HISCOX
ASSURANCES

Rapport Hiscox 2022 sur la gestion des cyber-risques

Contents

Cover illustration
www.johnholcroft.com

Introduction

Gareth Wharton
Cyber CEO, Hiscox

L'une des conclusions les plus évocatrices de notre rapport cette année est que la cyber-menace est désormais perçue comme le risque dominant par les entreprises de sept des huit pays dans lesquels cette étude a été menée (devant la pandémie, le ralentissement économique, le manque de compétences et d'autres problématiques). Si la prise de conscience du danger est la première étape pour y faire face, c'est assurément un signe encourageant. En revanche, le nombre d'entreprises ayant signalé des attaques a progressé, tout comme la gravité des attaques elles-mêmes. On ne peut plus douter de l'ampleur du problème.

Si les cybercriminels ont longtemps ciblé les entreprises de premier plan, il est clair qu'ils s'attaquent désormais à des proies plus petites. Les agences internationales ont récemment signalé que davantage de petites et moyennes entreprises étaient visées, une tendance confirmée par ce rapport.

Les entreprises dont le chiffre d'affaires est compris entre 90 000€ à 450 000€ peuvent désormais s'attendre à autant de cyberattaques que celles qui gagnent entre 900 000€ et 8.1m d'euros par an. Pourtant, alors que les grandes entreprises investissent toujours plus dans le renforcement de leurs cyber-défenses, les dépenses des petites entreprises ont considérablement chuté cette année. Cette observation semble s'inscrire dans une tendance de réduction globale des dépenses informatiques dans les entreprises de petite dimension. Mais cela n'arrive pas au bon moment.

La pandémie pourrait bien avoir sa part de responsabilité. Le télétravail a poussé de nombreuses petites entreprises à adopter des solutions de cloud plutôt qu'à développer leurs propres services à distance. Cela a eu pour conséquence d'inciter les cybercriminels à exploiter les vulnérabilités des applications de cloud et à cibler également les prestataires de services de cloud.

Un signe encourageant: ce rapport montre clairement que les entreprises répondent aux attaques avec davantage de vigueur. Elles sont de plus en plus nombreuses à prendre des mesures décisives. En tant qu'assureur, nous observons cette tendance dans la qualité des plans de cyber-résilience qui nous sont présentés. Grâce à une prise de conscience accrue, les organes d'administration des entreprises ont une meilleure compréhension de la question du développement des capacités de gestion des cyber-risques et des normes en la matière.

Nous estimons que nous avons un rôle important à jouer pour appuyer ce processus. À cette fin, nous proposons des formations en ligne de sensibilisation à la cybersécurité aux salariés de nos clients via la CyberClear Academy d'Hiscox. Le nombre toujours élevé de failles créées par de simples emails de phishing, comme en témoigne ce rapport, marque la nécessité de poursuivre la sensibilisation des salariés aux risques.

De même, l'objectif de ce rapport n'est pas simplement de montrer l'ampleur et la nature de la problématique de la cyber-menace, mais d'aider les entreprises à y faire face en identifiant et en adoptant des bonnes pratiques. Pour cela, nous vous invitons à utiliser notre outil interactif de modélisation des capacités de gestion des cyber-risques et à évaluer la cyber-maturité de votre entreprise en vous comparant à d'autres entreprises. Cette modélisation est conçue pour vous aider à identifier vos forces et faiblesses et à élaborer un plan d'action. À l'instar de ce rapport, nous espérons que cet outil vous permettra de mettre en place des défenses plus fortes contre la cyber-menace et d'améliorer votre résilience pour répondre aux problèmes lorsqu'ils se présentent.

Des signes montrent que les entreprises répondent de façon plus probante à la cyber-menace.

La cyber-assurance chez Hiscox

Hiscox dispose d'une véritable expertise en matière de cyber-assurance
Nous avons plus de 20 ans d'expérience dans le domaine de l'assurance contre les atteintes aux données et contre les cyber-risques et, au cours de cette période, nous avons souscrit des centaines de milliers de polices et géré des milliers de sinistres dans le monde. La compréhension des cyber-risques et des défis auxquels les entreprises font face est la clé de notre succès. En 2017, Hiscox a mis en place une équipe internationale centralisée dédiée à la cybersécurité, pour garantir la cohérence de nos produits, une approche coordonnée et des services collaboratifs.

Les produits d'assurance de nouvelle génération comprennent un ensemble d'outils et de services
Au-delà du classique transfert de risque, la cyber-assurance d'Hiscox vous offre un soutien direct et l'assistance de véritables experts (gestionnaires de crise, spécialistes informatiques, avocats spécialisés dans la protection des données et consultants en communication externe). Depuis 2018, Hiscox propose des formations gratuites pour les salariés de l'ensemble des petites et moyennes entreprises que nous assurons dans le monde, à travers la CyberClear Academy d'Hiscox, qui compte près de 30 000 utilisateurs.

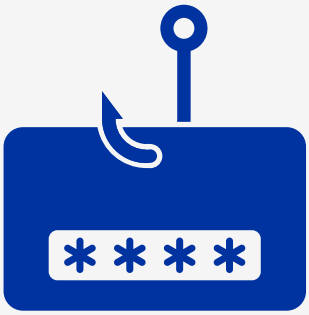
Partager notre expertise et sensibiliser
Nous avons développé des outils open-source, comme le Calculateur d'exposition aux cyber-risques d'Hiscox, qui aide les entreprises à comprendre l'impact financier d'une cyber-attaque. En 2021, nous avons développé un outil en ligne de modélisation de la cyber-maturité permettant aux entreprises de s'auto-évaluer pour comprendre leurs forces et faiblesses en matière de cybersécurité. Elles peuvent comparer leur performance gratuitement à celle de plus de 11 000 autres entreprises.

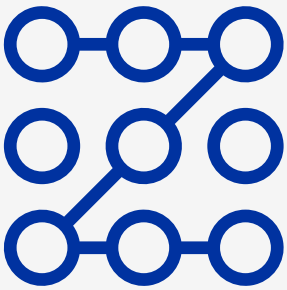
Vous tenir informé sur le paysage de la cybersécurité
Pour la sixième année consécutive, nous avons élaboré le Rapport international Hiscox sur la gestion des cyber-risques, qui propose un aperçu rapide des capacités de gestion des cyber-risques des entreprises, ainsi qu'un tableau des meilleures pratiques pour lutter contre une menace en perpétuelle évolution. Sur la base d'un échantillon représentatif d'entreprises de huit pays classées par taille et par secteur, ce rapport reflète l'expérience directe des acteurs se trouvant en première ligne dans la lutte contre la cybercriminalité.

Résumé

Intensification des attaques
48% des entreprises ont signalé une attaque au cours des 12 derniers mois, contre 43% l'an dernier.

Le risque est perçu comme élevé
Dans sept des huit pays observés dans notre étude, les entreprises ont identifié les cyberattaques comme la menace numéro un pour leur entreprise.





Pression financière
Parmi les entreprises ayant subi une attaque, une sur cinq a déclaré que sa solvabilité avait été menacée, soit une augmentation de 24% par rapport à l'an dernier.

Les risques du travail à distance
Covid a incité les entreprises à accélérer leur parcours dans le nuage, ce qui a entraîné une forte augmentation des attaques via des serveurs en nuage.

L'expertise s'avère payante
Le coût médian des cyber-attaques, exprimé en pourcentage du revenu, est deux fois et demie plus important pour les entreprises classées 'cyber-novices'.

Hausse des souscriptions de cyber-assurance
64% des entreprises ont désormais souscrit une cyber-assurance, soit par le biais d'un contrat dédié, soit par le biais de garanties dans le cadre d'un autre contrat. Elles étaient 58% dans ce cas il y a deux ans.

Augmentation des ransomwares
19% des participants ont rapporté une attaque par ransomware, contre 16% l'an dernier. Deux tiers d'entre elles ont versé une rançon.

Augmentation des dépenses
Sur l'ensemble des participants, les dépenses moyennes ont progressé de 60% l'an passé pour s'établir à 4.8m€, soit une hausse de 250% par rapport à 2019.

Aggravation des conséquences
Le coût médian des attaques a augmenté de 29% pour atteindre près de 15 300€.

Comparaison par pays

Principales conclusions	
Belgique Une entreprise belge sur sept (14%) a licencié des salariés en raison d'une cyber-attaque.	**France** Deux entreprises attaquées sur cinq (41%) ont subi un détournement de paiement, la proportion la plus importante parmi les pays du panel de l'étude.
Allemagne Si les entreprises allemandes sont les moins nombreuses à avoir versé une rançon, ce sont également celles qui ont payé les sommes les plus importantes.	**Irlande** Les entreprises irlandaises ont versé des rançons plus régulièrement que les autres, 25% d'entre elles ont payé cinq fois ou plus pour récupérer des données, mais les montants des rançons étaient parmi les plus faibles.
Pays-Bas Les entreprises néerlandaises ont été cette année les entreprises les plus ciblées de notre panel. La proportion d'entreprises attaquées au cours des 12 derniers mois a bondi de 41% à 57%.	**Espagne** L'Espagne est le seul pays dans lequel le nombre d'entreprises attaquées a décru l'an passé (de 53% à 51%).
Royaume-Uni Pour la troisième année consécutive, les entreprises britanniques ont été proportionnellement moins nombreuses à subir une attaque (42%), mais le coût médian des attaques, a doublé pour atteindre 25 200€.	**États-Unis** Les entreprises américaines ayant signalé une cyber-attaque sont bien plus nombreuses que l'an dernier (+7%) et la proportion d'entreprises ayant subi des coûts de 22 500€ ou plus a également augmenté, passant de 34% à 40%.

Comparaison par pays
suite

Au moins une cyber-attaque subie (%)

	2021	2022	+/-
Belgique	42	**43**	+1
France	49	**52**	+3
Allemagne	46	**46**	–
Irlande	39	**49**	+10
Pays-Bas	41	**57**	+16
Espagne	53	**51**	-2
Royaume-Uni	36	**42**	+6
États-Unis	40	**47**	+7

Coût financier médian d'une cyber-attaque (000€)

	2021	2022	+/-
Belgique	11	**9**	+2
France	16	**15**	-1
Allemagne	22	**19**	-3
Irlande	7	**15**	+9
Pays-Bas	11	**16**	+6
Espagne	11	**11**	–
Royaume-Uni	13	**25**	+14
États-Unis	9	**17**	+9

Au moins une attaque par ransomware subie (%)

	2021	2022	+/-
Belgique	19	**15**	-4
France	14	**19**	+5
Allemagne	19	**21**	+2
Irlande	16	**19**	+3
Pays-Bas	13	**26**	+13
Espagne	14	**22**	+8
Royaume-Uni	13	**16**	+3
États-Unis	17	**17**	–

Les victimes de ransomware qui ont payé (%)

	2021	2022	+/-
Belgique	49	**74**	+25
France	65	**62**	-3
Allemagne	54	**48**	-6
Irlande	75	**80**	+5
Pays-Bas	48	**79**	+31
Espagne	44	**64**	+20
Royaume-Uni	58	**63**	+5
États-Unis	71	**84**	+13

Souscription d'une cyber-assurance (%)

	2021	2022	+/-
Belgique	58	**59**	+1
France	57	**61**	+4
Allemagne	64	**67**	+3
Irlande	64	**69**	+5
Pays-Bas	55	**58**	+3
Espagne	63	**66**	+3
Royaume-Uni	61	**62**	+1
États-Unis	65	**65**	–

Part du budget informatique alloué à la cybersécurité (%)

	2021	2022	+/-
Belgique	21	**24**	+3
France	20	**22**	+2
Allemagne	21	**24**	+3
Irlande	21	**22**	+1
Pays-Bas	22	**24**	+2
Espagne	22	**24**	+2
Royaume-Uni	20	**22**	+2
États-Unis	23	**24**	+1

Perception vs. réalité

Un chat échaudé craint l'eau froide: Il semble en effet que les personnes ayant eu affaire à des cyber-pirates soient bien plus mobilisées sur ce sujet. Les entreprises qui ont subi une attaque l'année dernière sont beaucoup plus enclines à catégoriser la menace d'une cyber-attaque comme un 'risque élevé' que les autres.

La cyber-menace est désormais largement considérée comme le risque n°1 pour l'entreprise. Lorsqu'on compare les réponses des entreprises par pays, seules les entreprises irlandaises ont classé la cyber-menace en deuxième position des risques, derrière la pandémie. Il existe néanmoins une différence de perception majeure entre les entreprises qui ont effectivement subi une attaque et les autres. Plus de la moitié des victimes d'une cyber-attaque (55%) considèrent la cybersécurité comme un domaine à haut risque. Ce chiffre n'est que de 36% parmi les entreprises qui n'en ont pas subi. Conserver les données en toute sécurité, indépendamment du cyber-risque, semble être important pour toutes les entreprises, 72% d'entre elles reconnaissent qu'elles écorneront leur image de marque si elles ne traitent pas les données des clients et des partenaires de façon sécurisée.

Cette grande différence de perception se reflète d'ailleurs dans le nombre d'entreprises déclarant que les risques se sont accrus l'année dernière. Plus de deux entreprises attaquées sur cinq (41%) indiquent que leur exposition au risque a augmenté. Parmi celles qui n'ont pas été attaquées, ce chiffre se rapproche d'une sur cinq (23%).

Il y a quelques exceptions. Les entreprises de services financiers sont plus enclines à considérer la cyber-menace comme un risque élevé (55%) même si elles sont les moins nombreuses à avoir subi une attaque l'an dernier. Toutefois, elles figuraient dans le haut du tableau des entreprises attaquées l'année précédente. Par contraste, les entreprises participantes du secteur de l'agro-alimentaire, le plus attaqué cette année, ont mentionné la pandémie, le manque de compétences et la concurrence accrue comme les défis présentant les plus gros risques.

Un autre indicateur de la perception du risque est constitué par les sommes que les entreprises des différents secteurs consacrent à la cybersécurité. Les sociétés spécialisées dans les services aux entreprises sont de loin les plus dépensières en la matière, avec une moyenne de 31 millions€. Ce montant est plus de six fois supérieur à la moyenne. Le secteur des voyages et loisirs consacre les sommes les plus faibles à la cybersécurité.

Les entreprises expertes et celles disposant d'une cyber-assurance comprennent les risques

La majorité des entreprises classées 'cyber-expertes' affichent également une plus grande conscience du danger, de même que près de la moitié de celles qui ont souscrit une cyber-assurance (49%) (pour une compréhension complète de la façon dont notre modèle fonctionne pour évaluer les personnes, les processus et la technologie nécessaires à une cybersécurité efficace, rendez-vous sur www.hiscoxgroup.com/cyber-maturity). Les expertes sont près de deux fois plus nombreuses que les novices à considérer que leur exposition à une cyber-attaque est élevée ou très élevée: 58% contre 32%. Et ce, indépendamment du fait qu'elles ont mis en place des défenses plus solides.

Il est intéressant de relever que près de quatre cinquièmes des entreprises qui n'ont pas souscrit de garanties contre les cyber-risques, et qui n'ont pas l'intention de le faire, n'ont pas subi d'attaque l'an dernier. Plus de la moitié d'entre elles sont des novices (51%). Leur perception n'a pas encore évolué à l'instar de celle des victimes de cyber-attaques.

Les grandes entreprises et celles qui ont été attaquées affichent une plus grande confiance dans leur capacité effective de gestion des attaques. Les petites entreprises ont du retard à rattraper en la matière.

De façon générale, plus de trois cinquièmes des participants (62%) conviennent que leur entreprise est plus vulnérable aux attaques avec le développement du télétravail. Ce chiffre s'élève à 69% dans les entreprises de plus de 250 salariés. Chez les expertes, il est de 76% mais seulement de 49% en moyenne chez les novices.

Et quelle est la réalité?

Il existe une certaine corrélation entre la perception de l'exposition aux risques et

Comment la perception de la cyber-menace s'articule-t-elle avec le risque d'être attaqué ?

Perception vs. réalité
suite

l'incidence de cyber-attaques. Comme mentionné plus haut, les entreprises classées 'expertes' sont plus enclines à qualifier la cyber-menace de risque élevé. Elles ont tout à fait raison. Elles sont plus souvent confrontées aux cyber-pirates que les autres, probablement parce qu'elles constituent des cibles plus tentantes en raison de leur taille relative.

Il semblerait que le recours au télétravail ait modifié les axes d'attaque. Les serveurs d'entreprise constituent le principal point d'entrée des pirates, mais le nombre d'intrusions signalées via des serveurs de cloud a considérablement progressé. Cela va dans le sens de l'avertissement lancé par les agences internationales selon lequel les malfaiteurs ciblent de plus en plus des infrastructures de cloud.

Bien que les différents types d'attaques soient perçus de manière assez uniforme, la réalité illustre les points sur lesquels les entreprises doivent se concentrer. Les deux principaux types d'attaques, utilisation abusive des ressources informatiques (32%) et détournement de paiement (31%), semblent présenter un risque plus important que les ransomwares (19%). Il semble donc que les entreprises n'accordent peut-être pas suffisamment d'attention à la prévention contre les deux premiers.

Les cyber-pirates élargissent leur champ d'attaque

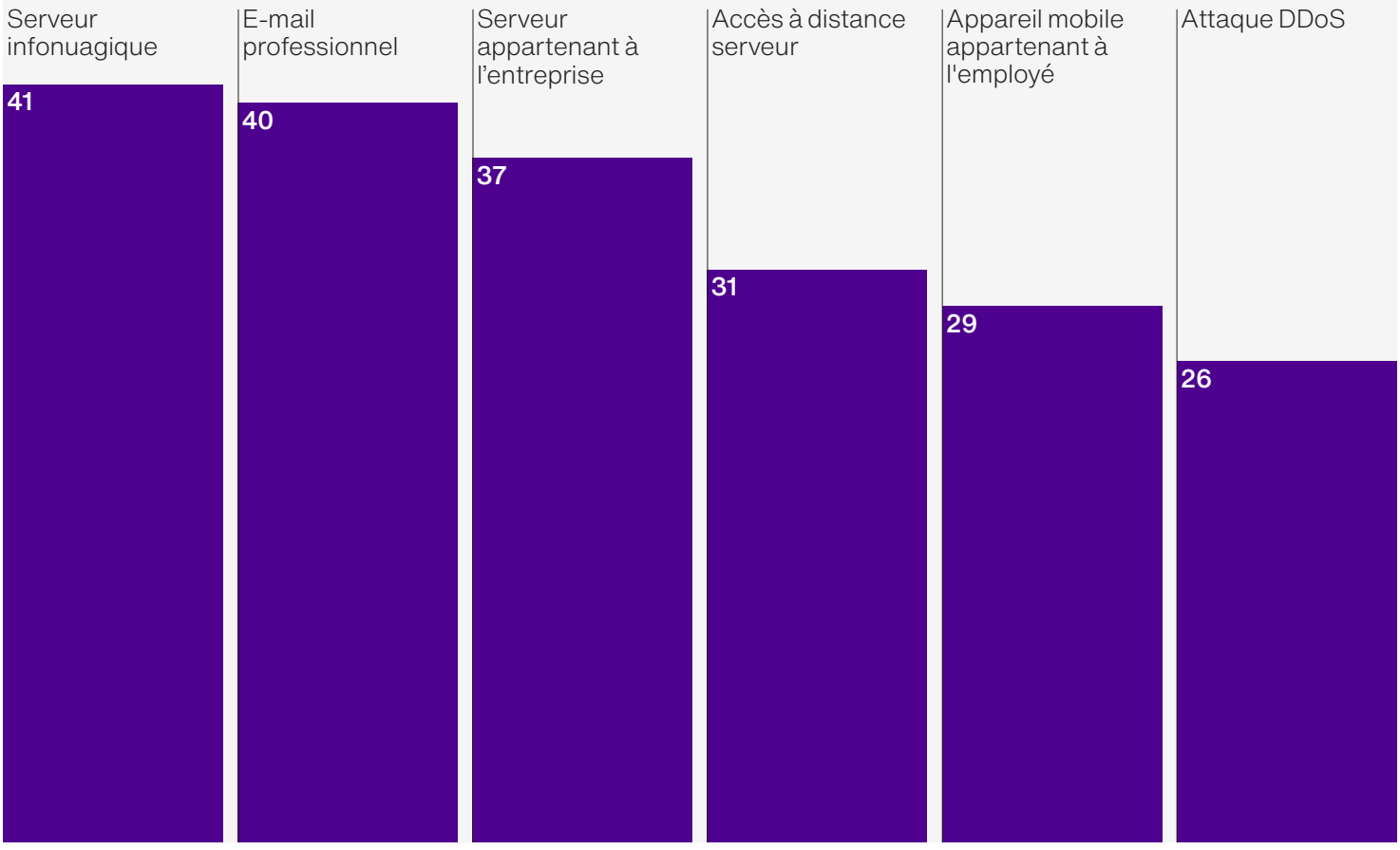
Le nombre moyen de cyber-attaques par entreprise n'a progressé que modérément cette année, passant de 179 à 190. Dans les très grandes entreprises, il a même légèrement diminué, même si les plus grandes d'entre elles (avec des revenus de plus de 4.5 milliards€) font état de plus de 1 100 attaques en moyenne. Pour la plupart des autres catégories d'entreprise, le nombre d'attaques a en réalité augmenté, car les pirates ont davantage ciblé les petites et moyennes entreprises.

Ainsi, les entreprises employant entre 250 et 999 salariés ont subi davantage d'attaques en moyenne (69 contre 45 l'an dernier). Celles employant entre 10 et 49 salariés ont subi en moyenne 56 attaques, contre 31 l'an passé, et les plus petites entreprises (moins de dix salariés) ont vu l'incidence d'attaques quasiment quadrupler (de 11 à 40).

Les entreprises dont le chiffre d'affaires est compris entre 90 000€ et 450 000€ peuvent désormais s'attendre à autant de cyberattaques que celles qui gagnent entre 900 000€ et 8.1m€ par an. Ces chiffres concordent avec les avertissements des agences internationales selon lesquels les pirates agissant au moyen de ransomwares délaissent les cibles les plus importantes pour se tourner vers des entreprises de taille moyenne.

Les pirates ont également eu tendance à cibler d'autres secteurs. Les secteurs les plus largement ciblés ont été les voyages et loisirs (61% des participants de ces secteurs ont signalé au moins une attaque), les services professionnels

Méthode d'entrée la plus courante (%)
Les serveurs en nuage sont désormais la première porte d'entrée des cyberattaques.



Perception vs. réalité
suite

(58%) et le commerce de gros et de détail (56%). Les secteurs les plus ciblés l'année précédente, l'énergie et le les transports/distribution, ont enregistré une chute importante du nombre d'attaques.

Les coûts continuent de grimper
Le coût médian par participant pour l'ensemble des attaques subies a progressé de 30% l'année dernière, pour s'établir à presque 15 300€. Mais ce chiffre masque une grande disparité dans les résultats, entre un minimum de 8 910€ en Belgique et un maximum de 25 290€ au Royaume-Uni, où les coûts ont plus que doublé. Les coûts ont également doublé en Irlande pour atteindre 15 120€.

Une entreprise britannique a enregistré un coût total de 6m€ pour l'ensemble des attaques qu'elle a subies. Dans les entreprises les plus touchées en Allemagne, en Irlande et aux Pays-Bas, les coûts ont dépassé les 4.5m€. Par contraste, les coûts médians ont été stables voire plus faibles en Belgique, France, Allemagne et Espagne.

Ces chiffres ne donnent qu'une idée de l'impact d'une cyber-attaque. Parmi les entreprises participantes, celles qui ont licencié des salariés à la suite d'une attaque a doublé (de 5% à 11%). Un cinquième des entreprises a versé une amende importante à une agence gouvernementale, soit près de deux fois plus que l'année précédente, et autant d'entreprises (21%) ont déclaré que l'impact était suffisamment important au point de menacer leur solvabilité.

Les entreprises du secteur de l'immobilier ont déclaré le plus grand nombre d'attaques (319), juste devant le secteur des services aux entreprises (304). Les pertes médianes les plus fortes ont été enregistrées dans le secteur du commerce de gros et de détail (27 000€), devant le secteur de l'énergie (21 150€) et le secteur de la pharmacie et de la santé 19 170€.

Augmentation des ransomwares
Davantage d'entreprises ont subi des attaques par ransomware (19% contre 16% l'année précédente). Deux tiers d'entre elles (66%) ont versé une rançon et plus de la moitié (53%) en ont versé plusieurs. C'est aux États-Unis et en Irlande que les entreprises ont versé le plus de rançons et en Allemagne qu'elles en ont versé le moins. La rançon la plus lourde s'est élevée à près de 90 000€, à peine plus que l'an dernier (85 500€). À noter une étrangeté: le secteur de l'agro-alimentaire a été le moins ciblé par les ransomwares (seules 14% des entreprises ont signalé une attaque) mais est celui dans lequel les rançons versées ont été les plus nombreuses (62% des entreprises touchées ont payé).

Quelques bonnes nouvelles: le montant médian de l'ensemble des rançons a diminué de 20% et les coûts de récupération ont presque été divisé par deux. Les entreprises ont été plus nombreuses à récupérer ou à reconstruire leurs données à partir de sauvegardes à plusieurs occasions. Les très grandes entreprises (1 000 salariés et plus) sont parvenues plus souvent à récupérer effectivement leurs données (68% contre 59% en moyenne) et ont subi bien moins de fuites de données (20% contre 29% en moyenne). Les entreprises de services professionnels, qui sont de loin les plus dépensières en matière de cybersécurité avec une moyenne de 30.1 millions€, ont plus rarement versé une rançon (seules 18% d'entre elles l'ont fait).

Nouvelle flambée des dépenses de cybersécurité
Sur l'ensemble des participants, les dépenses moyennes ont progressé de 60% l'an passé pour s'établir à 4.8 millions€, soit une hausse de 250% par rapport à 2019. Les entreprises allemandes, les plus dépensières l'année précédente, ont été dépassées par leurs homologues irlandaises qui ont dépensé en moyenne 12.5 millions€ par entreprise (contre 1.9 millions€ l'an dernier).

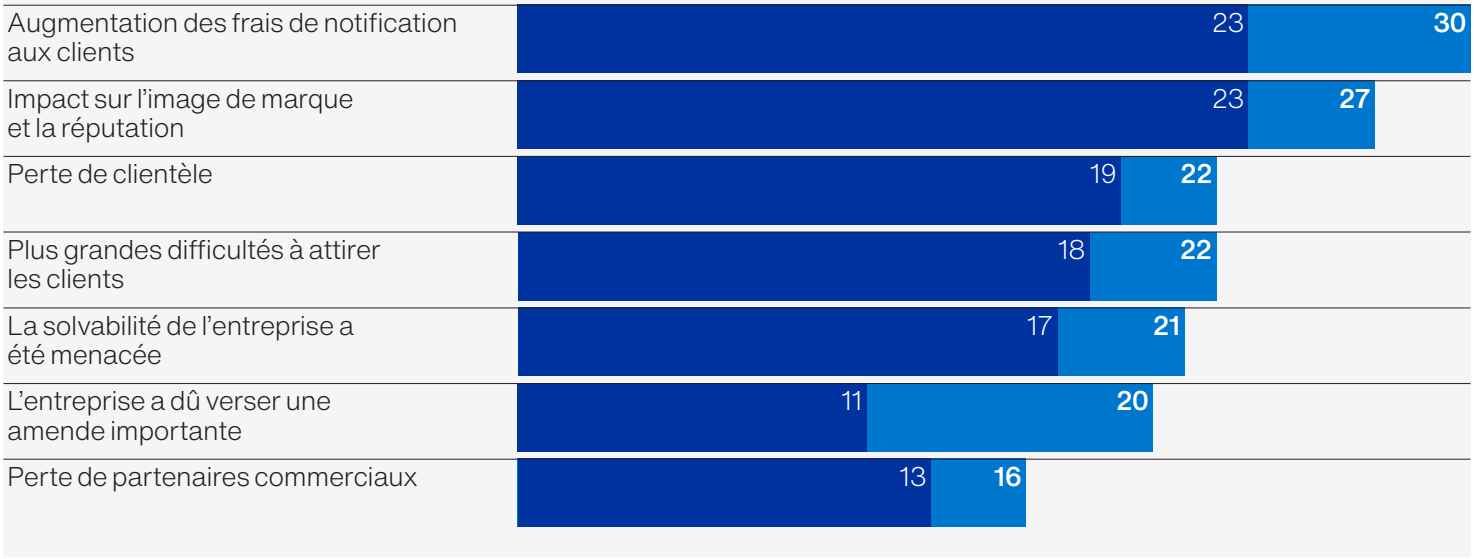
On observe néanmoins un écart important entre les grandes et les petites entreprises. Les dépenses moyennes dans les entreprises qui emploient entre 250 et 999 salariés ont doublé l'année dernière. Dans les très grandes entreprises de 1 000 salariés et plus, elles ont augmenté de 65%. Leurs dépenses moyennes ont été quasiment multipliées par cinq en trois ans, pour atteindre près de 18 millions€.

À l'autre extrémité, le scénario est différent. Les entreprises qui emploient entre 10 et 49 salariés ont presque divisé par deux leur budget cybersécurité, de 369 900€ à 225 900€. Dans les entreprises de moins de 10 salariés, les dépenses se sont effondrées, passant d'une moyenne de 135 000€ à seulement 26 100€.

Ce constat est probablement lié à la pandémie, car les entreprises ont moins d'argent pour leurs dépenses informatiques. Le pourcentage du budget informatique lloué à la cybersécurité a légèrement augmenté dans cette catégorie d'entreprises (20% contre 17% l'an dernier). Même si leurs finances sont réduites, elles ne négligent pas complètement l'importance de la cybersécurité.

Perception vs. réalité
suite

Impacts d'une cyberattaque (%)
Les effets d'une cyberattaque vont bien au-delà des conséquences financières directes. Les entreprises découvrent qu'il y a un impact accru à tous les niveaux.



Que font les experts?

Il est tentant de répondre à la question en disant qu'elles règlent le problème par l'argent. Mais cette affirmation n'est que partiellement vraie et ne répond pas à l'ensemble de la question. Les entreprises peuvent prendre de nombreuses mesures sans se ruiner.

Il est certain que les grandes entreprises de notre panel sont les plus représentées parmi les entreprises ayant obtenu la mention 'cyber-expert' dans notre modélisation de la cyber-maturité. De par leur taille, elles disposent de ressources bien plus importantes, notamment pour lutter contre la cybercriminalité.

Cependant, la taille génère de nouveaux défis. L'entreprise experte moyenne doit gérer 41 serveurs différents, dont plus de vingt sont généralement dans le cloud. Comme on l'observe par ailleurs dans ce rapport, cela peut constituer un domaine de vulnérabilité. De même, les grandes entreprises sont les principales cibles et sont attaquées plus souvent que les petites. Cela suscite des réactions particulières de leur part. Les entreprises ayant subi 30 attaques ou plus l'an passé, disposaient en moyenne d'un budget cybersécurité supérieur à 9m€.

Mais l'écart de dépenses entre les expertes et le reste des entreprises s'est considérablement réduit cette année. Les entreprises qualifiées de novices ont plus que triplé leurs dépenses de cybersécurité en moyenne (2.9m€), tandis que celles qualifiées d'intermédiaires ont augmenté les leurs de 63% en moyenne. Avec 5.6m€, elles dépassent désormais la somme allouée en moyenne par les expertes de plus 900,000€.

L'argent ne fait pas tout

Heureusement, tout n'est pas uniquement une question d'argent. Les expertes formalisent leur réponse en matière de cybersécurité. Elles ne l'élaborent pas au gré des attaques. Elles désignent une ou plusieurs personnes en charge de la cybersécurité avec des rôles bien définis, et ont l'appui du conseil d'administration/de la direction. La grande majorité (87%) font valoir que les hauts dirigeants ont une idée claire de la gestion de la cybersécurité (contre 69% dans l'ensemble du panel).

Elles appliquent généralement le cadre défini par le National Institute of Standards and Technology (Institut national des normes et de la sécurité, NIST) du gouvernement américain, en répartissant leurs investissements et leur temps sur les cinq fonctions suivantes: identifier, protéger, détecter, répondre et récupérer.

Les deux mesures qui ont le plus progressé sont l'élaboration d'un plan de réponse aux incidents et la simulation régulière d'une cyberattaque pour tester le plan de réponse aux incidents de l'entreprise. Ces activités sont particulièrement sensibles en ces temps incertains de conflit en Europe et de sanctions occidentales. En matière de cybersécurité, les expertes ont une liste de priorités comprenant l'évaluation régulière des infrastructures de données et de technologie de l'entreprise, la dispense de formations effectives à la cybersécurité à leurs salariés et le respect des exigences de sécurité de l'entreprise par les partenaires commerciaux. Il existe par ailleurs de nombreuses autres mesures recommandées qui sont relativement peu onéreuses à mettre en place. Ce sont les solutions simples que les entreprises doivent adopter. Environ deux tiers des expertes les ont toutes mises en œuvre.

Et la taille ne fait pas tout. Au sein de ce groupe, on dénombre à peu près autant de petites entreprises, à savoir celles de moins de 50 salariés, que de grandes entreprises de 1 000 salariés et plus. Les petites entreprises n'envisagent pas de couvrir autant de domaines que les grandes, mais elles ne sont pas loin derrière. À titre d'exemple: 44% des petites entreprises expertes déclarent qu'elles prévoient de simuler régulièrement une cyber-attaque pour tester leur plan de réponse aux incidents, contre 58% des grandes entreprises. Par comparaison, seules 37% des novices sont dans ce cas.

Les efforts pour lutter contre la cyber-menace renforcent la confiance. Une entreprise experte sur six indique que son exposition aux cyber-attaques a effectivement diminué l'année dernière. Pourquoi? Les deux principales raisons sont une meilleure mise en œuvre des processus ou procédures de cybersécurité, comme le déploiement de correctifs ou la réalisation de tests d'intrusion (mentionnés par 62% des entreprises de ce groupe), et la désignation de personnes en charge de la sécurité ou la mise en place d'une équipe renforcée (mentionnée par 46%).

Toutes les entreprises doivent adopter l'approche méthodique et structurée mise en œuvre par les expertes. Les réactions au coup par coup ne sont pas suffisantes.

Que font les experts?
suite

Grosse chute du nombre d'entreprises expertes
Dans l'ensemble, les notes d'évaluation des capacités de gestion des cyber-risques ont décru de 2,6%, avec une détérioration marquée de la gouvernance/assurance (fonction processus) et de la présence de salariés convenablement qualifiés et expérimentés (personnes). Des améliorations ont été constatées en matière d'outils et technologies (technologie).

Ce déclin global a entraîné une chute très importante du nombre d'entreprises classées expertes dans notre modélisation des capacités de gestion des cyber-risques (de 20% l'an dernier à seulement 4,5% cette année). Les États-Unis et le Royaume-Uni sont toujours en tête avec 6% d'entreprises classées expertes. La proportion d'entreprises classées novices a également fortement baissé, ce qui fait qu'il y a désormais un grand nombre d'intermédiaires.

Notre outil de modélisation de la cyber-maturité repose sur une auto-évaluation par les entreprises de leurs capacités de gestion des cyber-risques. Deux facteurs semblent avoir contribué à une perte de confiance. Le principal fait suite à la découverte très médiatisée en décembre 2021 de la vulnérabilité aux attaques de la librairie de logging Log4j, très utilisée dans les applications et services sur Internet. À la suite de cette annonce, le nombre de participants évaluant leur dispositif de cybersécurité comme 'optimisé' a chuté de 18% à 2,9% et le nombre d'entreprises indiquant qu'elles étaient très confiantes dans leurs capacités en matière de cybersécurité est passé de 73% à 67%.

Un autre facteur peut être constitué par la difficulté croissante à embaucher des personnes convenablement qualifiées, comme en témoignent les faibles scores obtenus dans la catégorie 'personnes' de notre modélisation des capacités de gestion des cyber-risques.

Que font les experts?
suite

Respecter les fondamentaux
Compte tenu de la publicité accordée à certaines cyber-attaques récentes, il est surprenant que près de la moitié des personnes interrogées (49%) considèrent que leurs outils de sauvegarde des données sont 'optimisés' ou 'mesurés'. Parmi les novices, ce chiffre est bien plus bas (tout juste 21%) et seules 17% d'entre elles sont correctement équipées pour rétablir leur système informatique et récupérer leurs données en cas de panne du système.

Si quatre entreprises expertes sur cinq ont une approche mesurée ou optimisée en ce qui concerne les contrôles de pré-sélection à l'embauche, l'interdiction de l'utilisation de nouveaux comptes génériques ou du partage d'identifiants entre utilisateurs, cette proportion n'est que d'une sur cinq pour les novices, voire moins. Respecter les fondamentaux est crucial, et d'un coût relativement faible, notamment lorsqu'on le rapporte au coût de gestion d'une attaque par ransomware.

Renforcer ses défenses après une attaque
Interrogées sur la question de savoir comment elles avaient répondu aux cyber-attaques, environ deux entreprises expertes sur cinq indiquent qu'elles ont mis en place des exigences supplémentaires en matière de cybersécurité et d'audit (51%), accéléré la formation des salariés (39%) et amélioré leurs capacités en cas de cyber-attaque (39%). Ces chiffres sont généralement plus élevés dans les grandes entreprises.

Les petites entreprises expertes ont par exemple déployé plus largement la première de ces mesures: plus de la moitié d'entre elles déclarent qu'elles ont mis en œuvre des exigences supplémentaires en matière de cybersécurité à la suite d'une attaque. Par ailleurs, elles sont plus nombreuses à avoir sollicité les services d'un professionnel du domaine de la réponse aux incidents, bien que cela puisse s'expliquer par le fait que leurs homologues de plus grande dimension ont déjà engagé des prestataires externes ou n'en ont pas besoin.

Souscription d'une cyber-assurance
Sur l'ensemble du panel de notre étude, plus d'un tiers (35%) des entreprises de 250 salariés et plus disposent d'une police de cyber-assurance dédiée, et 40% ont souscrit des garanties contre les cyber-risques dans le cadre d'un autre contrat. En dessous de ce seuil, ces chiffres sont respectivement de 28% et 29%.

La pertinence de souscrire une cyber-assurance est évidente pour les petites entreprises qui ne peuvent pas se doter de grandes équipes de cyber-spécialistes, et ce notamment parce qu'elles sont de plus en plus ciblées par les pirates, comme le montre notre rapport.

Dans l'ensemble du panel, la possibilité de bénéficier d'une assistance spécialisée, notamment en matière de gestion de crise ou d'expertise informatique, fait partie des trois principales raisons invoquées pour souscrire des garanties contre les cyber-risques (après les craintes concernant la sécurité des données et juste devant la nécessité de montrer aux clients que l'entreprise prend la cybersécurité au sérieux). Mais parmi les expertes, qui disposent généralement de compétences en interne, la raison numéro deux est la crainte que si l'entreprise est attaquée, les clients puissent porter réclamation contre elles. Au total, 46% des expertes disposent actuellement d'une police de cyber-assurance dédiée (contre 31% en moyenne et 29% des novices).

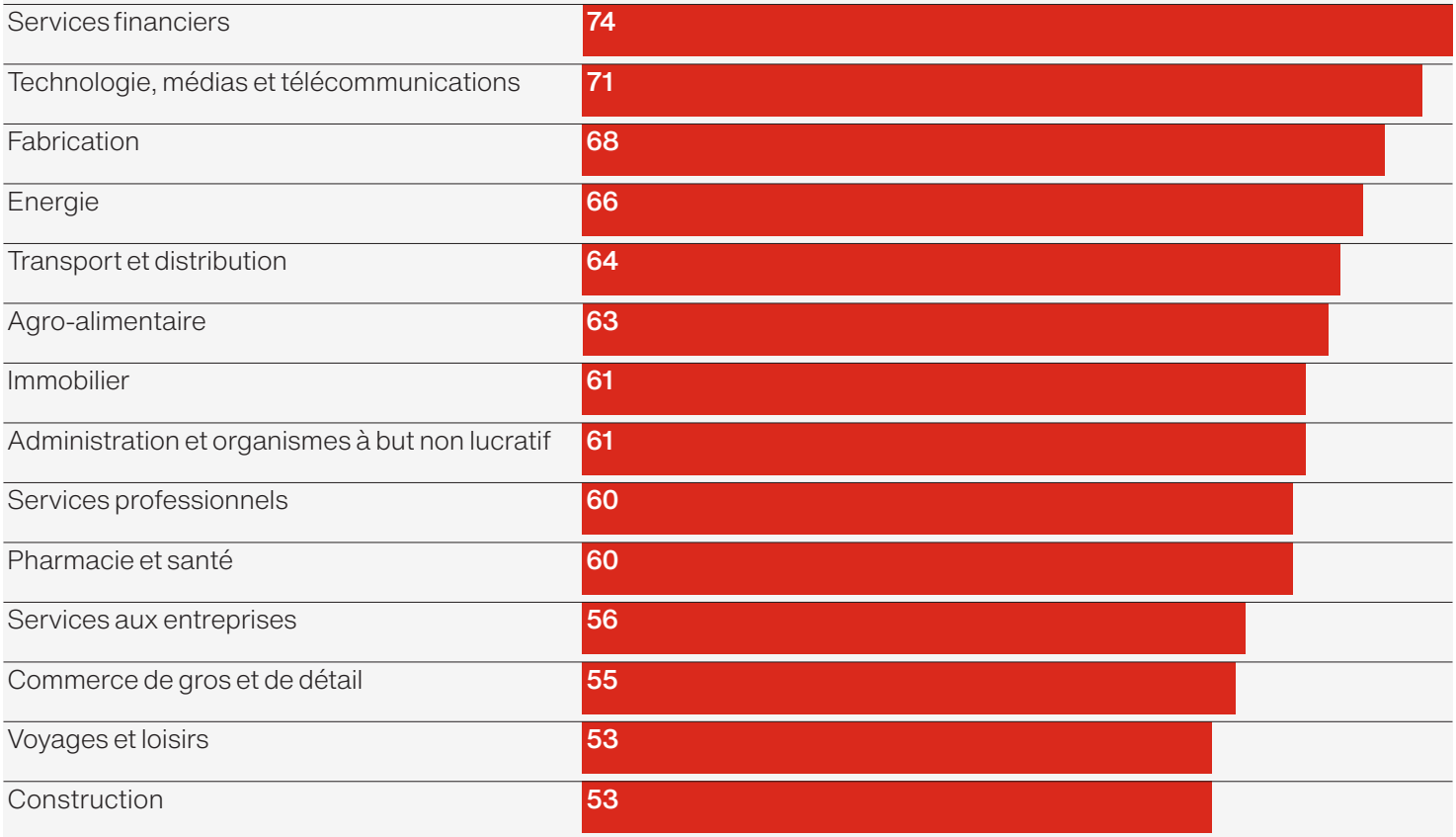
Sans surprise, c'est dans le secteur des services financiers que la souscription d'une police de cyber-assurance est la plus forte: 74% des entreprises ont en effet souscrit des garanties contre les cyber-risques, soit au titre d'une police dédiée, soit dans le cadre d'une police plus large, et 18% des entreprises prévoient de le faire à brève échéance. Les entreprises du secteur des construction et des loisirs se situent à l'autre extrémité du spectre: 53% des deux secteurs disposent d'une forme de couverture contre les cyber-risques.

Il est intéressant de noter que les entreprises assurées sont plus susceptibles de répondre à une cyber-attaque en renforçant leurs défenses que les autres. L'une des raisons pourrait être qu'un assureur leur demanderait si elles ont pris des mesures d'atténuation contre certaines menaces ou si elles l'ont aidé à régler un problème après une attaque.

Les expertes ont également répondu de façon plus adaptée aux défis posés par la pandémie. Elles sont beaucoup plus nombreuses à avoir augmenté le télétravail, adopté des technologies basées sur le cloud et collaboratives, transféré les paiements en ligne et accéléré leur plan de transformation numérique.

Que font les experts?
suite

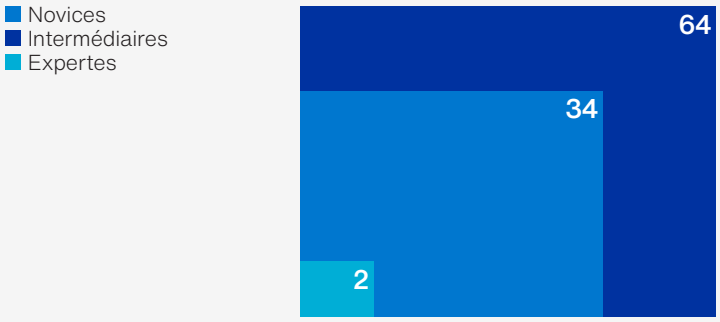
Adoption de la cyberassurance par secteu (%)
En tant que police autonome ou en complément d'une autre police.



Aperçu par pays

Belgique

Cyber-maturité (%)

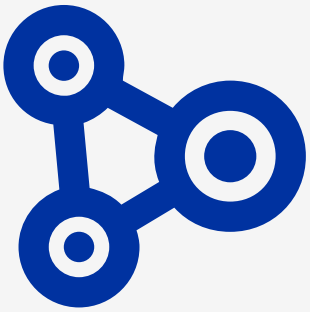


+10%

Mauvaise publicité et impact négatif sur l'image de marque en hausse de 10% sur les deux dernières années.

x2

Le nombre d'entreprises ayant causé une faille pour des partenaires commerciaux a doublé l'an dernier pour atteindre 24%.

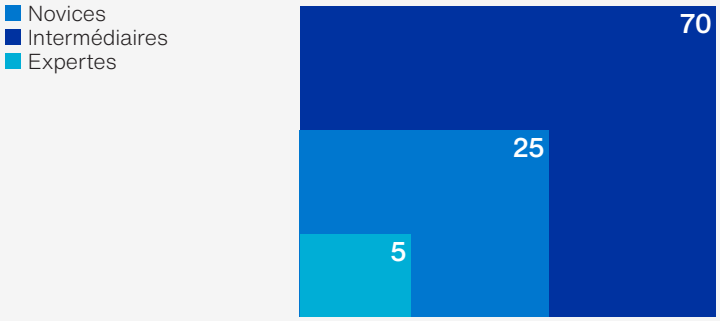


Top trois des priorités de dépenses

1. Répondre aux menaces et vulnérabilités existantes.
2. Se mettre en conformité réglementaire ou se mettre à niveau.
3. Améliorer la sécurité des services et applications destinés aux clients.

France

Cyber-maturité (%)



24%

Pourcentage d'entreprises dont la solvabilité a été réellement menacée par une attaque.

#1

La principale raison d'investir dans la cyber-assurance est la sécurité des données.

Top trois des priorités de dépenses

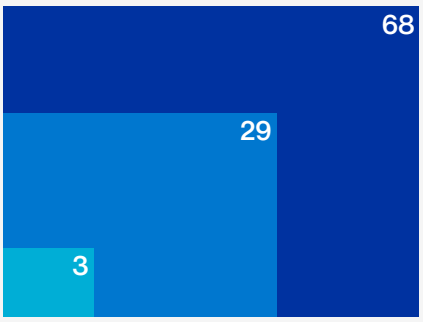
1. Répondre aux menaces et vulnérabilités existantes.
2. Se mettre en conformité réglementaire ou se mettre à niveau.
3. Améliorer la sécurité des services et applications destinés aux clients.

Aperçu par pays
suite

Allemagne

Cyber-maturité (%)

- Novices
- Intermédiaires
- Expertes

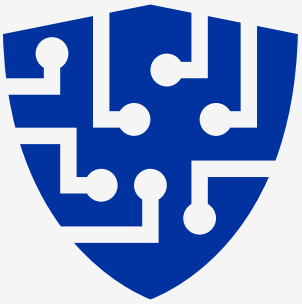


3.1m€

Cyber-attaque la plus lourde subie l'année dernière.

27%

Pourcentage d'entreprises ayant souscrit des garanties de cyber-assurance ou amélioré leurs garanties de cyber-assurance après une attaque.



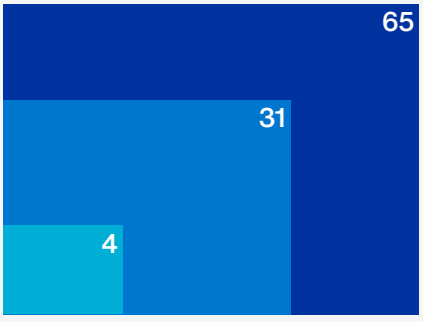
Top trois des priorités de dépenses

1. Répondre aux menaces et vulnérabilités existantes.
2. Améliorer la sécurité des services et applications destinés aux clients.
3. Politiques et procédures internes de cybersécurité.

Irlande

Cyber-maturité (%)

- Novices
- Intermédiaires
- Expertes



#1

La principale raison d'investir dans la cyberassurance est la crainte du coût d'une violation potentielle.

34%

Pourcentage d'entreprises ayant souscrit des garanties de cyber-assurance ou amélioré leurs garanties de cyber-assurance après une attaque. Contre 24% l'an dernier.

Top trois des priorités de dépenses

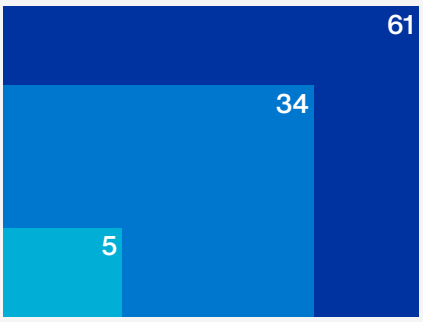
1. Formations à la cybersécurité et sensibilisation des salariés.
2. Réaliser des scans de vulnérabilité de l'environnement.
3. Respecter les exigences en matière de sécurité des partenaires.

Aperçu par pays
suite

Pays-Bas

Cyber-maturité (%)

- Novices
- Intermédiaires
- Expertes

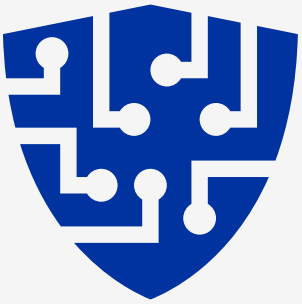


2m€

Cyber-attaque la plus lourde subie l'année dernière.

x3

Les entreprises sont trois fois plus nombreuses à avoir souscrit des garantie de cyber-assurance ou amélioré leurs garanties de cyber-assurance.



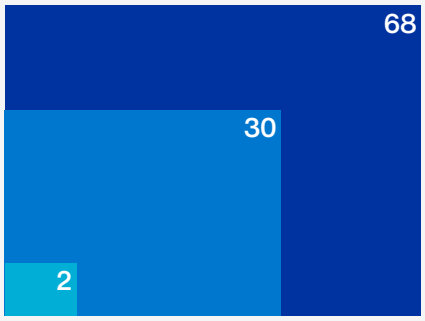
Top trois des priorités de dépenses

1. Répondre aux menaces et vulnérabilités existantes.
2. S'assurer que les partenaires respectent nos exigences de sécurité.
3. Améliorer la sécurité des services et applications destinés aux clients.

Espagne

Cyber-maturité (%)

- Novices
- Intermédiaires
- Expertes



#1

La principale raison d'investir dans la cyber-assurance est le souci de la sécurité des données.

x2

Le nombre d'entreprises ayant perdu des clients en raison d'une faille a plus que doublé au cours des deux dernières années.

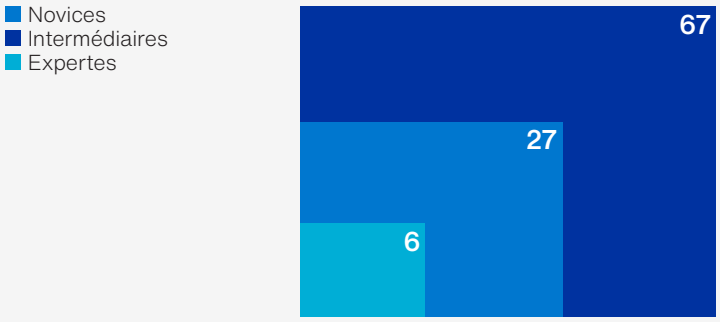
Top trois des priorités de dépenses

1. Répondre aux menaces et vulnérabilités existantes.
2. Améliorer la sécurité des services et applications destinés aux clients.
3. Se mettre en conformité réglementaire ou se mettre à niveau.

Aperçu par pays
suite

Royaume-Uni

Cyber-maturité (%)



x2

Le nombre d'entreprises ayant dû s'acquitter d'une amende importante après une faille a plus que doublé depuis l'an dernier.

20%

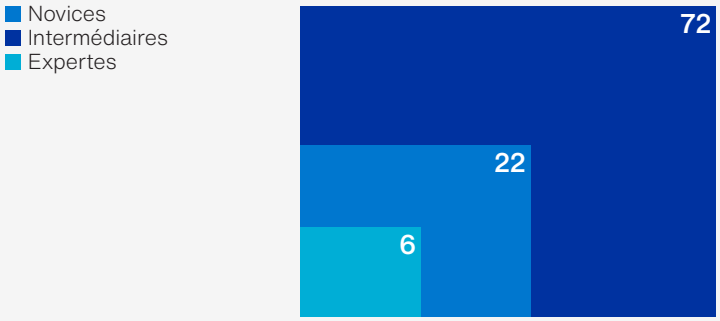
Pourcentage d'entreprises dont la solvabilité a été réellement menacée par une attaque.

Top trois des priorités de dépenses

1. Répondre aux menaces et vulnérabilités existantes.
2. Se mettre en conformité réglementaire ou se mettre à niveau.
3. Respecter les exigences en matière de sécurité des partenaires.

États-Unis

Cyber-maturité (%)



29%

Pourcentage d'entreprises ayant connu de plus grandes difficultés pour attirer de nouveaux clients après une attaque.

#1

La première raison d'investir dans la cyberassurance est de limiter les réclamations des clients suite à une attaque.

Top trois des priorités de dépenses

1. Répondre aux menaces et vulnérabilités existantes.
2. Évaluation des infrastructures de données et de technologies.
3. Respecter les exigences en matière de sécurité des partenaires.

Priorités en matière de dépenses

Après deux années de pandémie, et plusieurs vulnérabilités de grande ampleur, les entreprises semblent revenir aux fondamentaux. Elles mettent l'accent sur les menaces existantes (en veillant à ce que les appareils soient dotés des correctifs adéquats et mis à jour), et s'assurent que les polices et procédures sont à jour, notamment en testant leurs plans de réponse aux incidents. Finalement, elles luttent contre les attaques de phishing (le principal mode d'intrusion des attaques par ransomware) en dispensant des formations à la cybersécurité au sein de l'entreprise.

Très grandes entreprises (1 000 salariés et plus)
✓ Répondre aux menaces et vulnérabilités existantes
✓ Se mettre en conformité réglementaire et/ou se mettre à niveau
✓ Revoir les politiques et procédures internes de cybersécurité
✓ Améliorer la sécurité des services et applications destinés aux clients
✓ Élaborer ou mettre en œuvre un cadre formel de gestion de la cybersécurité pour les technologies/l'informatique

Petites entreprises (0–49 salariés)
✓ Répondre aux menaces et vulnérabilités existantes
✓ Se mettre en conformité réglementaire et/ou se mettre à niveau
✓ Mettre en œuvre des systèmes pour détecter les salariés, connections, appareils ou logiciels non autorisés
✓ S'assurer que les partenaires commerciaux/tiers respectent les exigences en matière de sécurité
✓ Réaliser des scans de vulnérabilité de l'environnement

Cette liste n'est pas exhaustive et ne comprend que les principales priorités des entreprises selon notre étude. Les mesures énumérées dans cette liste ne doivent pas être considérées comme une recommandation d'Hiscox et nous ne garantissons pas qu'une entreprise qui mettrait en œuvre toutes les mesures de cette liste soit totalement protégée contre les cyber-risques.

Hiscox a sollicité Forrester Consulting pour évaluer les capacités de gestion des cyber-risques des entreprises. Au total, 5,181 professionnels en charge de la stratégie de cybersécurité de leur entreprise ont été sondés (plus de 900 personnes par pays pour les États-Unis, le Royaume-Uni, la France et l'Allemagne; plus de 400 pour la Belgique, l'Espagne et les Pays-Bas; et plus de 200 pour la République d'Irlande). Les participants ont rempli le questionnaire en ligne entre le mardi 30 novembre 2021 et le vendredi 21 janvier 2022.

Le profil complet des participants est détaillé ci-dessous.

Niveau (%)	
Fondateur/cadre de niveau C	32
Vice-président	23
Administrateur	34
Directeur	12

Secteur (%)	
Services aux entreprises	9
Construction	7
Énergie	4
Services financiers	9
Agro-alimentaire	4
Administration et organismes à but non lucratif	5
Fabrication	8
Pharmacie et santé	8
Services professionnels	9
Immobilier	4
Commerce de gros et de détail	8
Technologie, médias et télécommunications	18
Transport et distribution	5
Voyages et loisirs	3

Service (%)	
Haute direction	12
e-commerce	3
Finance	9
Direction juridique	4
Ressources humaines	5
Informatique et technologie	19
Marketing et communications	5
Opérations	10
Propriétaire	18
Achats	3
Gestion de produit	4
Gestion des risques	4
Ventes	4

Nombre de salariés (%)	
1 000+	25
250-999	15
50-249	15
10-49	19
1-9	26

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

22054 05/22