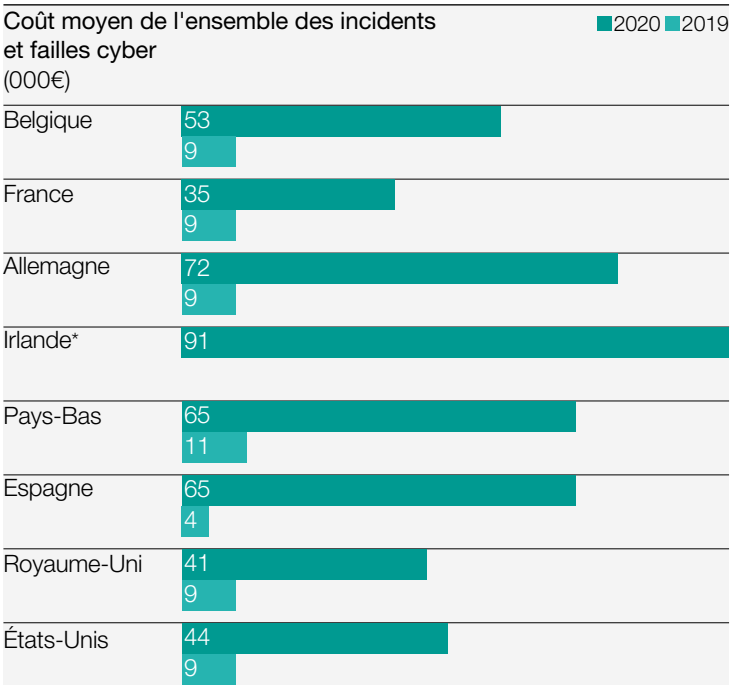
Deux fois plus d'entreprises ont réagi à une faille cette année en prenant des mesures additionnelles, comme l'imposition de nouvelles exigences de sécurité, et l'augmentation des investissements dans la formation des salariés.

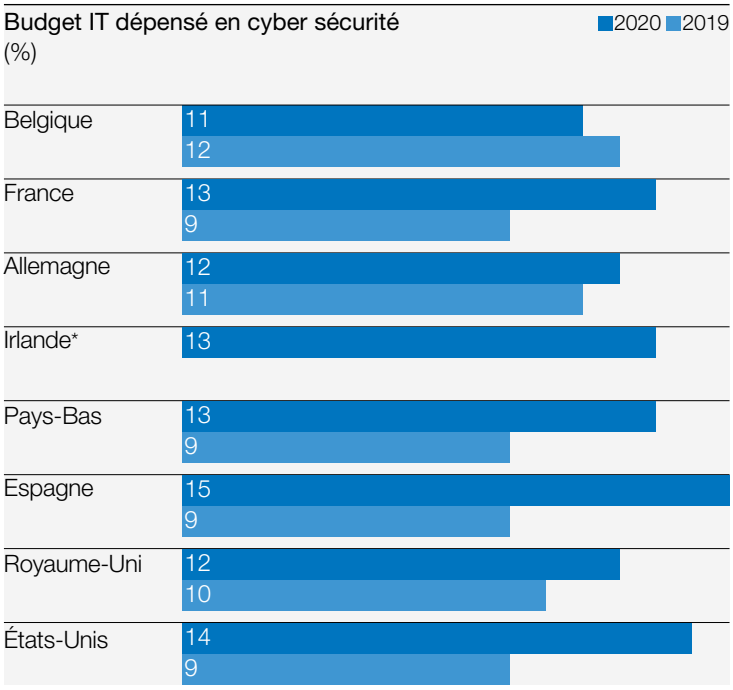
Comparaisons par pays

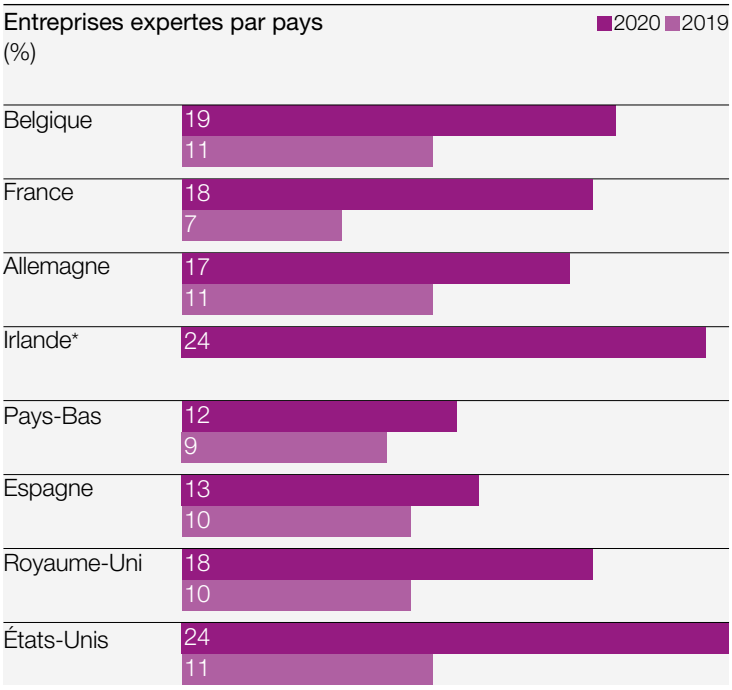
Les coûts des cyber événements et ses investissements dans la sécurité augmentent partout dans le monde.











*Données valables uniquement pour 2020.

L'étendue du problème

Tandis qu'un nombre moins important d'entreprises a éprouvé un cyber incident ces dernières années, leurs coûts est monté en flèche.

Des cibles moins nombreuses, mais des pertes plus importantes
Le nombre d'entreprise ayant signalé un événement de cybersécurité au cours des 12 derniers mois a diminué cette année, passant de 61% à 39%. On peut s'en réjouir. La mauvaise nouvelle est que les conséquences financières ont été bien plus importantes qu'avant.

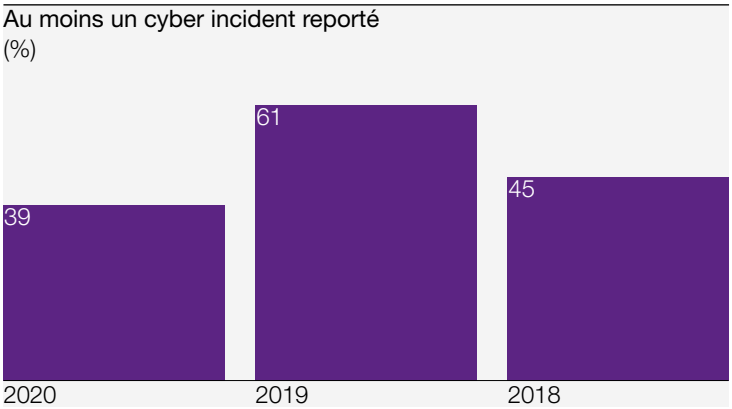
Au-moins un cyber incident reporté

Pour la première fois, nous avons demandé aux entreprises de quantifier séparément le nombre de cyber-incidents et de failles qu'elles ont subis, ce qui nous a permis d'affiner l'analyse de la résilience des entreprises. Un cyber-incident est tout événement qui n'a pas pour effet de compromettre la confidentialité, l'intégrité ou la disponibilité de données ou informations. Une faille de cybersécurité est un événement qui compromet la confidentialité, l'intégrité ou la disponibilité de données ou informations causant une perte importante à la société. Parmi celles ayant rapporté un quelconque cyber-événement, le nombre médian d'incidents était de 50 et le nombre médian de failles était de 15. Les entreprises belges et allemandes ont été les plus ciblées avec un nombre médian d'incidents de 100 et 80, respectivement. Si l'on observe les failles, la situation était inversée, ce qui semble indiquer que les entreprises allemandes ont moins bien réussi à se protéger des pirates informatiques.Si on considère l'ensemble du panel d'entreprises participantes (y compris celles qui n'ont déclaré aucun cyber-incident ou qui ont répondu «ne sait pas»), l'entreprise médiane a subi 20 incidents et six failles.

Emergence de «super cibles»
Les chiffres sont largement impactés par le fait qu'un nombre relativement faible d'entreprises dans chacun des huit pays consultés ont signalé 500 événements ou plus dans chaque catégorie. Ces tendances sont apparues parce que nous avons modifié notre questionnaire cette année, permettant aux participants de donner des réponses libres au nombre de cyber-événements qu'ils avaient enregistrés.

On pourrait penser qu'il ne s'agit que de très grandes entreprises. Ce n'est pas le cas (voir le diagramme). Il y a des super cibles dans chacun des cinq segments de tailles d'entreprise que nous avons définis. Parmi les entreprises de plus petite taille, les résultats sont surprenants.

Ces chiffres peuvent être expliqués de plusieurs manières. Dans de nombreux secteurs, la majorité des micro-entreprises n'ont aucun responsable en charge de la cybersécurité. Les plus petites entreprises du secteur des transports et de la distribution semblent particulièrement vulnérables, 59% d'entre elles ayant déclaré qu'elles n'avaient aucun préposé interne ou externe à la



cybersécurité. Dans le même temps, dépendre d'un prestataire de services peut également avoir l'effet inverse lorsque celui-ci fait lui-même l'objet d'une attaque. Il est également envisageable que certaines entreprises aient été un peu larges dans leur décompte en signalant les emails de spam.

Parmi les explications à cette tendance, on peut avancer le manque de mesures de prévention dans certaines petites entreprises. L'analyse des données suggère que les entreprises disposant de moins de 12 postes informatiques qui n'ont pas généralisé l'installation d'anti-virus/anti-spyware dans l'entreprise sont particulièrement susceptibles de constituer des super cibles.

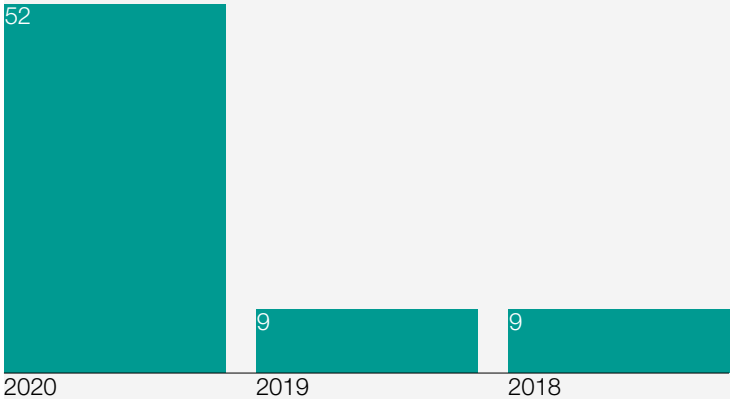
Pour toutes ces raisons, les plus grandes entreprises étaient plus susceptibles de constituer des cibles que les petites entreprises. Plus de la moitié (51%) des très grandes entreprises (plus de 1,000 salariés), ont indiqué qu'elles avaient enregistré au moins un cyber-incident. Elles ont également fait état de loin du plus grand nombre de cyber-incidents (une médiane de 100) et de failles (80). Si elles ont très probablement constitué des cibles privilégiées par rapport au reste du panel, elles ont également été plus performantes pour déceler ces attaques.

L'insuffisance des dépenses pertinentes de cybersécurité semble être une tendance générale. Dans la grande majorité des secteurs, ce sont les entreprises disposant de plus de 700 postes informatiques dont moins de 8% du budget informatique a été consacré à la cybersécurité, qui ont constitué des super cibles.

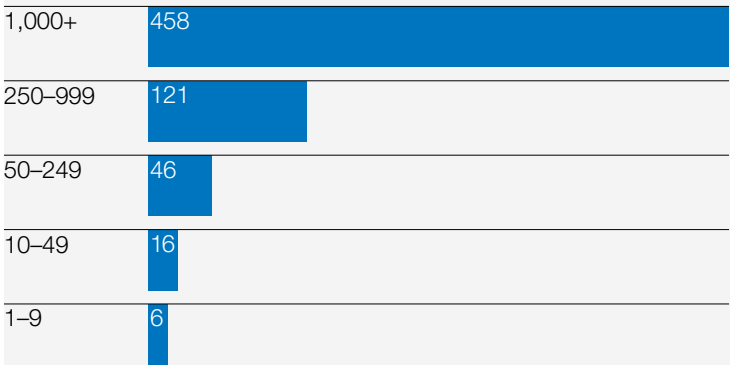
1,6 milliards €

Total des coûts dépensés par notre échantillon du fait de cyber événements au cours des 12 derniers mois.

Coût médian de tous les cyber-événements
(000€)



Coût de l'ensemble des incidents et failles
Employés (000€)



Les secteurs qui ont été les plus lourdement touchés sont les services financiers, la fabrication et les TMT, 44% des entreprises de chacun de ces secteurs ayant rapporté au moins un incident ou une faille. Curieusement, ce sont ces trois secteurs qui ont obtenu les meilleurs résultats dans notre modélisation des capacités de gestion des cyber-risques, mais les entreprises sont souvent amenées à devenir des expertes lorsqu'elles sont dans des secteurs fortement ciblés.

Un grand nombre de «ne sait pas»
Une tendance préoccupante est que 11% de l'ensemble des répondants ont déclaré qu'ils ne savaient pas combien de fois ils avaient été ciblés. Ce chiffre n'était que de 4% l'an dernier. Une autre observation étonnante est que les entreprises les plus nombreuses à avoir répondu «ne sait pas» (15%) sont des entreprises de plus de 1,000 salariés.

Il convient de relever que la baisse du nombre total d'entreprises ayant rapporté un cyber-événement peut s'expliquer par la place plus importante accordée aux micro-entreprises dans le panel d'études cette année. Environ 63% des entreprises de moins de dix salariés ont déclaré n'avoir subi aucun incident ni aucune faille. Toutefois, près de la moitié d'entre elles (49%) n'ont pas de responsable de la cybersécurité et il pourrait ainsi y avoir des événements non pris en compte.

Des coûts en hausse atteignant 1,6 milliards €
Les chiffres de cette année illustrent le prix à payer pour avoir une présence en ligne aujourd'hui. Le coût médian payé par les 1,971 sociétés qui ont subi des cyber-incidents et des failles, et qui ont évalué leurs impacts financiers au cours des 12 derniers mois, s'élève à 51,200€. Cela représente près de six fois le coût observé l'année précédente (9,000€).

Coût médian de l'ensemble des cyber événements

En additionnant le coût de l'ensemble des cyber-événements rapportés par notre panel d'étude, nous arrivons à un coût total de 1,6 milliards €. Ce chiffre est à comparer aux 1,1 milliards € relevés l'an dernier, alors que le nombre de société attaquées était près de 33% supérieur.

Qui a été le plus vulnérable?
Pour résumer, les plus grandes sociétés sont celles qui ont payé leur présence en ligne au prix le plus fort. Cela ne devrait pas surprendre car elles ont été également les plus lourdement ciblées.

Coût de tous les incidents et failles

Au-delà des chiffres médians, l'impact financier a été extrêmement différent selon les pays, les secteurs et les sociétés. Le total de pertes le plus élevé enregistré par une société est de 79,9 millions € (une entreprise britannique de services financiers), tandis que la perte la plus élevée pour un événement unique est de 14,4 millions € (une entreprise de services professionnels britannique). En comparaison, le coût médian du pire incident unique est d'à peine 3,700€.

Pire incident ou faille

Les entreprises irlandaises et allemandes ont enregistré les pertes médianes les plus fortes, mais l'impact a été largement réparti. Parmi les entreprises ayant subi des attaques, le coût médian pour les entreprises du secteur de l'énergie a été multiplié par plus de trente, tandis que d'autre secteurs ont dû faire face à des pertes plusieurs fois supérieures à celle de l'année précédente. Les chiffres suggèrent que les cybercriminels ont de plus en plus tendance à considérer les entreprises du secteur de l'énergie et de la fabrication comme des cibles lucratives.

L'avis d'Hiscox

Nous avons constaté un changement dans le comportement des pirates au cours des six à douze derniers mois, en ce qu'ils s'attaquent plus à certains secteurs comme l'énergie et la fabrication. Nous pensons qu'il y a trois raisons à cela: dépendance importante à l'automatisation (gérée par des ordinateurs); secteurs en retard en matière de cyber-résilience (sauvegardes inadéquates, insuffisance des procédures de planification et de test concernant le rétablissement en cas de catastrophe); pour ces raisons, les entreprises de ces secteurs sont moins tolérantes à ce qui prend souvent la forme d'une panne très impactante, et constituent des cibles de choix pour les attaques par ransomware.

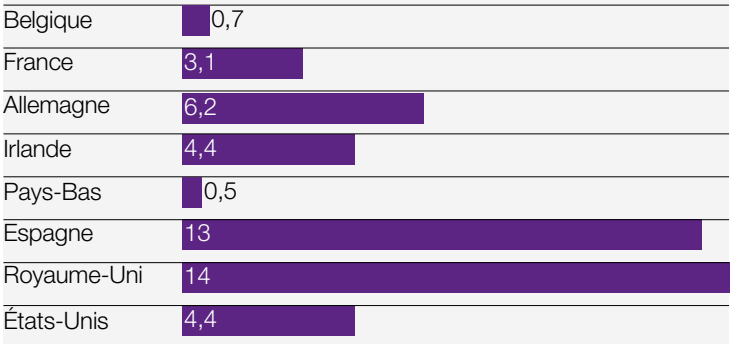
Ransomware: une entreprise lucrative

Les chiffres de cette année donnent un aperçu terrifiant du coût et de la fréquence des attaques par malware et ransomware. Nous avons demandé aux répondants de détailler les types d'incidents et de failles qu'ils avaient subis.

Type de failles les plus fréquentes

Les très grandes entreprises ont été plus nombreuses que les petites entreprises à avoir rapporté des failles dans la plupart des catégories. Cela peut signifier qu'elles constituent des cibles plus lucratives ou qu'elles ont simplement été meilleures pour identifier les attaques.

Pire incident/faille
(m€)



Secteur les plus lourdement touchés
Pertes médianes (€)

	2020	2019
Energie	306,000	9,000
Fabrication	91,000	11,000
Services financiers	151,000	27,000
TMT	69,000	9,000
Pharmacie	55,000	9,000

Type de failles les plus fréquentes
(%)

350

Entreprises de notre échantillon ont reporté avoir payé une rançon après un ransomware ou une attaque malware.

Infections par malware et ransomware
incidents et failles

	Malware sans ransomware	Malware avec ransomware
Nombre d'attaques	173	411
Coûts moyens	447,000€	843,000€
Pertes maximales pour une même société	9,2m€	46m€
Perte unique la plus importante	1,4m€	6,4m€
Total des pertes	77m€	346m€

Les chiffres les plus spectaculaires concernent les infections par malware et ransomware. Dans l'ensemble, 350 entreprises (soit environ une entreprise sur six ayant signalé un cyber-événement – 16%) ont versé une rançon à la suite d'une attaque par ransomware.

Qu'une rançon ait été payée ou non, les pertes plus importantes étaient presque 3 fois plus importantes pour les entreprises ayant subi une attaque par ransomware par rapport à celles ayant subi un malware. 821,000€ contre 436,000€. Les plus fortes pertes pour n'importe quelle entreprise ayant inclus des coûts autres que ceux de ransomware, étaient 5 fois plus élevés, avec 44,8 millions €.

Infections par malware et ransomware

Les chiffres montrent l'importance d'une bonne détection avant que le malware ne devienne un ransomware. Parmi les entreprises ayant signalé un quelconque cyber-événement, les entreprises américaines et françaises sont les plus nombreuses à avoir versé une rançon (18% alors que la moyenne s'établit à 16%). La bonne nouvelle est que davantage d'entreprises ont déclaré avoir récupéré leurs données depuis une sauvegarde ou avoir reconstitué leurs données sans devoir payer une rançon (19% et 17%, respectivement).

L'avis d'Hiscox

Nous assistons à une évolution des techniques d'attaque par ransomware. Généralement, dans les attaques de grande ampleur, il y a deux phases distinctes après l'infection initiale: un mouvement latéral – les pirates recherchent des éléments de valeur (données RH, financières) et évaluent la taille de la cible pour déterminer le montant de la rançon; attaques par ransomware – elles se produisent souvent le week-end, laissant moins de chance pour réagir et permettant aux pirates de causer davantage de dommages. Il peut généralement se passer entre une et trois semaines entre ces deux phases. Les sociétés disposant de bonnes capacités de détection peuvent stopper une attaque pendant ce laps de temps et subir ainsi des désagréments moins durables, avec un coût global plus faible et un impact moindre sur les affaires.

Impacts de plus long-terme

Les incidences plus légères d'une faille de cybersécurité ne sont souvent pas mentionnées ou sont simplement trop difficiles à quantifier. Elles sont néanmoins tout aussi graves. Davantage de répondants ont mentionné cette année des difficultés à attirer de nouveaux clients (15% des entreprises ciblées, contre 5% auparavant), la perte de clients (11% contre 5% avant) ou la perte de partenaires commerciaux (12% contre 4% l'an dernier).

Près d'une entreprise française sur cinq (19%) a déclaré avoir plus de difficultés à attirer des clients après un incident ou une faille. Environ 16% des entreprises belges ont perdu des partenaires commerciaux (alors que la moyenne est de 12%).

Dans l'ensemble, 15% des entreprises ciblées ont indiqué avoir réévalué la cybersécurité de leur chaine logistique (contre 8% l'année précédente) ou avoir fait plus fréquemment l'objet d'une telle évaluation par leurs propres clients (15% contre 10%). La mauvaise publicité, affectant l'image de marque ou la réputation de la société, a été mentionnée par 14% des répondants (contre 5% l'an passé). Une entreprise sur huit (13%) a déclaré avoir observé une chute de ses indicateurs de performance commerciale, comme la valeur de son action (contre 5% l'année précédente).

Comment résumer les données de cette année?

Tandis que le nombre de compagnies touchées par des cyber événements baisse, la fréquence et l'intensité des attaques sont en forte hausse. Toutefois, cela reste clairement faible comparé aux coûts additionnels causés par le ransomware, c'est une tendance qui concerne toute personne impliquée dans la cyber sécurité.

Modélisation des capacités de gestion des cyber-risques

Il y a une augmentation bienvenue du nombre de sociétés obtenant la mention "expert" à la suite de notre test d'évaluation des capacités de gestion des cyber-risques.

Les grandes entreprises montrent la voie

Le nombre de sociétés obtenant la mention «expert» dans notre modélisation des capacités de gestion des cyber-risques a presque doublé en un an, passant de 10% à 18%. De la même manière, le nombre d'entreprises obtenant la mention «novice» a chuté de 74% à 64%. Cette évolution fait suite à une légère baisse des notes d'évaluation des capacités de gestion des cyber-risques l'année précédente, laissant penser, alors, que les progrès avaient marqué le pas.

Le niveau de matrise du risque cyber des entreprises

L'inclusion pour la première fois des sociétés irlandaises a contribué à tirer vers le haut le résultat moyen. Les entreprises irlandaises partagent la tête du classement avec les entreprises américaines, 24% d'entre elles obtenant la mention «expert», et ont pratiquement toutes désigné un responsable en charge de la cybersécurité ou une équipe dédiée (89%).

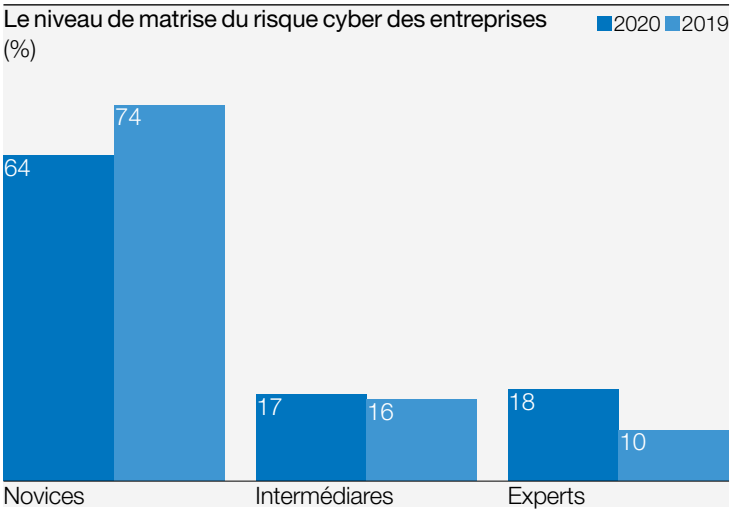
Cela peut s'expliquer par le grand nombre d'entreprises internationales de finance et de technologie à avoir choisi l'Irlande comme lieu d'implantation principal en Europe, bien que les résultats du pays dans ces secteurs ne soient pas très éloignés de la moyenne.

Cela étant dit, chaque pays a contribué à cette amélioration. La France, qui était à la traine lors des deux précédents rapports a vu sa part d'entreprises expertes tripler, passant de 6% à 18%, une tendance venant sans doute récompenser les niveaux exceptionnels de dépenses en matière de cybersécurité au cours des deux dernières années.

La taille reste la clé

La gestion des cyber-risques est clairement un domaine dans lequel la taille compte. Les grandes sociétés ont des ressources plus importantes. Il existe une corrélation évidente entre le nombre de personnes exerçant une fonction de sécurité et les résultats d'une entreprise en matière de gestion des cyber-risques. A titre d'exemple, les sociétés employant plus de 50 personnes dans leur équipe de sécurité constituent uniquement 11% du panel mais représentent 19% d'expertes. Dans les très grandes entreprises employant plus de 1,000 salariés, 29% disposent d'équipes de sécurité de cette taille.

Les grandes sociétés dépensent davantage que leurs homologues de petite taille. Tandis que les micro-entreprises ont dépensé 11,818€ dans la cybersécurité l'année passée, les entreprises de plus de 1,000 salariés ont dépensé en moyenne 7,27 millions €. Dans l'ensemble, ces dépenses ont été réalisées pour acquérir de l'expertise. Les entreprises se classant expertes ont dépensé en moyenne 3,8 millions € dans la cybersécurité, les novices n'ayant quant à elles dépensé en moyenne que 1,18 millions €.



Il est donc intéressant de constater qu'avec plus d'entreprises de petite taille dans le panel cette année, les résultats de l'évaluation des capacités de gestion des cyber-risques se sont encore améliorés. Cela s'explique en grande partie par le fait que le nombre de moyennes, grandes et très grandes entreprises classées comme expertes a été multiplié par deux (voire plus) par rapport à l'année dernière.

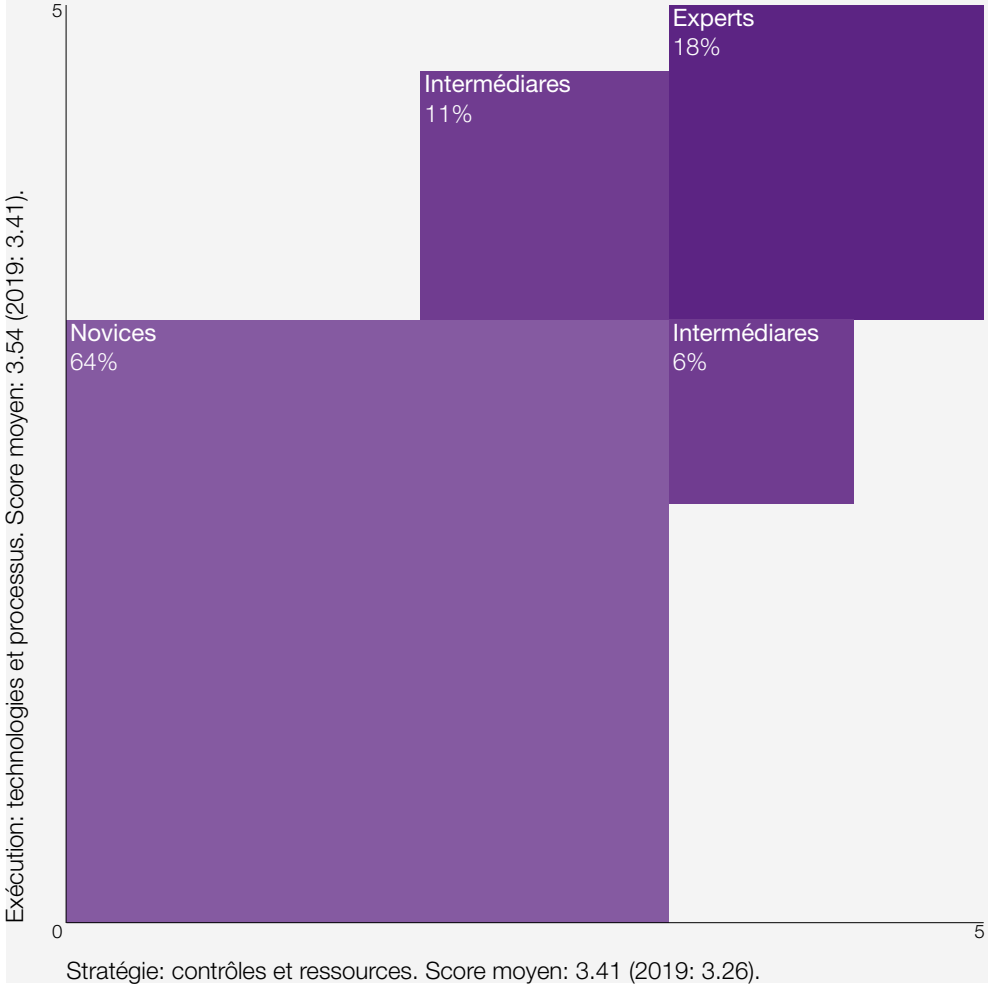
Par contraste, près de quatre micro-entreprises sur cinq embauchant entre un et 9 salariés (79%) se sont classées comme «novices». Parmi tous les répondants, le nombre de personnes ayant répondu que leur entreprise n'avait désigné aucune personne en charge de la cybersécurité a progressé de 16% à 20% (cette tendance concerne 48% des micro-entreprises). Le nombre d'entreprises ayant recours à des prestataires de service externes est resté constant, s'établissant à 19%.

2x

Le nombre d'entreprises qualifiées comme "expertes" a presque doublé en un an.

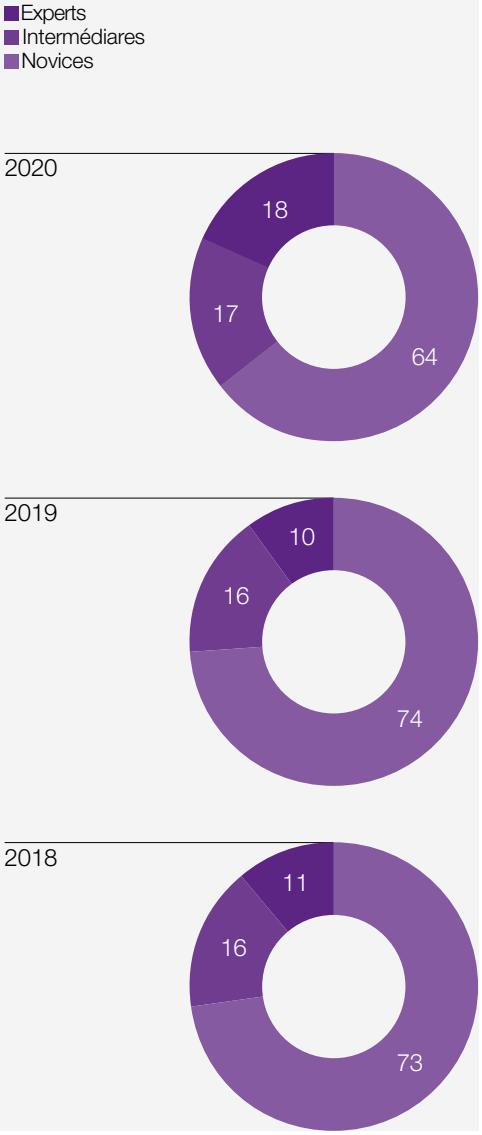
Comment la modélisation est-elle élaborée?

Notre modélisation des capacités de gestion des cyber-risques mesure l'alignement des capacités des entreprises par rapport aux meilleures pratiques dans quatre domaines, stratégie de contrôle et ressources d'un côté et technologie et procédures de l'autre. Les entreprises qui obtiennent quatre sur cinq sur les deux axes sont considérées comme «expertes». Celles qui obtiennent cette note sur un axe seulement sont «intermédiaires». Celles qui n'y parviennent sur aucun axe sont des «novices».



Evolution de la compétence cyber

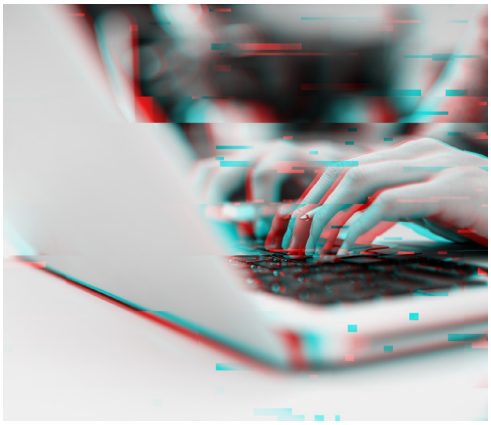
(%)



Qu'est-ce que les experts peuvent enseigner aux autres?

Respecter les fondamentaux
Identifier chaque appareil dans l'entreprise. Sauvegarder les données à distance. Et tirer les enseignements de chaque incident ou faille. Les experts sont plus enclins à durcir leurs règles à la suite d'une faille, via une évaluation régulière de la sécurité, la mise en place de mesures de sécurité et d'audit additionnels et l'augmentation des dépenses de gestion de crise.

Suivre un cadre
Score moyen que toutes les portes et fenêtres virtuelles sont fermées. Un cadre comme celui créé par le US National Institute of Standards and Technology (Institut national des normes et de la sécurité des Etats-Unis, NIST) a élaboré une liste de bonnes pratiques utiles construites autour de cinq impératifs: identifier, protéger, détecter, répondre et récupérer. En moyenne, les experts mettent en place deux fois plus d'initiatives dans l'ensemble de ces cinq catégories que les novices.



Ne pas lésiner
Les cyber-experts consacrent une grande partie de leurs budgets informatiques à la cybersécurité et de plus en plus d'entreprises de cette catégorie prévoient d'augmenter les dépenses dans chaque domaine lié à la cybersécurité dans l'année à venir. En des termes simples, plus une société emploie de personnes en charge de la cybersécurité, plus elle a de chances de se classer comme experte.

Investir dans la formation
Les novices ont subi beaucoup plus de failles issues d'attaques par phishing et par malware réussies. Des formations régulières pour sensibiliser le personnel sont cruciales. Ce n'est que partiellement une question de ressources. Près de trois quarts des micro-entreprises qui sont classées comme expertes ont l'intention de prioriser la mise en place de formations aux salariés de la société dans l'année à venir.

Impliquer la Direction
Neuf entreprises expertes sur dix déclarent que la «cybersécurité est une priorité majeure aux yeux des dirigeants/du Conseil d'Administration». Seule la moitié des novices est en mesure de déclarer la même chose. Lorsqu'il s'agit d'établir les priorités pour l'année à venir, seules 26% des micro-entreprises classées comme novices reconnaissent la nécessité d'insister sur l'engagement de la Direction ou du Conseil d'Administration dans les politiques et procédures en matière de cybersécurité.

Développer la résilience
Aucune entreprise ne sera jamais totalement sécurisée. Mais toutes les entreprises peuvent développer leur résilience en se préparant aux failles, en réalisant des tests et en disposant des capacités nécessaires pour répondre rapidement et efficacement aux failles. Une politique de cyber-assurance dédiée aide à développer cette résilience en donnant aux entreprises non seulement la certitude de bénéficier de garanties, mais également la capacité de s'appuyer sur une expertise en matière d'évaluation des risques, de gestion de crise et de formation des salariés.

Comment certaines petites entreprises ont réussi

Comme le montrent les chiffres du tableau ci-dessous, il y a également eu une augmentation sensible du nombre de petites et de micro-entreprises qui se sont classées expertes. Qui sont-elles et en quoi ont-elles réussi? Parmi ces entreprises, une sur six (16%) fait partie du secteur des TMT et dispose d'une bonne connaissance du monde du numérique, tandis que les entreprises de commerce de détail/gros et de construction sont également bien représentées (respectivement 11% et 10%). La plupart semblent avoir atteint le statut d'experts en prenant sérieusement en considération la cybersécurité. L'analyse montre que toutes ces entreprises ont pris les mesures suivantes:

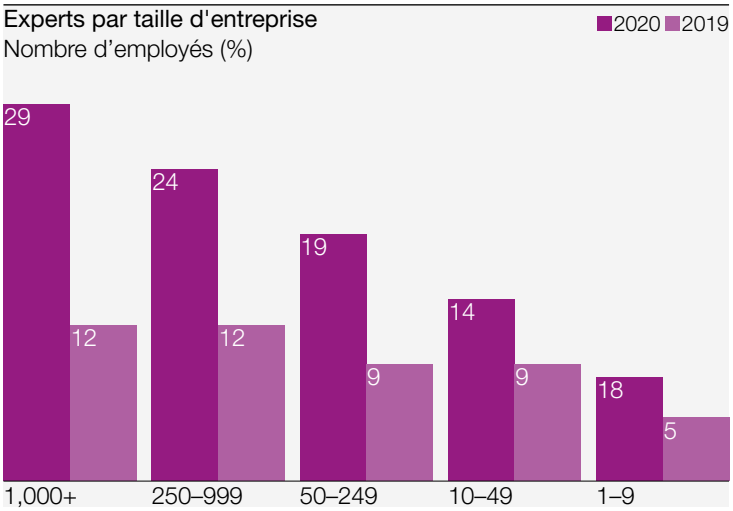
- nombreuses formations de sensibilisation à la cybersécurité;
- déploiement généralisé de systèmes anti-virus/anti-malware dans l'entreprise;
- prise de décisions sur la base d'une définition claire des besoins professionnels/des tolérances en matière de cybersécurité.

Secteurs les mieux préparés

Dans l'ensemble, les entreprises de services financiers et du secteur des technologies, médias et communications (TMT) ont encore été dans le top trois du classement (avec respectivement 24% et 23% de ces entreprises classées dans la catégorie «expert»), et elles ont été rejointes cette année par les entreprises du secteur de la fabrication (24%). Les entreprises de services professionnels, dont les pertes ont pratiquement été multipliées par dix, se sont classées très en dessous de la moyenne, seules 14% d'entre elles obtenant la mention «expert». L'explication peut résider dans le fait que le secteur est composé d'un nombre de micro-entreprises plus important que la plupart des autres secteurs. Le secteur de l'agro-alimentaire ferme la marche, seules 7% des entreprises de ce secteur se classant comme expertes.

Est-ce que les experts s'en sont mieux sortis?

En règle générale, les entreprises les mieux préparées s'en sont mieux sorties que les novices. Ces dernières ont été trois fois plus nombreuses que les entreprises expertes à subir une faille, avec un nombre médian de 30 failles par entreprise contre 9 pour les experts.



Experts par taille d'entreprise

La prépondérance des grandes et très grandes entreprises (plus de 1,000 salariés) parmi les experts peut expliquer leur ratio de failles plus élevé car les grandes entreprises offrent davantage de points d'entrée et des gains supérieurs aux cybercriminels, et sont vraisemblablement mieux armées pour découvrir les failles. Parmi toutes les entreprises, deux sur cinq se classent comme expertes, tandis que 60% des entreprises de moins de 100 salariés se classent novices.

L'une des conclusions les plus frappantes est que près d'une entreprise novice sur cinq (19%) à avoir subi un cyber-événement, a dû verser une rançon. Les petites entreprises, plus vulnérables, courent le risque de subir des attaques et les moins bien préparées payent clairement le prix fort.

L'avis d'Hiscox

Nous constatons deux grands types d'attaques par ransomware: Ciblées – frappant davantage les grandes entreprises (connues sous le nom de « big game ransomware ») et prenant la forme d'escroqueries de hameçonnage très personnalisées envoyées à certaines personnes clés ciblées par un groupe de pirates. Balayage de masse – Les pirates recherchent les faiblesses principales des serveurs exposés sur Internet (récemment des serveurs d'accès à distance et des VPN). Dans ces cas-là, les attaques ne font généralement pas de distinction et les pirates infectent toutes les sociétés qui se trouvent être vulnérables.

Développer la résilience

Cette année, un nombre important d'indicateurs suggère que la plupart des entreprises prennent la menace cyber plus au sérieux qu'avant.

Augmentation des dépenses

Tout d'abord, on assiste à une augmentation des dépenses de cybersécurité. Le rapport montre une tendance spectaculaire et généralisée d'augmentation des dépenses de cybersécurité l'année dernière, avec une dépense moyenne des entreprises de notre panel s'élevant à 1,8 millions € contre prêt de 1,3 millions € l'année précédente. Cela constitue une augmentation de 39%. Ce chiffre reflète à la fois une hausse globale des budgets informatiques et un bond de 30% pour la seule partie consacrée à la cybersécurité (de 9,9% à 12,9%). Les très grandes entreprises ont montré l'exemple.

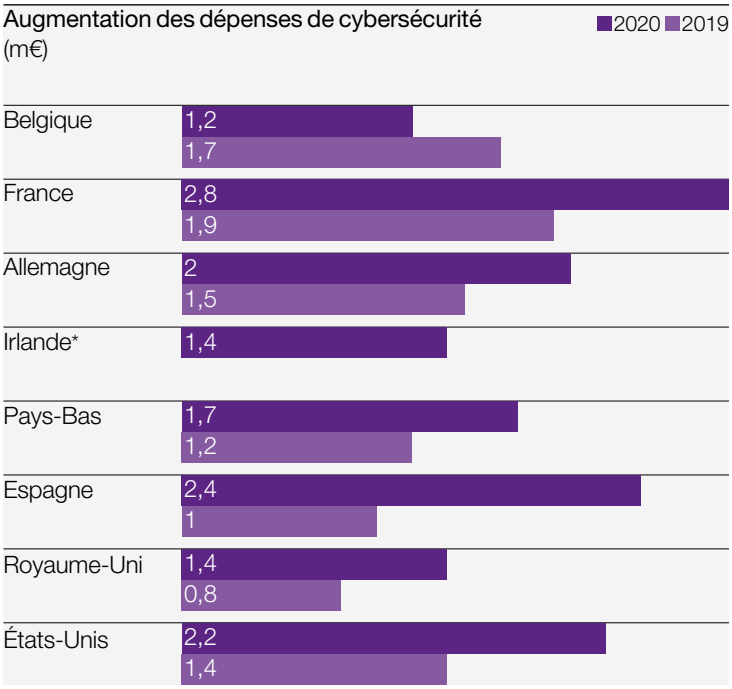
Les entreprises françaises ont encore une fois été les plus dépensières, portant leur budget moyen alloué à la cybersécurité de 1,9 millions € à 2,8 millions €. Les entreprises espagnoles et américaines les talonnent de près avec un budget moyen de 2,4 et 2,2 millions €, respectivement. Les entreprises britanniques, en retard dans les études précédentes, ont commencé à rattraper le train en marche, avec une dépense moyenne dans la cybersécurité de 1,4 millions €, contre 818,000 € l'an dernier.

Un peu plus de trois quarts des répondants ont communiqué les chiffres de leurs dépenses de cybersécurité. Si l'on part du principe que ces entreprises sont représentatives de l'ensemble du panel, les dépenses totales de cybersécurité l'an dernier se sont élevées à la somme impressionnante de 10,4 milliards €. En comparaison, elles n'étaient que de 7,2 milliards € l'année précédente avec 3% d'entreprises en moins dans le panel. Presque trois-quarts des entreprises (72%) ont prevu d'augmenter leurs dépenses cyber dans la prochaine année de 5% ou plus. C'est plus que les deux-tiers (67%) observés l'an dernier.

Augmentation des dépenses de cybersécurité

Le fossé entre celles qui ont augmenté leur budget et celles qui ne l'ont pas fait est immense. Les micro-entreprises de moins de dix salariés ont dépensé en moyenne prêt de 11,800 € dans la cybersécurité. Les très grandes entreprises ont quant à elles dépensé en moyenne 7,3 millions €.

En moyenne, les cyber-experts prévoient d'augmenter leur budget d'un peu plus de 15% tandis que les novices augmentent le leur d'un peu moins de 12%. Cela indique que le fossé entre le wagon de tête et le wagon de queue va se creuser davantage.



Des dépenses élevées sont-elles synonymes de bonnes capacités de gestion des cyber-risques?

La réponse n'est pas évidente. D'un côté, les entreprises qui ont dépensé une part à deux chiffres de leur budget informatique dans la cybersécurité ont eu tendance à subir moins d'incidents ou de failles que celles dépensant moins de 5%. Toutefois, les plus dépensières, qui sont généralement les plus grandes entreprises, ont payé en moyenne un prix plus fort après avoir subi une faille. La taille est corrélée à davantage de clients, des coûts de notification plus élevées et des rançons plus onéreuses.

*Données valables uniquement pour 2020.

Identification des priorités de dépenses en 2020
(%)

	Experts	Novices
Terminent ou continuent à se conformer à la réglementation	82	44
Signalent des menaces ou failles existantes	81	44
Se conforment aux exigences de sécurité chez eux ou chez leurs partenaires commerciaux	80	42
S'assurent que leurs partenaires commerciaux ou intermédiaires soient conforment avec les exigences de sécurité requises	79	40
Améliorent la sécurité des services ou applications en contact avec les clients	78	40

Il est également opportun de se demander si les entreprises dépensent correctement leur argent. On assiste à un changement clair d'affectation des dépenses sur les trois dernières années. Le nombre d'entreprises prévoyant de consacrer davantage de fonds à l'acquisition de nouvelles technologies de cybersécurité a progressivement chuté pendant cette période, passant de 57% à 46%, tandis que celles prévoyant d'investir davantage sur les formations de sensibilisation des salariés sont passées de 34% à 40%. Plus d'un tiers d'entre elles (35%) prévoient d'accroître la planification en matière de cybersécurité, contre 26% il y a deux ans.

Identification des priorités de dépenses en 2020

Une prise de conscience accrue

Comme l'année dernière, nous avons demandé aux répondants quelles étaient leurs dépenses prioritaires pour l'année à venir, en utilisant le cadre de cybersécurité du National Institute of Standards and Technology (NIST) cadre de la sécurité: identifier, protéger, détecter, répondre, et récupérer. Au cours des trois dernières années, les initiatives considérées comme les plus urgentes ont peu évolué. Mais les entreprises qui ont coché ces priorités sont de plus en plus nombreuses année après année, ce qui indique une prise de conscience croissante de la nécessité d'une approche large et active de la cybersécurité.

Les dépenses augmentent dans chaque catégorie

La propension à investir dans ces initiatives augmente en fonction de la taille des entreprises et de leur niveau d'expertise en matière de gestion des cyber-risques (voir le tableau ci-dessous). Les experts de notre panel ont clairement une liste de choses à faire plus importante. Pas moins de quatre cinquièmes d'entre elles ont, en effet, mentionné les priorités énoncées ci-avant pour l'année à venir. Elles sont également enclines à mettre davantage l'accent sur la «réalisation d'évaluations de la cybersécurité» et bien plus que les autres à insister sur «la sécurisation de l'Internet des choses au sein de l'entreprise – IoT.

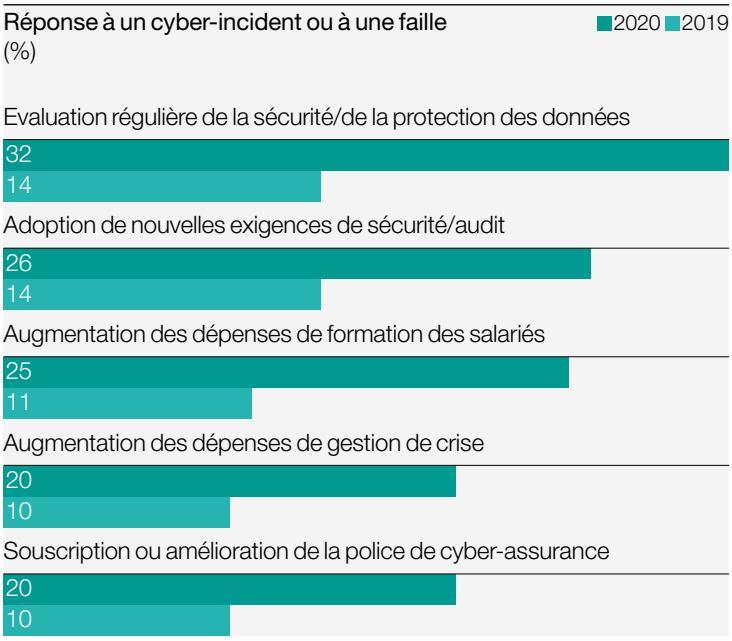
Un nouvel impératif

Il existe un autre indicateur marquant une nouvelle détermination dans la lutte contre la cyber-menace. Cette tendance s'observe dans la réponse apportée par les entreprises à un cyber-incident ou à une faille au cours des 12 derniers mois. Dorénavant, les entreprises agissent avec un nouvel impératif. De façon générale, les entreprises sont deux fois plus nombreuses que l'an dernier à avoir pris des mesures additionnelles pour lutter contre la piraterie informatique.

Les dépenses augmentent dans chaque catégorie du NIST
(%)

	2020	2019	2018
Identifier	50	46	44
Protéger	50	45	44
Détecter	50	47	45
Répondre	44	39	39
Récupérer	46	43	41

Réponse à un cyber-incident ou à une faille
(%)



Réponse à un cyber-incident ou à une faille

Les experts montrent la voie en matière de cyber-assurance
Le pourcentage d'entreprises ayant déclaré avoir souscrit une police de cyber-assurance après un cyber-incident ou une faille (pas nécessairement au cours de l'année passée) a progressé fortement tout au long des trois dernières études, s'élevant de 9% à 20%.

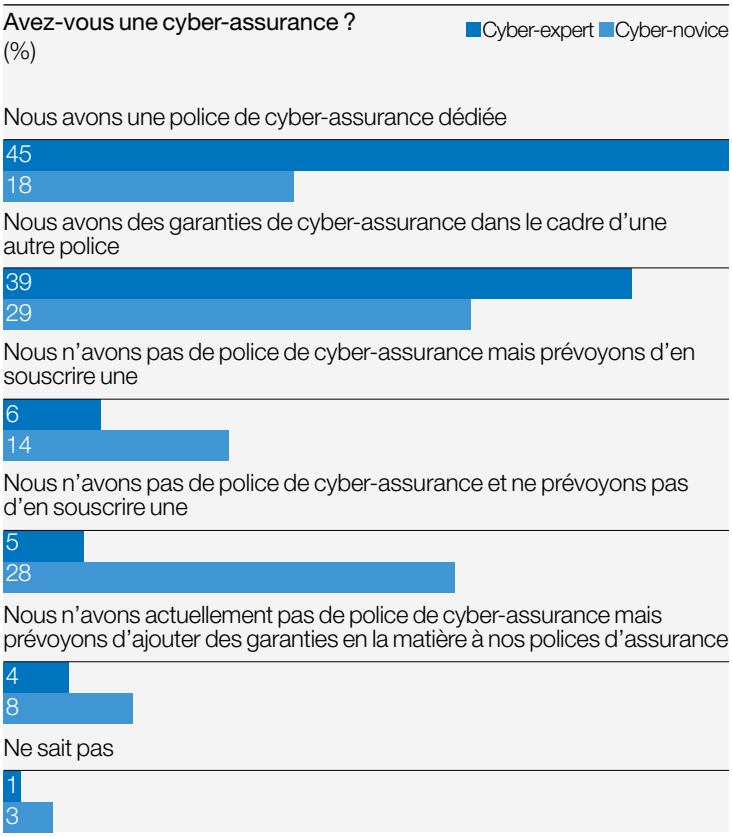
Cette année, nous avons modifié le questionnaire pour demander aux répondants s'ils disposent d'une police de cyber-assurance «dédiée» (au lieu de s'appuyer sur la garantie des cyber-risques dans le cadre d'une police plus générale). A peine plus d'un quart des entreprises (26%) ont déclaré avoir souscrit une police de cyber-assurance et 18% ont quant à elles déclaré qu'elles envisageaient de souscrire une police dédiée ou d'ajouter ces garanties à leurs polices.

Avez-vous une cyber-assurance?

Dans ce domaine, les experts sont très largement en avance sur les autres. Près de la moitié des entreprises ayant obtenu la mention «expert» (45%) déclare avoir souscrit une police de cyber-assurance dédiée et plus de trois quarts d'entre elles (70%) envisagent de souscrire des garanties contre les cyber-risques ou d'améliorer leurs garanties existantes.

La proportion d'entreprises ayant souscrit une police de cyber-assurance dédiée augmente de façon régulière en fonction de la taille des entreprises dans notre étude: à peine plus de 12% pour les micro-entreprises et jusqu'à 42% pour les très grandes entreprises. Dans chaque catégorie, à l'exception des plus grandes entreprises, de plus en plus d'entreprises s'appuient sur une autre police, plus générale (qui peut les couvrir ou non en cas de faille grave).

La tendance à souscrire une police de cyber-assurance dédiée varie fortement d'un pays à un autre. L'Irlande arrive en tête du classement, 38% des entreprises irlandaises déclarant avoir souscrit une police de cyber-assurance spécialisée. Elle est talonnée par les Etats-Unis (33%) et la Belgique (30%). Le Royaume-Uni (22%) et la France (23%) figurent en bas de la liste.



L'avis d'Hiscox
En qualité d'assureur de cyber-risques, nous ne pouvons qu'encourager la souscription d'une police de cyber-assurance dédiée. Il est important de signaler qu'une police de cyber-assurance dédiée a vocation à remettre les entreprises sur pied et en ordre de marche après une cyber-attaque. La cyber-assurance propose un certain nombre de services (réponse spécialisée en matière informatique, communication de crise, conseil juridique et, si nécessaire, suivi de carte bancaire), pour aider les entreprises à se remettre en ordre de marche rapidement. Les garanties d'autres polices proposent rarement tous ces services spécialisés et, dans certains cas, n'apportent aucune solution.

Méthodologie de recherche

Hiscox a sollicité Forrester Consulting pour évaluer les capacités de gestion des cyber-risques des entreprises. Au total, 5,569 professionnels en charge de 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, plus de 500 pour la Belgique, la France, l'Espagne et les Pays-Bas et plus de 300 pour la République d'Irlande). Les répondants ont rempli le questionnaire en ligne entre le 24 décembre 2019 et le 3 février 2020.

Le nombre de petites entreprises comptant moins de 250 salariés a été augmenté dans le panel, passant de 56% à 60%. Les entreprises de moins de neuf salariés représentent désormais 29% du panel, contre 20% l'an dernier. Les commerçants individuels représentent 10% du total, contre 5% l'an dernier. Les grandes (entre 250 et 999 salariés) et très grandes entreprises (1,000 salariés et plus) représentent toujours un total cumulé de 40% du panel.

Enfin, nous avons adopté cette année une approche fondée sur la valeur médiane, et non sur la moyenne, pour les incidents, failles et coûts, et avons recalculé les chiffres de l'année précédente en conséquence. Etant donné l'extrême variation des chiffres sous-jacents entre les entreprises les plus petites et les plus grandes, cette approche fournit une représentation plus juste du panel d'étude dans son ensemble.

Le profil complet des participants est illustré ci-dessous.

Niveau des répondants	%
Directeur exécutif/fondateur	31
Vice-président	21
Administrateur	39
Responsable	9

Taille de l'entreprise interrogée	%
1,000+	25
250–999	15
50–249	15
10–49	15
1–9	29

Secteurs	%
Services aux entreprises	7
Energie	4
Construction	8
Services financiers	9
Agro-alimentaire	4
Organismes sans but lucratif	7
Fabrication	8
Pharmacie et santé	9
Services professionnels	9
Immobilier	4
Commerce de gros et de détail	9
TMT	16
Transport et distribution	4
Voyages et loisirs	4

Services dans lesquels les répondants travaillent	%
Conseil d'administration/ haute direction	13
eCommerce	2
Finance	8
Direction juridique	3
Ressources humaines	4
Informatique/technologie	21
Marketing/communications	3
Opérations	10
Propriétaire	21
Achats	3
Gestion de produits	4
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

www.hiscox.fr/courtage/blog/lancement-du-rapport-cyber-hiscox-2020

20647 6/20