Rapport Hiscox 2023 sur la gestion des cyber-risques

HISCOX

Sommaire

Illustration de couverture: johnholcroft.com
Conception du rapport: somethingbrighter.com

Introduction

Cette année, le rapport met en lumière plusieurs évolutions dans le paysage de la cybersécurité qui intéresseront toutes les personnes concernées par la lutte contre la piraterie informatique.

Eddie Lamb
Directeur de la sensibilisation aux risques Cyber Hiscox

L'un des résultats les plus notables de cette année est l'augmentation sensible du nombre de petites entreprises ciblées: 36 % d'entre elles ont fait l'objet d'une attaque. Ce chiffre a augmenté de moitié au cours des trois dernières années. Une chose est désormais claire, ce n'est pas parce qu'une entreprise est petite qu'elle échappera aux griffes des cyber-criminels. Toutefois, et il faut s'en féliciter, le rapport montre également que les plus petites entreprises ont augmenté leurs dépenses à un rythme nettement plus rapide que les autres types d'entreprise, ce qui pourrait aider à contrer les attaques croissantes.

On trouve dans notre panel, un certain nombre de grandes entreprises ayant enregistré des pertes à sept chiffres. La bonne nouvelle est tout de même que les coûts ont globalement été contenus chez l'ensemble des participants de l'étude. Cette observation s'explique partiellement par la tendance de recours à la fraude, comme le détournement de paiement au moyen d'un piratage de messagerie professionnelle, ce qui nécessite généralement moins de compétences techniques mais s'avère moins lucratif. La généralisation de la cyber-assurance peut également avoir joué un rôle. Près de trois quarts des entreprises attaquées disposaient d'une certaine forme de couverture Cyber.

Les attaques impliquant des rançongiciels sont restées stables et la proportion de rançons versées a légèrement chuté cette année. La principale raison pour laquelle les victimes ont payé, était d'éviter que des données sensibles ne soient divulguées. Cela marque une légère évolution dans le *modus operandi* des pirates qui commencent à privilégier l'exfiltration de données à la place de leur chiffrement. On constate de plus en plus qu'il est totalement aléatoire de traiter avec les extorqueurs. En effet, moins de la moitié des entreprises ont récupéré toutes leurs données.

Malgré l'augmentation constante du nombre de cyber-attaques, le rapport de cette année apporte également quelques bons présages. De façon justifiée ou non, la perception des risques évolue sensiblement, et beaucoup d'entreprises ne voient plus la cyber-menace comme le danger numéro un. Cela peut s'expliquer par la progression d'autres problématiques, notamment les difficultés économiques. Mais c'est également le reflet de la hausse des budgets de cybersécurité, d'un meilleur déploiement des mesures de sécurité et d'une prise de conscience accrue des dirigeants, ou tout simplement du fait que la cybersécurité est devenue un risque à gérer comme n'importe quel autre risque d'entreprise.

Améliorer la compréhension et sensibiliser au défi que représente la cybersécurité est l'un des objectifs de ce rapport. C'est également un aspect fondamental de notre mission d'assureur. La Hiscox CyberClear Academy propose des formations en ligne de sensibilisation à la cybersécurité aux salariés de nos clients, auxquelles ont participé 36 000 personnes issues de 7 000 entreprises depuis 2017. Étant donné le nombre de personnes qui continuent à être victimes d'emails de phishing (toujours en tête des attaques par ransomware), la répétition des formations de sensibilisation doit être une priorité pour toutes les entreprises dont la présence en ligne est importante.

Nous espérons que ce rapport aidera les entreprises à jauger leur propre résilience à la cyber-menace et à comparer le niveau de leur capacité en la matière à celui de leurs homologues. Pour se faire, nous vous invitons à découvrir notre outil interactif de modélisation des capacités de gestion des cyber-risques grâce auquel vous pourrez identifier les forces et faiblesses des mesures de cybersécurité de votre entreprise et prévoir un plan d'action pour renforcer vos défenses. Vous pouvez comparer votre organisation par taille, par secteur et par pays à plus de 16 000 autres entreprises. Le combat contre la piraterie informatique est une lutte sans fin, mais la préparation est la clé pour déjouer les attaques et limiter les éventuels dommages pour votre entreprise.

Résumé

Plus de la moitié des entreprises ont signalé des attaques

Le nombre de cyber attaques a progressé pour la troisième année consécutive: 53% des entreprises ont subi une attaque, contre 48% l'an dernier.

La perception évolue

Cinq pays sur huit considèrent désormais les cyber-attaques comme le principal risque des entreprises. Les problématiques économiques et de concurrence suscitent davantage d'attention.

Le coût des attaques a été contenu

Le coût médian par entreprise attaquée est en léger recul, passant d'environ 15 640€ à un peu plus de 14 766€.

Des pertes lourdes sont toujours possibles

Une entreprise attaquée sur huit (12%) a enregistré des coûts de 230 000€ ou plus.

Les petites entreprises sont plus durement touchées

Au cours des trois dernières années, le nombre d'entreprises de moins de dix salariés ayant subi une attaque a augmenté de plus de moitié pour atteindre 36%.

La fraude est la menace numéro un

Un tiers des entreprises attaquées ont subi des pertes financières à la suite d'un détournement de paiement (34%).

Résister aux ransomwares

Une entreprise attaquée sur cinq a fait l'objet d'une demande de rançon, mais celles qui ont payé sont moins nombreuses (63% contre 66% l'an passé). Parmi les entreprises ayant versé une rançon, moins de la moitié ont récupéré l'intégralité de leurs données.

Augmentation des dépenses de cybersécurité

Le coût médian des dépenses de cybersécurité a progressé de 39% sur les trois dernières années pour atteindre 142 600€. Dans les entreprises de moins de dix salariés, il a quadruplé en deux ans.

Le maillon faible

Le piratage de messagerie professionnelle a été le mode d'intrusion le plus utilisé par les pirates, suivi des serveurs d'entreprise ou des serveurs cloud.

Perception des cyber-risques

Les cyber-risques demeurent la source de préoccupation numéro un des entreprises, mais des élans d'optimisme commencent à apparaitre.

Le facteur 'peur' en déclin

Les entreprises apprennent-elles à vivre avec la cyber-menace? Les participants de l'étude continuent de placer le risque d'une cyber-attaque en tête de leurs préoccupations. Mais nous avons assisté cette année à une évolution sensible de la perception du risque, et cela marque une avancée notable.

La proportion d'entreprises ayant cité la cyber-menace comme risque élevé a chuté de 45% à 40% cette année, mais cette observation doit néanmoins être mise en parallèle avec une tendance globale d'accroissement de la confiance des entreprises dans toutes les catégories de risque. La cyber-menace ressort juste avant les problématiques économiques, comme la récession, l'inflation ou les taux de change (38%) et l'émergence d'un nouveau concurrent (36%).

Alors que la cyber-menace reste perçue comme le danger numéro un dans la plupart des secteurs d'activité, plusieurs secteurs (les services aux entreprises, la construction, le transport, l'agro-alimentaire et les voyages et loisirs) considèrent désormais que les problématiques économiques sont plus importantes.

La cyber-menace constituait alors la principale menace dans sept pays sur huit. Or, ce chiffre a chuté à cinq cette année, même si elle reste dans le top trois des risques dans tous les pays, hormis la Belgique, où prévalent les risques comme le manque de compétences, les pertes économiques et la concurrence. Cela constitue un autre facteur indiquant que certaines entreprises estiment désormais que d'autres risques représentent une menace équivalente ou supérieure à la cyber-menace.

Principaux risques pour les entreprises (%)

		2023	2022
1.	Cyberattaque	40	45
2.	Pertes liées à des problématiques économiques, par ex. récession, inflation, taux de change	38	40
3.	Émergence d'un nouveau concurrent	36	36
4.	Manque de compétences	35	40
5.	Dommage à la réputation, par ex. articles négatifs dans la presse, défaillance produit, etc.	35	37
6.	Modifications réglementaires ou législatives	34	37
7.	Pandémie/maladies infectieuses affectant nos opérations	33	42
8.	Conflits géopolitiques affectant nos opérations, par ex. pénuries d'approvisionnement, retards, etc.	33	–
9.	Fraude/crime en col blanc à l'encontre de mon entreprise	32	38
10.	Conditions climatiques extrêmes/catastrophes naturelles affectant nos opérations	29	33

Un meilleur déploiement et une hausse des dépenses forgent l'optimisme
Davantage d'entreprises se sentent à la hauteur du défi. Les entreprises sont plus nombreuses à avoir fait part d'une diminution de leurs cyber-risques (16 % contre 12 % l'an dernier). Elles estiment que cela est dû à un meilleur déploiement des processus de cybersécurité, ainsi qu'à des budgets étendus. Les grandes entreprises sont également plus nombreuses à souligner une prise de conscience accrue de leur direction. Parmi les grandes entreprises ayant déclaré que leur exposition au risque d'attaque avait diminué, deux sur cinq (41%) mentionnent que l'implication de leur direction a conduit à une meilleure gestion, voire à un transfert des risques (cyber-assurance).

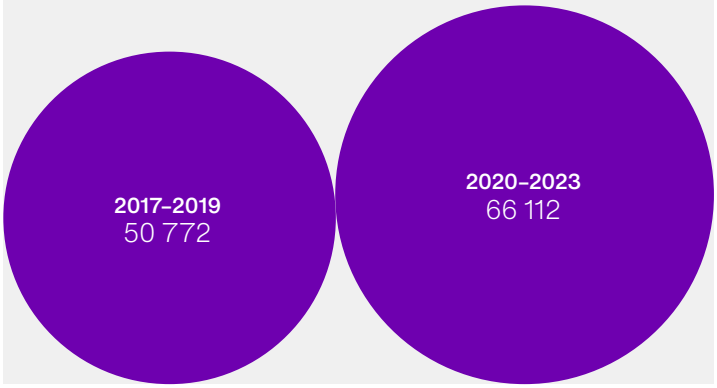
Les cyber-risques sont toujours néanmoins bien présents, en particulier pour ceux qui ont le sentiment qu'ils augmentent. Près d'un tiers (32%) des entreprises considérant que leur exposition aux risques s'est aggravée au cours des 12 derniers mois ont cité l'augmentation du télétravail comme cause. Cette préoccupation a été plus marquée parmi les entreprises de plus de 250 salariés (35 %), que parmi les petites (30 %), bien que les petites entreprises aient été marginalement plus nombreuses à évoquer une inquiétude liée à l'utilisation par leurs salariés de leurs propres appareils (27 % en ont fait état contre 26 % des grandes entreprises). Sur ce sujet, la notion de contrôle semble plus importante que jamais.

L'augmentation des correctifs suscite des inquiétudes
L'inquiétude grandit également concernant la capacité à installer tous les correctifs des fournisseurs plus d'une grande entreprise sur cinq (22 %) le mentionne comme l'une des causes de l'augmentation des cyber-risques, contre 16 % l'an passé. L'installation de correctifs est nécessaire pour pallier les vulnérabilités de sécurité des logiciels ou optimiser la performance. Les vulnérabilités et risques communs (Common vulnerabilities and exposures, CVE) ont progressé de 30 % si l'on compare la moyenne des trois dernières années à celle des trois années précédentes.

Certes, les logiciels ont toujours comporté des vulnérabilités, mais au cours des cinq à dix dernières années, les scanners automatiques, les programmes d'identification des bugs, les chercheurs et la production participative (crowdsourcing) ont permis d'améliorer la découverte des vulnérabilités et les notifications publiques.

Une fois découvertes, les éditeurs de logiciels doivent fournir des correctifs. Ensuite, il appartient aux autorités réglementaires et/ou aux compagnies d'assurance d'exiger que les sociétés qui utilisent les logiciels concernés installent les correctifs rapidement. L'installation régulière des correctifs et mises à jour des systèmes est particulièrement difficile pour les grandes entreprises dans lesquelles la gestion de ces installations est souvent complexe.

Ensemble des vulnérabilités et cyber-risques en nombre
Moyenne sur trois ans



L'expérience d'une attaque est un moteur de la confiance
Près de la moitié (48 %) des entreprises ayant subi une cyber-attaque considèrent la menace comme un risque élevé. Toutefois, comme l'an dernier, les grandes entreprises et celles qui ont été attaquées sont plus confiantes dans leur capacité à gérer une attaque, ainsi que dans l'approche du gouvernement face à la menace. Elles font davantage confiance aux facteurs internes (telles que leur technologie et l'implication de la direction) et externes (autorités réglementaire, gouvernement) pour fournir un environnement sûr ou aidant à atténuer les dommages.

Les petites entreprises sont plus hésitantes quant à leurs capacités
A l'inverse, les petites entreprises présentent un déficit de confiance. Seules trois entreprises de moins de 250 salariés sur cinq (61%) déclarent avoir confiance en leur capacité de gestion des cyber-risques. Pour les grandes entreprises, ce pourcentage est de 71%. Les petites entreprises interrogées n'ont pas la certitude que leur direction érigera la cybersécurité au rang de priorité et sont plus enclines à remettre en question la fiabilité de leur technologie informatique.

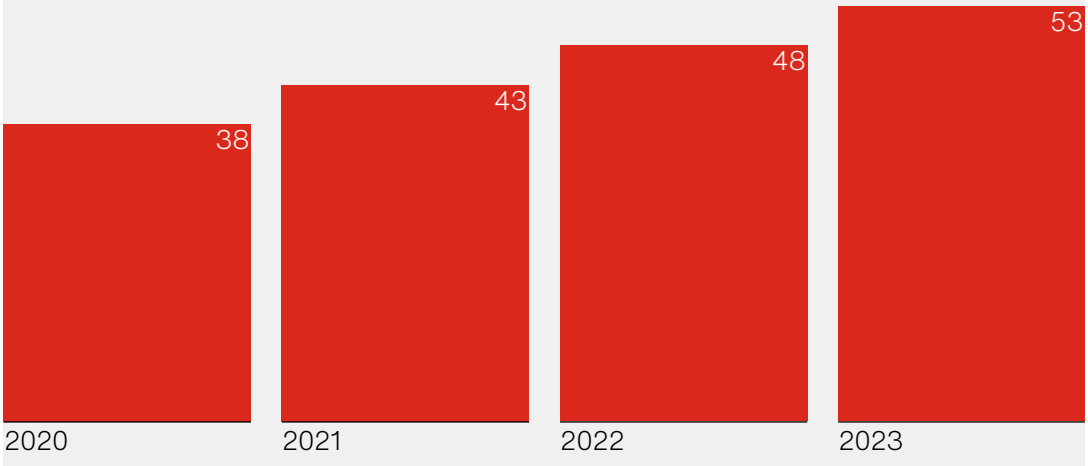
L'écart le plus faible entre les grandes et les petites entreprises concerne la question des atteintes potentielles à l'image de marque de la société si les données des clients et partenaires ne sont pas traitées de façon sécurisée. Elles s'accordent à ce sujet de façon unanime, avec 72 % des grandes entreprises et 70 % des petites se déclarant d'accord ou tout à fait d'accord.

Réalité des cyber-risques
La portée et l'intensité des attaques augmentent mais l'impact financier reste contenu.

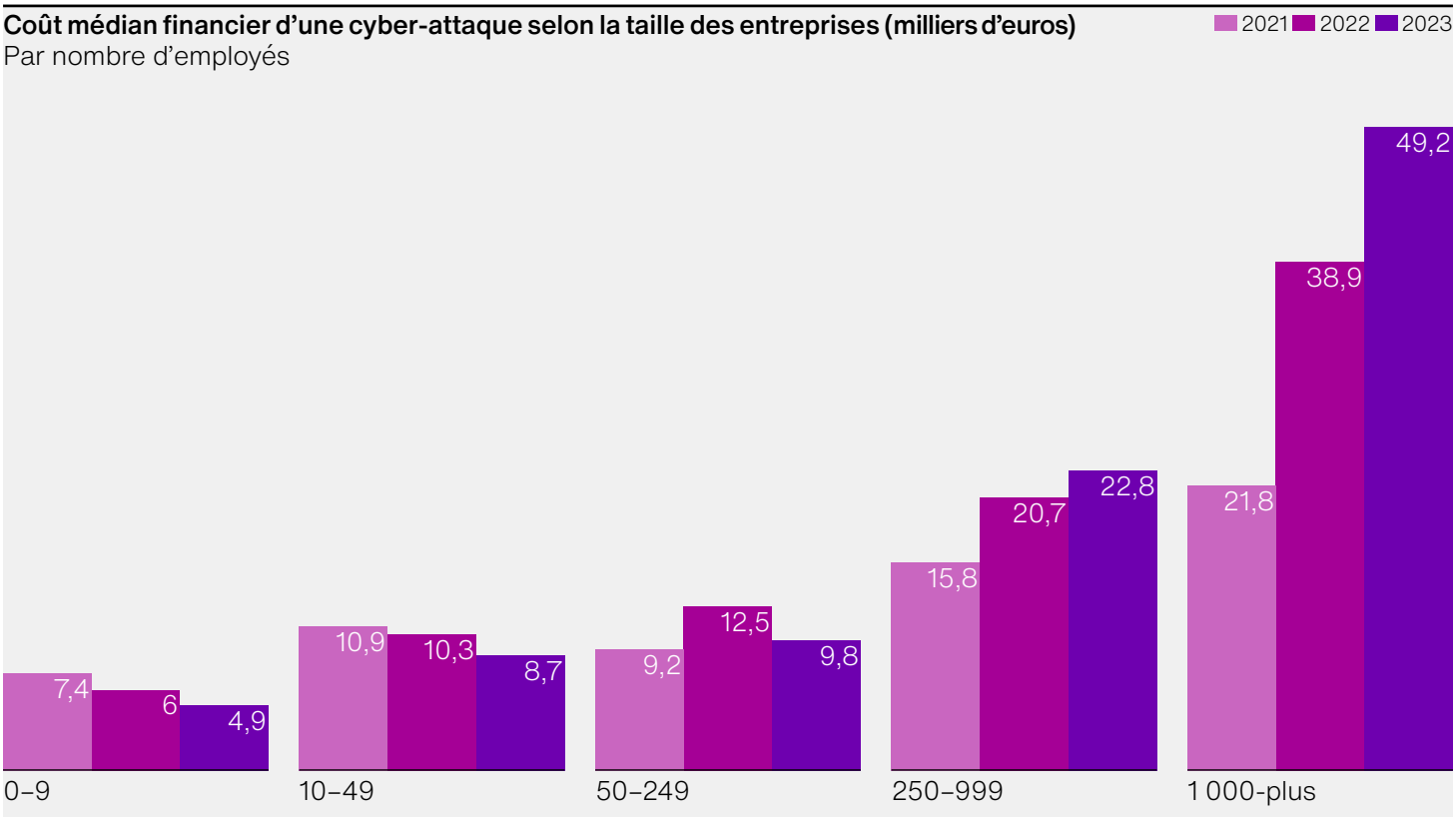
Les plus petites entreprises sont désormais des cibles
Le nombre d'entreprises signalant au moins une attaque a augmenté pour la troisième année consécutive – 53% contre 48% l'an dernier – et l'intensité des attaques s'est considérablement accentuée. Les entreprises ont fait état d'un nombre moyen de sept attaques, contre quatre l'an passé.

Ces chiffres ne représentent toutefois qu'une partie du tableau. Dans les plus grandes entreprises (de 1 000 salariés et plus), les cyber-attaques sont désormais monnaie courante. 70% d'entre elles ont rapporté au moins une attaque, contre 62% l'an dernier. Mais cela n'est pas l'apanage des grandes entreprises. Au cours des trois dernières années, le nombre d'entreprises de moins de dix salariés ayant subi une attaque est passé de 23% à 36%. Bien que les petites entreprises parviennent mieux à gérer leurs coûts et commencent à investir davantage dans la cybersécurité, il existe clairement un risque accru qu'elles doivent prendre en compte de façon sérieuse.

Entreprises ayant subi au moins une cyber-attaque (%)



Coût médian financier d'une cyber-attaque selon la taille des entreprises (milliers d'euros)
Par nombre d'employés



Impact financier stable
Malgré ce déferlement d'attaques, l'impact financier des cyber-attaques décroit d'année en année, ce qui laisse penser que les entreprises ont de meilleures capacités de détection et de neutralisation des attaques. On constate une légère augmentation du nombre d'entreprises ayant réussi à déjouer une attaque (8% contre 7% l'an dernier).

Si on observe les chiffres médians, le coût des attaques est tombé juste en dessous de 15 640€ un peu plus de 14 720€ par entreprise touchée. Le coût médian de la cyber-attaque la plus lourde a également chuté de 6 118€ à 4 922€. Néanmoins, ces chiffres masquent une grande disparité des résultats, qui s'étalent entre 1 968€ pour les entreprises de moins de dix salariés jusqu'à 9 844€ pour les entreprises de 1 000 salariés et plus.

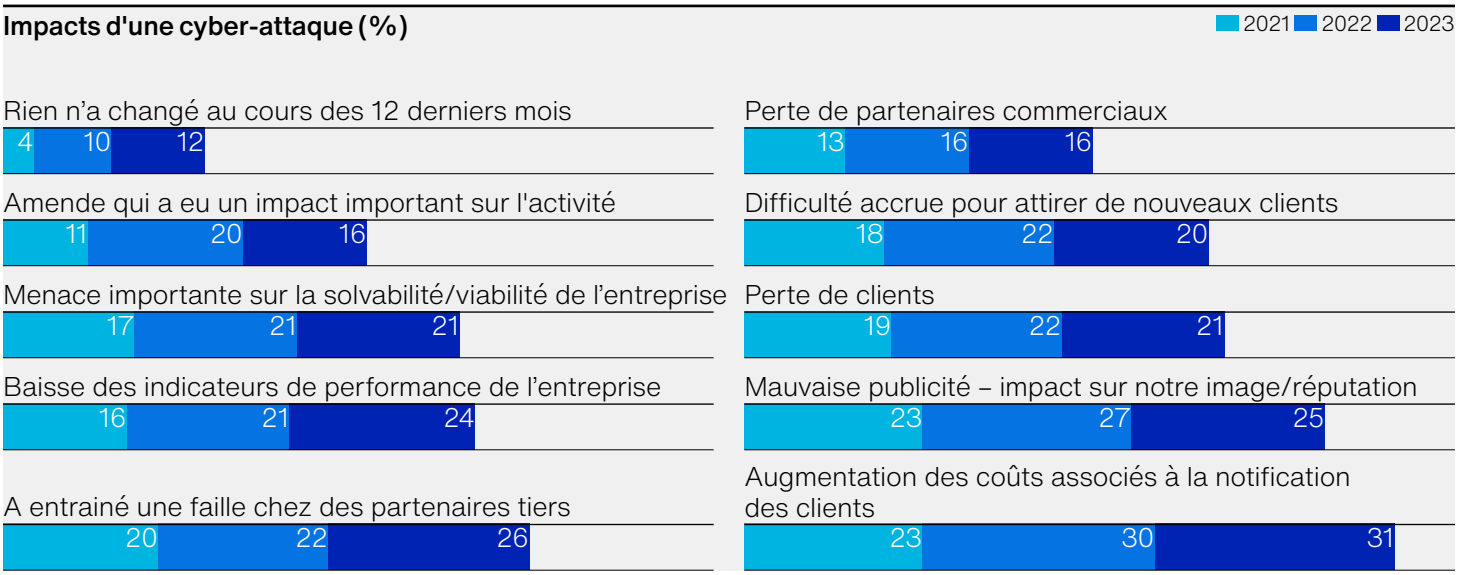
Dans notre rapport de 2022, seules quatre entreprises avaient rapporté des coûts de cyber-attaques supérieurs à 5 millions d'euros. Cette année, huit entreprises ont subi des cyber-attaques d'un tel niveau et trois d'entre elles ont dépassé les 10 millions d'euros. Une entreprise attaquée sur huit (12%) a enregistré des coûts de 235 000€ ou plus.

Les petites entreprises gèrent mieux les coûts
Les chiffres de cette année sont encourageants. Les petites entreprises parviennent à contenir les coûts des cyber-attaques. Les entreprises dans les deux catégories de taille les plus petites ont vu leurs coûts médians chuter deux années de suite. Cela est d'autant plus remarquable compte tenu du fait que l'incidence des attaques a augmenté pour les petites entreprises depuis trois ans, de la même manière que pour les plus grandes. Néanmoins, les coûts continuent de progresser pour les plus grandes entreprises. Pour les entreprises de 1 000 salariés et plus, le coût des cyber-attaques a augmenté de 125% en deux ans, s'établissant aux alentours de 49 220€.

Des coûts très variables en fonction des secteurs
Quatre secteurs ont enregistré des coûts moyens de 18 400€ ou plus: la fabrication, les transports/distribution, l'énergie (qui figure dans les trois secteurs les plus ciblés sur les trois dernières années) et les administrations/organismes à but non lucratif. Les secteurs des transports/distribution et des administrations/organismes à but non lucratif ont connu de fortes augmentations de coûts d'une année sur l'autre (28% et 83% respectivement). Quant aux entreprises de fabrication, elles ont eu des pertes moyennes les plus fortes avec la plus lourde attaque subie, à 6 587€.

La bonne nouvelle est que la plupart des secteurs sont parvenus à contenir, voire à réduire, le coût moyen de la plus lourde attaque subie. Pour les entreprises du secteur de l'énergie, le chiffre est passé de plus de 10 120€ à un peu moins de 6 440€ sur deux ans. Dans l'industrie agro-alimentaire, il a plus que diminué de moitié, s'établissant à 4 140€.

Impacts d'une cyber-attaque (%)



Vulnérabilités et impacts

Le piratage de messagerie professionnelle est, cette année encore, le principal point d'entrée des pirates, selon 35% des entreprises ciblées (et 40% des répondants du secteur des administrations/organismes à but non lucratif). Les serveurs d'entreprise, qu'ils soient internes à l'entreprise (31% des participants) ou hébergés dans le cloud (29%) ont été cités en deuxième et troisième positions. Mais dans les deux cas, ces pourcentages étaient très inférieurs à ceux de l'année précédente, ce qui suggère que la prévention porte ses fruits.

Le secteur de l'énergie semble particulièrement en proie aux intrusions via le serveur interne à l'entreprise. Le secteur de la construction est en première ligne des secteurs touchés par la violation de serveur cloud, ainsi que le secteur du voyage et loisirs et de la technologie. La principale conséquence des cyber-attaques a été la perte financière causée par les détournements de paiement (mentionnée par 34% des entreprises attaquées contre 28% deux années auparavant). La perte de données et la propagation d'un virus ont perdu du terrain pour la deuxième année consécutive.

Certains effets des cyber-attaques ont été ressentis plus largement cette année qu'auparavant. Près d'un tiers des entreprises (31%) attaquées ont fait état d'une augmentation des coûts liés à l'information de leurs clients au sujet d'une attaque. Ce chiffre progresse pour la deuxième année consécutive. Il en va de même pour les entreprises qui signalent une violation pour le compte de tiers (26% contre 20% il y a deux ans).

Il y a lieu de relever que le scénario catastrophe n'est pas si éloigné qu'on pourrait le penser. Une entreprise attaquée sur cinq (21%) a déclaré que l'impact était suffisamment important pour menacer sa viabilité. Le constat est le même pour un cinquième des très petites entreprises (moins de dix salariés).

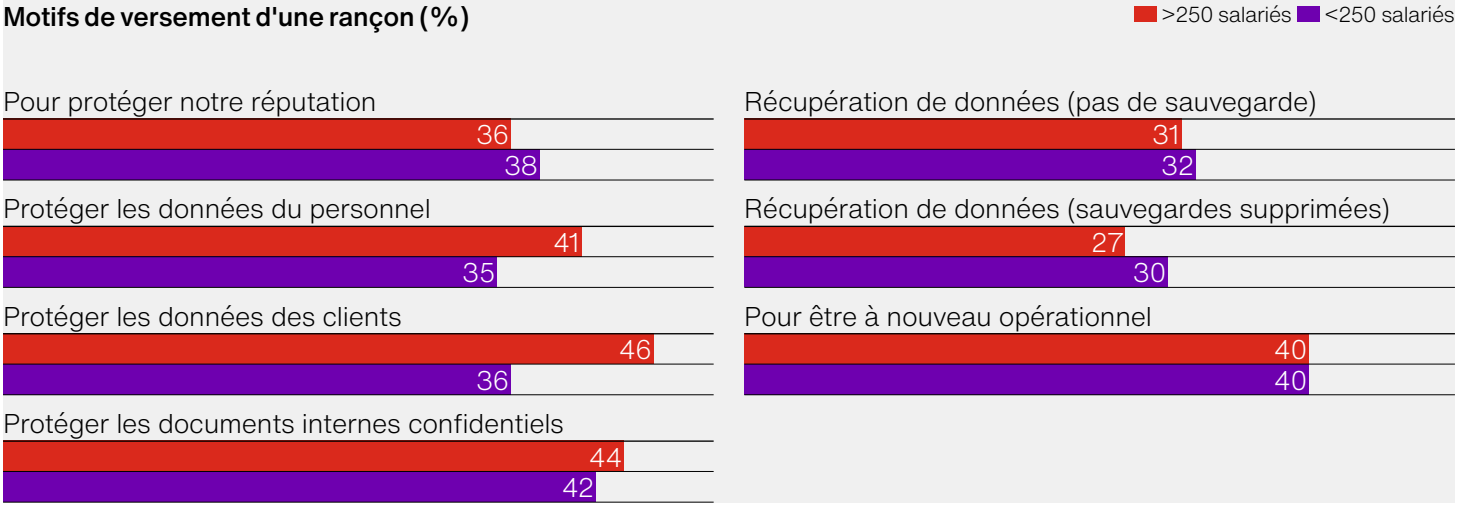
Pays par pays: L'Irlande se démarque

Quels pays sont les plus vulnérables? En nombre d'entreprises attaquées, l'Irlande se démarque cette année avec plus de sept entreprises sur 10 ciblées (71%), soit un tiers de plus que la moyenne du panel d'étude. Les entreprises irlandaises ont également été les plus ciblées, près de trois fois plus souvent que la moyenne, avec une prévalence des ransomwares (30% contre 20% en moyenne au sein de notre panel). Le serveur, premier fautif: plus de la moitié des participants irlandais ont répondu que le premier point d'entrée des pirates était le serveur appartenant à l'entreprise (57%) ou un serveur cloud (50%).

D'un point de vue financier, les pays les plus touchées ont été le Royaume-Uni (avec un coût moyen par entreprise de 22 264€), les Pays-Bas et les États-Unis (19 688€). Dans les entreprises britanniques et américaines, le piratage de messagerie professionnelle a été l'attaque la plus utilisée (mentionnée par respectivement 38% et 37% des répondants).

Il y a eu une nette augmentation du nombre d'entreprises allemandes ayant signalé une attaque (58% contre 46% l'an dernier), avec un nombre moyen d'attaques par entreprise grimpant de six à dix. A l'inverse, la Belgique et les Pays-Bas ont enregistré une baisse du nombre moyen d'attaques subies. Il peut être pertinent de relever que les Pays-Bas ont été le seul pays de notre étude à avoir amélioré sa note d'évaluation des capacités de gestion des cyber-risques dans notre modélisation de la maturité cette année.

Motifs de versement d'une rançon (%)



Le Ransomware reste une menace

Une entreprise attaquée sur cinq (20%) a reçu une demande de rançon, un chiffre en légère hausse par rapport à l'an dernier (19%). La proportion d'entreprises ayant versé une rançon a chuté de 66% à 63%, mais la rançon moyenne a progressé de 13% pour atteindre 9 844€. Sur la même base, les coûts moyens de récupération ont légèrement baissé (4 968€). La rançon la plus élevée s'est élevée à 492 200€, même si le chiffre médian de l'attaque la plus lourde était 4 922€, là où il n'était que de 3 680€ l'année d'avant.

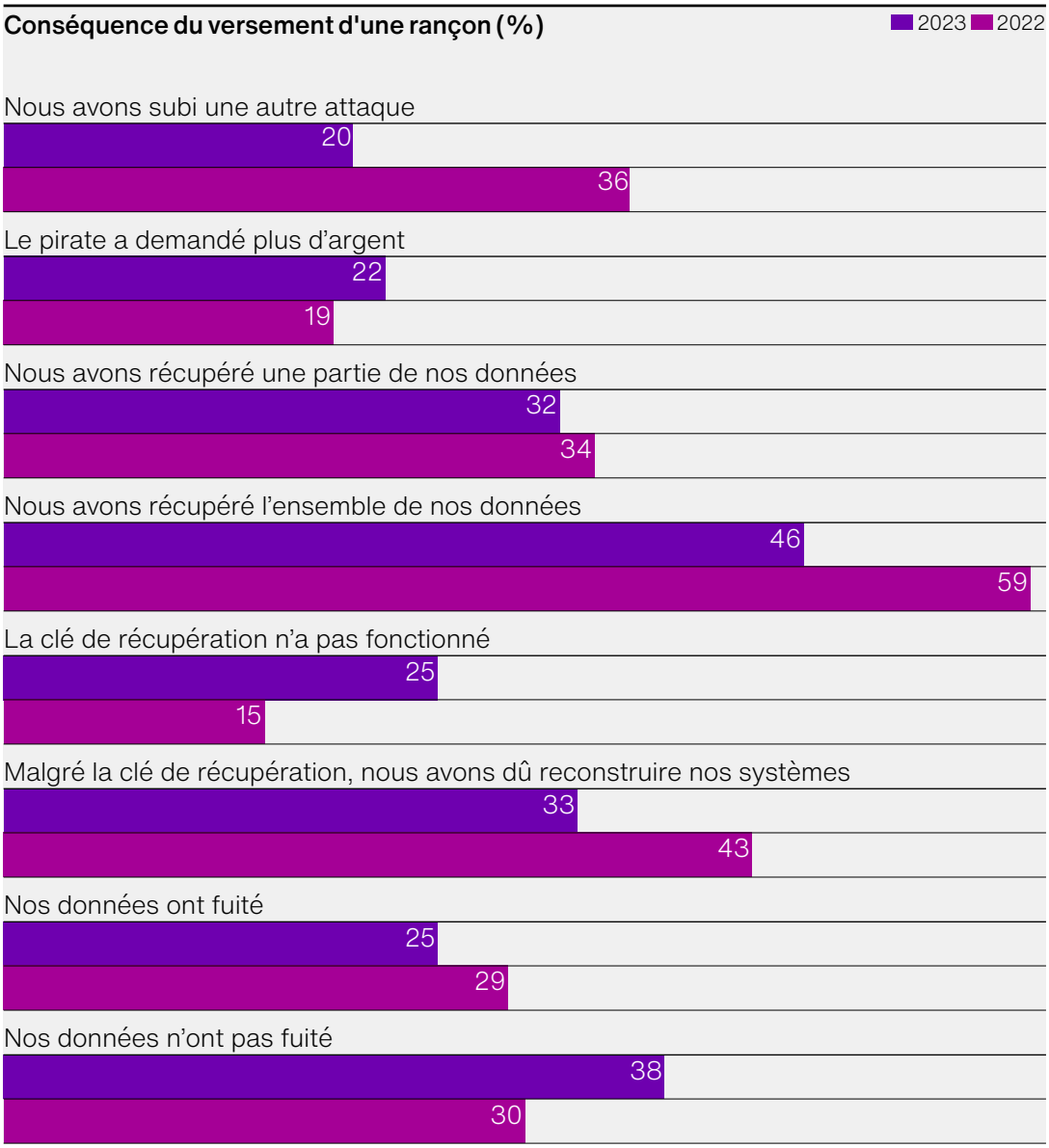
Les principales raisons avancées pour justifier le versement de la rançon ont été la protection des informations internes confidentielles (43%) ou des données des clients (42%). C'est cette dernière raison que les grandes entreprises ont le plus mentionnée pour justifier le versement d'une rançon. Le principal mode d'intrusion des pirates est encore l'envoi d'emails de phishing (selon 63% des victimes). Pour la troisième année d'affilée, le phishing est de loin la première cause d'attaque par ransomware, et la deuxième méthode la plus courante reste le vol d'identifiants. La lutte contre ces deux types d'attaque commence par la formation des salariés.

Se prémunir des ransomwares n'est jamais une chose aisée, mais former les salariés à l'utilisation de mots de passe complexes, à la protection de leurs identifiants grâce à l'authentification à plusieurs facteurs (MFA) et au phishing constituent autant de moyens relativement simples et peu onéreux pour atténuer les risques dans les entreprises, quelle que soit leur taille.

Est-il utile de payer?

Dans la plupart des cas, non. Seules 46% des victimes ont indiqué avoir récupéré l'intégralité de leurs données après versement de la rançon, contre 59% l'an passé. Environ un tiers d'entre elles (32%) ont récupéré une partie de leurs données, tandis que dans un quart des situations, les données ont fuité ou la clé de récupération n'a pas fonctionné. En outre, une entreprise sur cinq (20%) a subi de nouveau une autre attaque.

Une observation encourageante est que les entreprises sont plus nombreuses cette année à avoir récupéré leurs données à partir d'une sauvegarde (46%), même si un tiers des entreprises attaquées (32%) ont déclaré avoir payé parce qu'elles n'avaient pas de sauvegarde. Ce chiffre n'était que de 26% l'an dernier. Les entreprises ayant obtenu une note faible dans notre modélisation de la cyber-maturité, ont indiqué comme principal motif de versement d'une rançon, la nécessité d'être de nouveau opérationnelles (44%), ce qui signifie que les entreprises les moins bien préparées ont peu d'autre choix que de payer. Il est en effet essentiel pour elles de se remettre rapidement en ordre de marche. Si l'on considère que seules 46% des entreprises récupèrent l'intégralité de leurs données après versement d'une rançon et que 22% font l'objet d'autres demandes des pirates, est-ce réellement un risque à prendre? En matière de cybersécurité, la maturité donne une chance de se rétablir après un ransomware sans payer, voire même de limiter les conséquences de l'attaque dès le départ.


Conséquence du versement d'une rançon (%)
2023
2022
Nous avons subi une autre attaque
20
36
Le pirate a demandé plus d'argent
22
19
Nous avons récupéré une partie de nos données
32
34
Nous avons récupéré l'ensemble de nos données
46
59
La clé de récupération n'a pas fonctionné
25
15
Malgré la clé de récupération, nous avons dû reconstruire nos systèmes
33
43
Nos données ont fuité
25
29
Nos données n'ont pas fuité
38
30

Étude de cas
Une entreprise paralysée en une fraction de seconde

Une attaque de rançongiciel
Tout a commencé comme un jour normal au garage Autobedrijf de Pee. Comme le réceptionniste était en congé, le propriétaire, Arjan de Pee, surveillait personnellement les emails entrants. C'est alors qu'il aperçut un email de KPN, le réseau mobile, avec une facture jointe. Il l'ouvrit afin de l'imprimer. Tout à coup, son écran sembla subitement virer au noir.

"*Tous les systèmes ont planté"* indiqua-t-il. "*Tout ce que j'avais devant moi, c'était un écran noir avec du texte blanc, comme à l'époque du DOS."*

La suite
Arjan tenta immédiatement de limiter les dégâts en débranchant le câble réseau. En vain. Tous les fichiers étaient déjà inexorablement chiffrés. "*Chaque dossier contenait un fichier texte avec un message précisant que les fichiers étaient bloqués et qu'ils ne seraient débloqués qu'en échange d'un versement en Bitcoin*."

Sans s'exécuter, Arjan appela sa société de services informatiques. Ils intervinrent immédiatement et purent réinstaller les programmes. Une heure plus tard, l'entreprise était remise en ordre de marche.

Le coût
Le dommage financier a été limité au paiement de l'intervention de la société et de l'installation de mesures de cybersécurité supplémentaires. Mais le dommage émotionnel était considérable. "*Notre société existe depuis 34 ans et j'ai perdu toutes les photos de l'ouverture*" déplora-t-il: "*Je ne les récupèrerai jamais.*"

A retenir
Tout cela a permis à Arjan de faire passer un message qu'il considère important pour les autres chefs d'entreprise: "*Il est judicieux de prendre des mesures complémentaires pour protéger vos biens.*" Et cela inclut les ressources numériques.

Arjan protège maintenant les données de ses clients en utilisant des contrôles d'accès et il s'assure que les données critiques soient sauvegardées et stockées séparément. Les cybercriminels peuvent toujours attaquer, mais au moins il y a d'autres barrières en place pour protéger les données personnelles des clients. "*En outre, je demande aux clients de communiquer uniquement leurs données personnelles strictement nécessaires.*"

Conseils
Arjan a d'autres conseils. Premièrement, anticipez ce qui se passerait si tous vos ordinateurs tombaient en panne. Comment permettre à votre entreprise de reprendre ses activités le plus rapidement possible? Que faut-il mettre en place pour cela? Et comment les processus d'entreprise peuvent-ils être relancés hors ligne?

Deuxièmement, apprenez comment prévenir une cyber-attaque et discutez-en avec tous vos salariés ou dispensez des formations à la cybersécurité à vos salariés. Commencez par les choses simples, comme la mise en place de mots de passe longs et complexes sur tous les postes informatiques.

Développer la résilience
Élaborer une stratégie proactive, et faire les dépenses adéquates pour la soutenir.

Comment les entreprises doivent-elles renforcer leur résilience aux cyber-attaques?
Il y a deux manières d'aborder la gestion des cyber-risques. La première est d'adopter une attitude proactive. La seconde est d'avoir une démarche réactive ou défensive.

Les entreprises de notre étude se situent majoritairement dans la première catégorie. Près de la moitié d'entre elles (48%) sont principalement motivées par des facteurs positifs tandis que 6% seulement répondent à des facteurs réactifs ou négatifs. Parmi les principales motivations, on trouve la volonté de rassurer les clients sur le fait que l'entreprise prend la cybersécurité au sérieux (27%) et le souci d'éviter les interruptions d'activités (26%). Les facteurs négatifs concernent le respect des exigences réglementaires (25%) ou la mise en place de mesures à la demande des clients (17%).

La même attitude proactive se retrouve dans les petites entreprises de moins de 50 salariés, mais chez elles, le facteur dominant est la volonté d'éviter l'interruption d'activités. Les entreprises qui n'ont pas subi d'attaque cette année étaient plus enclines à répondre à des facteurs positifs, 56% d'entre elles ayant adopté une attitude proactive contre 42% des entreprises attaquées. Dans la mesure où l'attitude proactive semble être la bonne démarche à adopter, sur quoi les entreprises devraient-elles mettre l'accent?

Quels sont les facteurs annonçant une cyber-attaque?

Une évaluation de la cyber-maturité permet d'analyser dans quelle mesure vos contrôles de sécurité sont efficaces pour gérer les risques auxquels une entreprise est confrontée. Plus les défenses d'une entreprise sont éprouvées, plus celle-ci est prête à prévenir une cyber-attaque ou à en minimiser l'impact.

Bien qu'une cyber-attaque ne soit jamais totalement prévisible, le manque d'attention à l'égard de ces dix critères de maturité peut indiquer une attaque probable selon notre modélisation de la cyber-maturité.

- Étude de vulnérabilité/tests d'intrusion.
- Test des vulnérabilités des nouveaux logiciels.
- Mise en œuvre de l'authentification à plusieurs facteurs.
- Agréger/stocker de façon centralisée les données relatives aux événements de sécurité.
- Contrôler les communications chiffrées.
- Utiliser des VPN.
- Identifier les nouveaux équipements/logiciels/sources de données sur le réseau.
- Détecter les communications suspectes sur le réseau.
- Corriger les vulnérabilités de sécurité.
- Suivi/analyse des données d'événements de sécurité.

Que font les entreprises cyber-expertes?
Les cyber-expertes sont des entreprises dont la note est supérieure à quatre sur cinq dans la modélisation et elles sont encore très peu nombreuses à atteindre ce niveau (à peine 3% cette année). (Voir les résultats complets de l'évaluation de cette année à la page 14). Les entreprises du secteur de l'énergie comptent proportionnellement plus d'expertes (6%) devant les services financiers et les administrations (4%).

Les grandes entreprises sont moins présentes dans le groupe des moins bien notées (les novices). Seules 20% des entreprises de 1 000 salariés et plus sont des novices contre 42% des plus petites entreprises (1-9 salariés). Il y a également 1% de personnes en télétravail en moins dans les entreprises expertes.

Il convient de relever que l'un des grands critères de différenciation des entreprises classées expertes est l'implication de la direction dans l'effort de cybersécurité. 86% d'entre elles indiquent que la haute direction est bien au fait de la gestion de la cybersécurité, contre 57% des novices seulement.

Les principales mesures prises par nos cyber-expertes incluent

Petites entreprises (moins de 250 salariés)

✔	Appliquer l'authentification à plusieurs facteurs, utilisée pour les accès sensibles ou privilégiés aux systèmes informatiques, comme l'accès aux données à caractère personnel, l'accès à distance et les fonctions d'administration des systèmes.
✔	Contrôler les communications entre les appareils connectés au réseau, par exemple en utilisant un firewall installé sur la machine comme Windows Defender.
✔	Identification proactive et suppression des logiciels malveillants, comme les antivirus ou l'EDR (solution de détection et de blocage des menaces sur les terminaux).
✔	Sauvegarder les données à distance de façon sécurisée, afin de se prémunir du risque de ne pas pouvoir récupérer des données perdues.
✔	Gérer le cycle de vie des correctifs de logiciels et des mises à jour nécessaires des systèmes informatiques et logiciels.

Grandes entreprises (plus de 250 salariés)

✔	Identification proactive et la suppression des logiciels malveillants, comme les antivirus ou l'EDR (solution de détection et de blocage des menaces sur les terminaux).
✔	Agréger et stocker de façon centralisée les données relatives aux événements de sécurité.
✔	Assurer, autoriser et appliquer le chiffrement des données stockées sur les appareils portables comme les téléphones et ordinateurs.
✔	Contrôler les communications chiffrées entrantes et sortantes de vos systèmes, par exemple pour bloquer un contenu potentiellement nuisible.
✔	Veiller à ce que chaque utilisateur ait un identifiant et un nom d'utilisateur cohérent et unique dans vos systèmes informatiques.

Dépenses moyennes de cybersécurité (en euros)
Selon le nombre de salariés

	1-9	10–49	50–249	250–999	1 000-plus
2023	7 452	44 068	135 884	848 424	4 592 732
2022	4 232	32 476	55 384	863 696	5 060 000
2021	1 840	18 400	54 556	327 336	2 300 000

Le lien avec les budgets alloués à la cybersécurité
Sans surprise, le facteur financier est également considéré comme important. L'augmentation des budgets alloués à la gestion des cyber-risques est l'une des raisons majeures permettant d'être plus serein face à la cyber-menace. Environ 45% des grandes entreprises affirmant que leur exposition aux cyber-attaques a diminué, l'expliquent par l'augmentation de leurs budgets et de meilleures solutions de réduction des risques. Ce chiffre n'était que de 36% l'an dernier. Cela soulève une question évidente: y a-t-il un lien entre le volume des budgets et la réduction des cyber-attaques? On serait tenté de répondre par l'affirmative cette année.

Comme mentionné plus tôt, les petites entreprises ont réussi à réduire le coût médian des cyber-attaques en dépit de leur plus grande intensité. Dans le même temps, les petites entreprises de 1-9, 10-49 et 50-249 salariés ont sensiblement augmenté leurs dépenses moyennes, de 77%, 36% et 145% respectivement. En deux ans, les entreprises de moins de dix salariés ont réellement quadruplé leurs dépenses en matière de cybersécurité. Comparativement, de l'autre côté du spectre, dans les entreprises de 250 salariés ou plus, les dépenses médianes ont été réduites cette année. Pourtant, l'impact financier des attaques a continué de croître.

Si l'on observe les données par pays, les entreprises belges ont dépensé moins en matière de cybersécurité que n'importe quel autre groupe, 55 986€ en moyenne contre 132 480€ l'année précédente. Les pertes moyennes liées aux cyber-attaques ont quasiment doublé et 62% des participants ont fait état de coûts de 9 200€ ou plus (presque deux fois la moyenne du panel d'entreprises étudiées). Par contraste, les entreprises allemandes ont été les plus dépensières, avec une médiane de 196 880€ et ont vu leurs pertes chuter, passant de 19 320€ à 14 766€. Qu'on se le dise, elles ont été en moyenne les plus dépensières sur les trois dernières années. Mais elles constituent le seul groupe à avoir enregistré une réduction sensible des coûts liés aux attaques sur cette période. Une chose est sûre, les entreprises cyber-expertes de notre étude ont tendance à allouer une plus grande partie de leur budget informatique à la cybersécurité: 25% contre 23% en moyenne, et moins de 22% pour les novices.

L'argument des ressources
L'argent n'est qu'une donnée de l'équation. Le nombre de personnes consacrées à la lutte contre la cyber-menace est également important. Les entreprises belges, irlandaises et américaines sont en tête en la matière avec en moyenne 97, 95 et 84 personnes dans l'équipe en charge la cybersécurité. Ces chiffres sont très supérieurs au reste du panel. Derrière ces moyennes, se trouve une statistique intéressante: 15% des entreprises américaines et britanniques n'ont pas de responsable de la cybersécurité. En comparaison, seules 8% des entreprises allemandes sont dans ce cas. Les États-Unis et le Royaume-Uni sont pourtant deux des trois pays les plus touchés par des attaques dans notre panel de cette année.

La présence d'un responsable de la cybersécurité est l'un des facteurs clés de différenciation entre les expertes et le reste. Seules 4% des entreprises qualifiées d'expertes n'avaient pas de responsable de la cybersécurité cette année. Ce chiffre contraste avec plus d'un quart (27%) des novices. La plupart d'entre elles sont de petites entreprises pour lesquelles il s'agit clairement d'une problématique de ressources. Plus d'un tiers (34%) des entreprises de moins de dix salariés ont déclaré qu'elles n'avaient désigné aucun responsable de la cybersécurité. Cette proportion tombe à 9% dans les entreprises de 10 à 49 salariés. Pourtant, et c'est peut-être ce qui est le plus inquiétant, les petites entreprises sont également en retard dans les domaines à moindre coût telle que la mise en place de mesures de sécurité supplémentaires ou la formation des salariés à la suite d'une attaque.

L'importance du transfert de risques

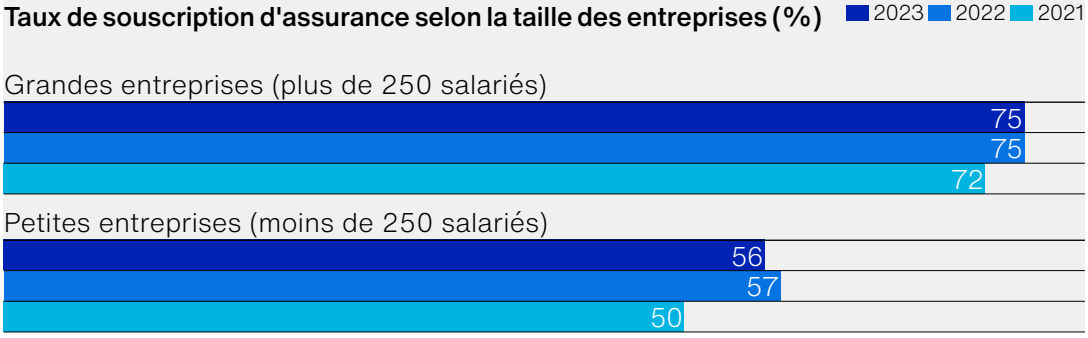
L'une des grandes différences entre les expertes et les novices de notre panel est la mise en œuvre de mesures positives pour répondre aux attaques, comme l'amélioration des processus ou procédures (44% des expertes ont indiqué avoir mis en place de telles mesures l'an dernier contre seulement 30% des novices). L'une des mesures principales consiste à transférer le risque en souscrivant une cyber-assurance.

Il y a une relation étroite entre l'expérience d'une attaque et la décision de s'assurer. Près de trois quarts des entreprises attaquées (73%) disposent soit d'une police de cyber-assurance dédiée soit d'une couverture contre les cyber-risques dans le cadre d'une autre police. En comparaison, à peine plus de la moitié (52%) des entreprises qui n'ont pas été attaquées sont couvertes. Les entreprises ayant souscrit une cyber-assurance sont également moins enclines à prendre d'autres mesures pour améliorer la sécurité à la suite d'une attaque: 36% contre 29% des entreprises non-assurées.

Près de 42% des expertes indiquent qu'elles disposent d'une police de cyber-assurance dédiée, et 36% bénéficient d'une couverture contre les cyber-risques dans le cadre d'une autre police. Par contraste, les chiffres équivalents pour les novices sont de 24% et 26% seulement. Plus d'une entreprise novice sur cinq déclare ne pas avoir l'intention de souscrire une cyber-assurance. Les petites entreprises (moins de 250 salariés) ne sont pas au niveau des grandes en ce qui concerne la souscription d'une assurance.

Les motifs de souscription d'une police dédiée sont variés, mais chez les expertes, la raison principale est de démontrer aux clients et aux prospects que l'entreprise est attentive à la protection contre les cyber-risques. Près de la moitié des expertes (46%) évoquent cette raison, soit deux fois plus que la moyenne.

Taux de souscription d'assurance selon la taille des entreprises (%)



Évaluation globale de la cyber-maturité 2023

Notre outil de modélisation des capacités de gestion des cyber-risques mesure l'alignement des entreprises sur les meilleures pratiques dans six domaines selon trois axes fonctionnels. Le système de notation attribue des notes de un à cinq, une note supérieure à quatre qualifiant l'entreprise de 'cyber-experte'. Entre 2.51 et 3.9, l'entreprise se qualifie de 'cyber-intermédiaire'. En dessous de 2.5, les entreprises sont considérées comme 'cyber-novices'.

	Humain	Processus	Technologie	Moyenne
Gestion de la résilience de l'entreprise	2.90	2.93	3.00	2.94
Gestion de la cryptographie et des clés	2.78	2.73	2.86	2.79
Gestion des identifiants et accès	2.99	2.81	2.85	2.87
Gestion de la sécurité et des événements	2.86	2.78	2.69	2.85
Gestion des menaces et vulnérabilités	2.89	2.91	3.28	3.03
Gestion de la confiance	2.93	2.98	3.02	2.98
En moyenne	2.89	2.85	2.94	2.90

Étude de cas
Le rôle crucial de l'assurance

L'arrêt total
Ce n'est qu'une fois que vous avez été frappé de plein fouet par une cyber-attaque que vous appréciez pleinement l'importance de la cyber-assurance. Les propriétaires de Schäfer Trennwandsysteme GmbH, une entreprise de taille moyenne située dans le pittoresque Westerwald, l'ont bien compris, lorsque leurs systèmes informatiques ont tous arrêté de fonctionner un jeudi matin.

Alors que tout était paralysé, seul un fichier lisible présent dans chaque dossier indiquait que leurs fichiers de données étaient désormais chiffrés.La direction était en état de choc. Rien ne permettait d'imaginer qu'ils étaient dans le collimateur de pirates informatiques. L'entreprise n'avait ni brevets, ni données secrètes. Mais heureusement, elle avait souscrit une police de cyber-assurance auprès d'Hiscox*.

La suite
Le partenaire en résolution d'incident d'Hiscox est intervenu avec deux gestionnaires de crise. Avec l'aide de l'équipe de gestion de crise, il a permis aux processus de l'entreprise de se remettre en fonctionnement rapidement.

En outre, le partenaire a fait appel à des experts informatiques qui ont travaillé pour rechercher comment l'attaquant s'était introduit: Où se trouvait le logiciel malveillant? L'équipe d'intervention s'est plongée dans les systèmes de l'entreprise et a pu comprendre ce qui s'était passé grâce aux fichiers de journalisation.

*Cet exemple de sinistre est basé sur l'expérience d'un assuré d'Hiscox. Schäfer Trennwandsysteme GmbH ne fait pas partie des données d'étude du Rapport Hiscox sur la gestion des cyber-risques.

Les obligations légales
La protection des données était une problématique, avec une impossibilité de savoir si des données personnelles avaient fuité ou non.

Hiscox a mis l'entreprise en contact avec un cabinet d'avocats qui a travaillé avec le délégué à la protection des données externe de l'entreprise, lequel a ensuite remis un rapport au délégué à la protection des données du Land de Rhénanie-Palatinat.

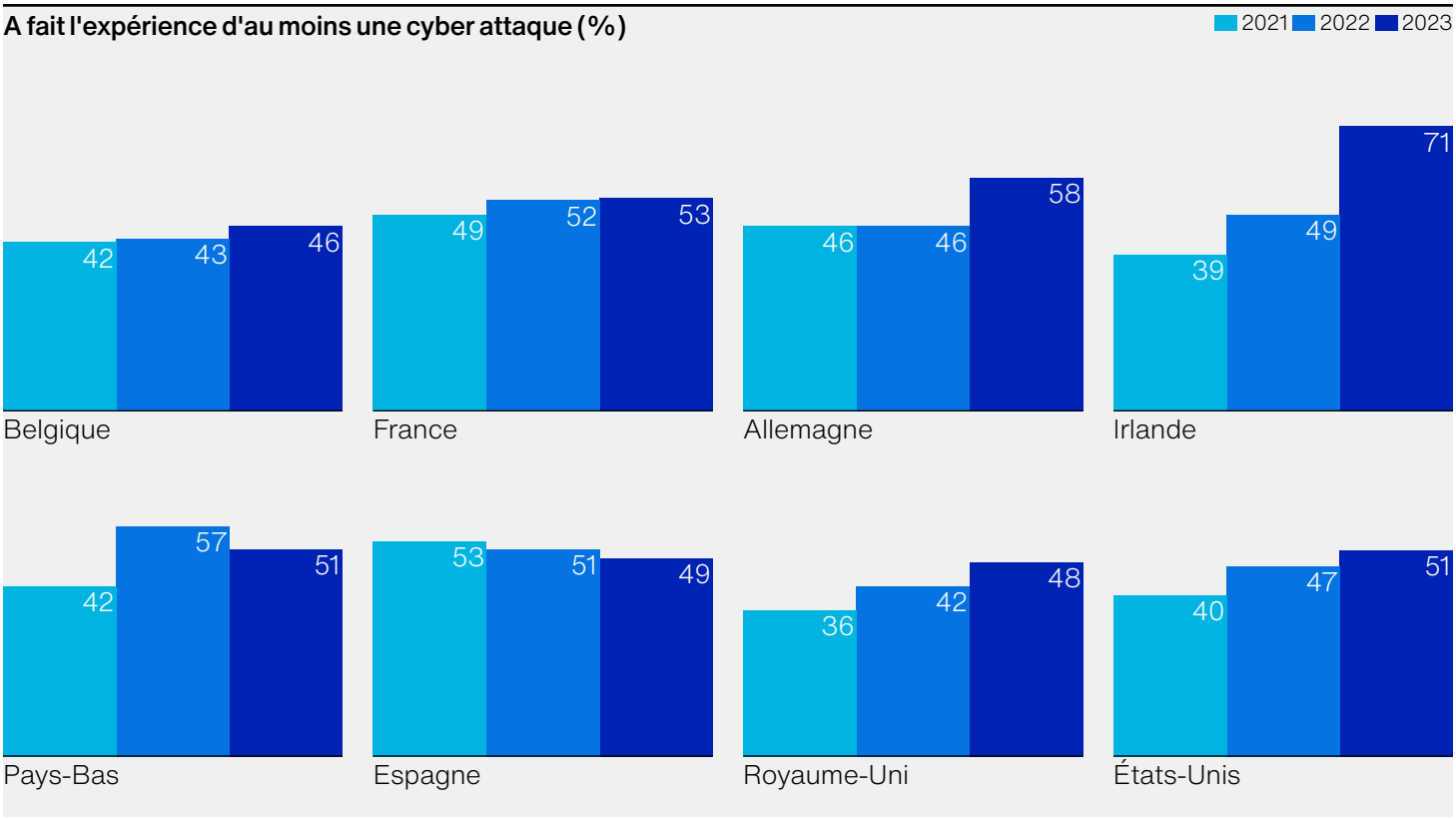
La législation imposait d'y procéder, mais "*c'était appréciable d'avoir un partenaire compétent à nos côtés*", déclara Martin Schäfer, DG de Schäfer Trennwandsysteme GmbH.

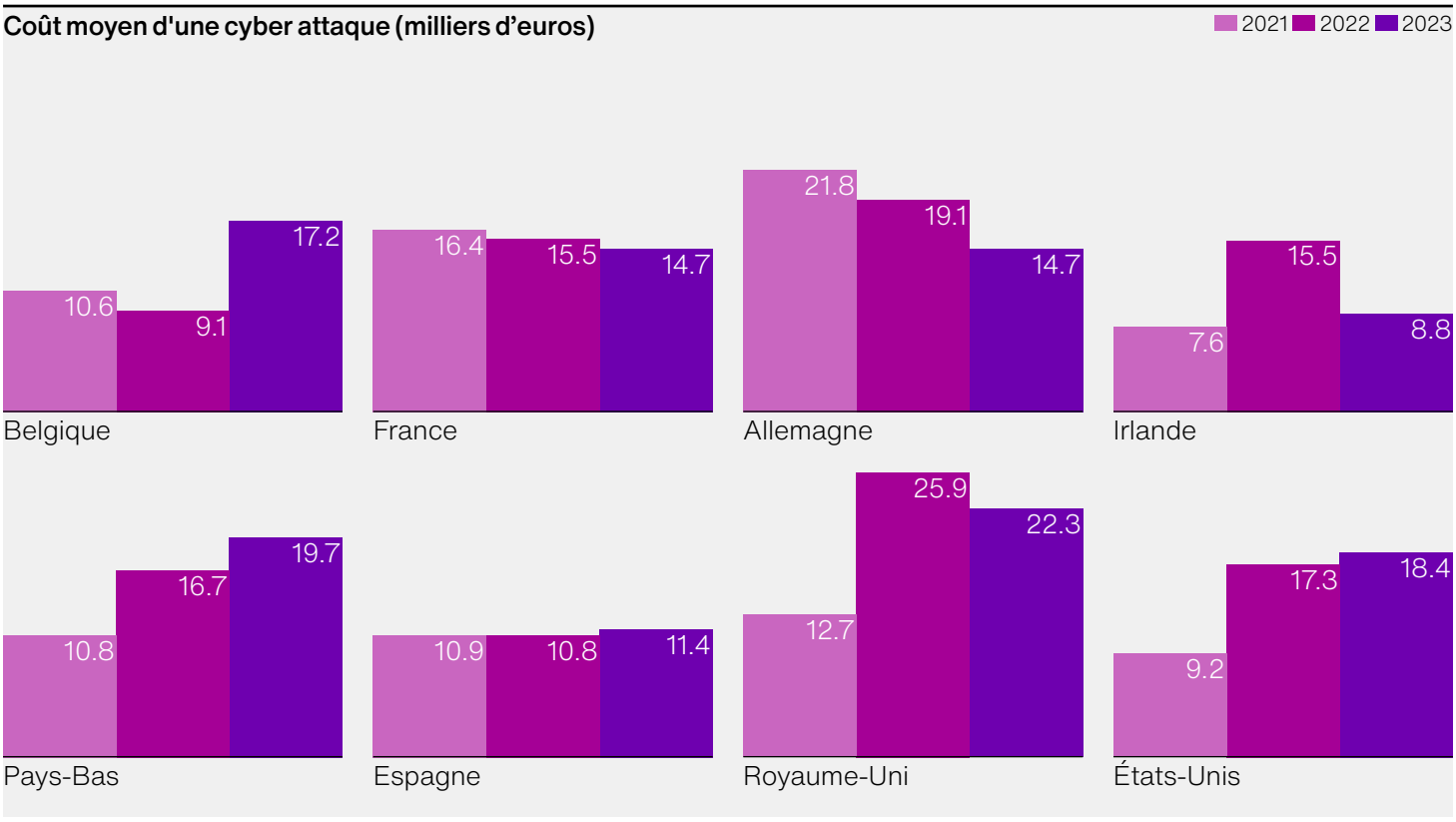
Les relations publiques
La communication était également importante. Hiscox a dépêché un expert en communications. Il était clair que cet incident allait s'ébruiter. Les communications devaient être gérées activement. C'est pourquoi l'entreprise communiqua assez rapidement, ce qui a permis d'instaurer un climat de confiance et de compréhension parmi les salariés, les fournisseurs et, avant tout, les clients.

Au départ, l'entreprise pensait que toutes les données avaient disparu. Mais avec l'aide de l'équipe d'intervention, l'entreprise en récupéra une grande partie en quatre à cinq jours.

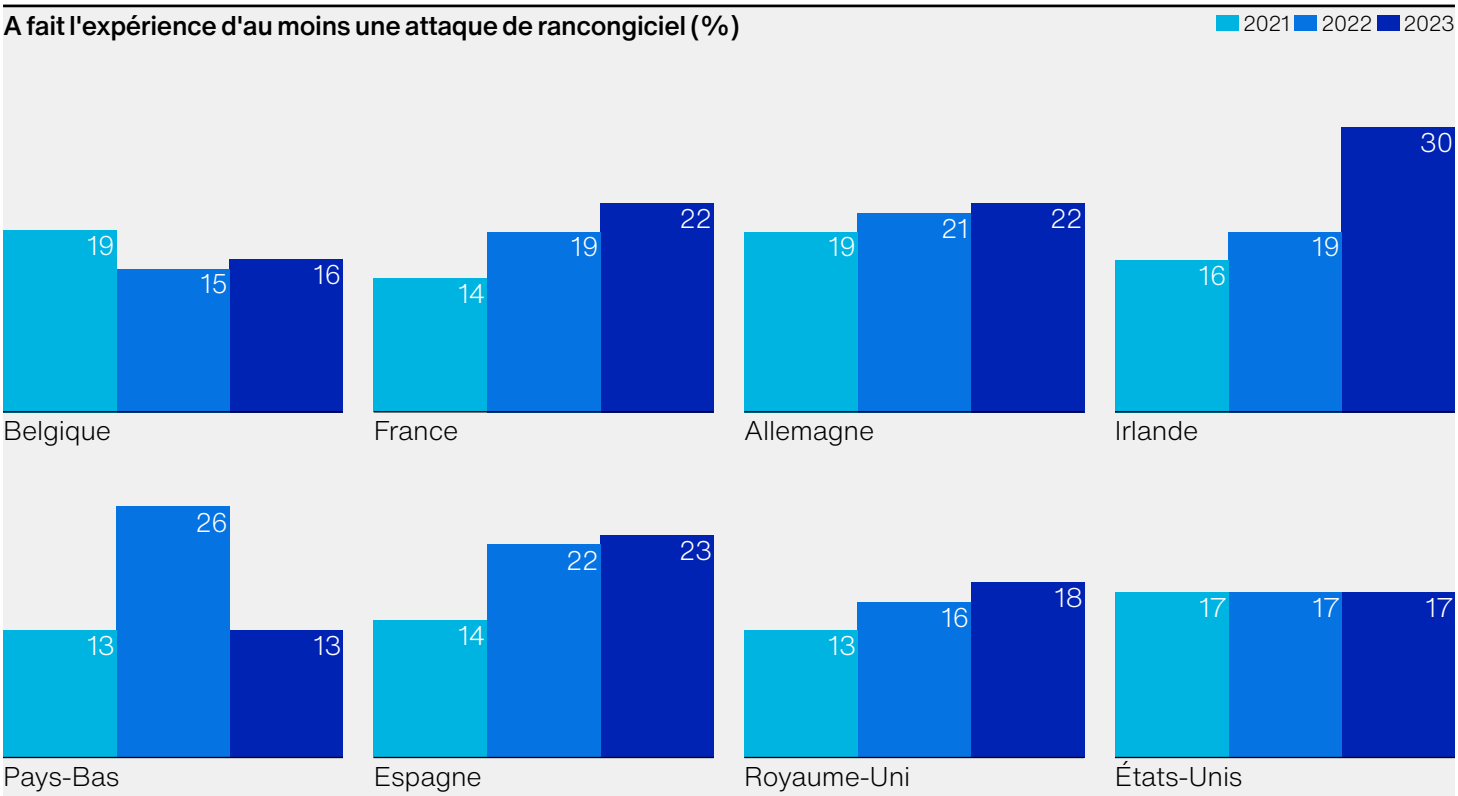
L'attaque a également démontré la valeur de l'assurance. Les prestataires d'Hiscox ont aidé les clients rapidement et de façon concrète dans les domaines de la gestion de crise, de l'expertise informatique et de la protection des données. "*Quand on regarde en arrière, c'était appréciable d'avoir de nombreux conseillers avisés à nos côtés.*" conclut un directeur.

Comparaison par pays

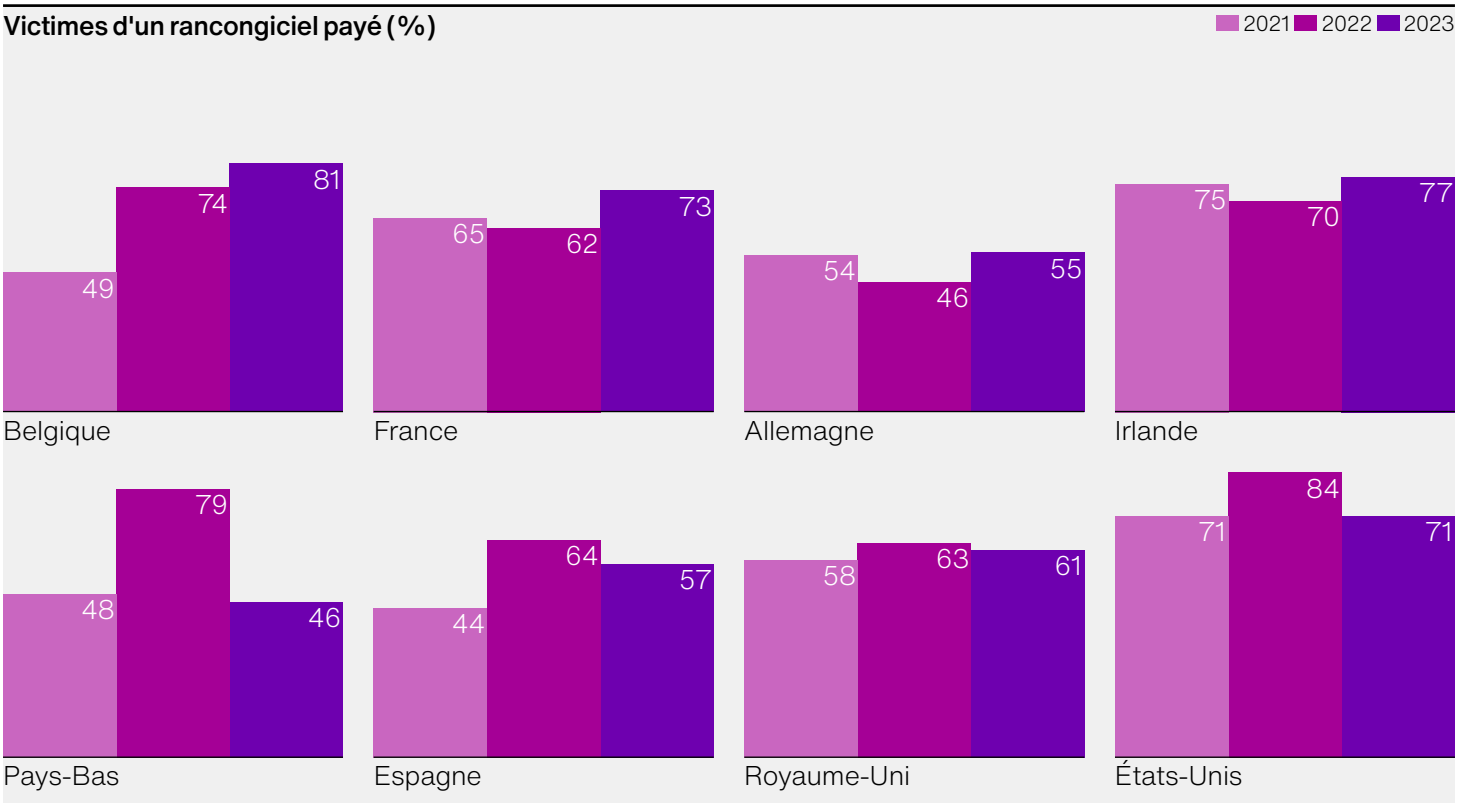




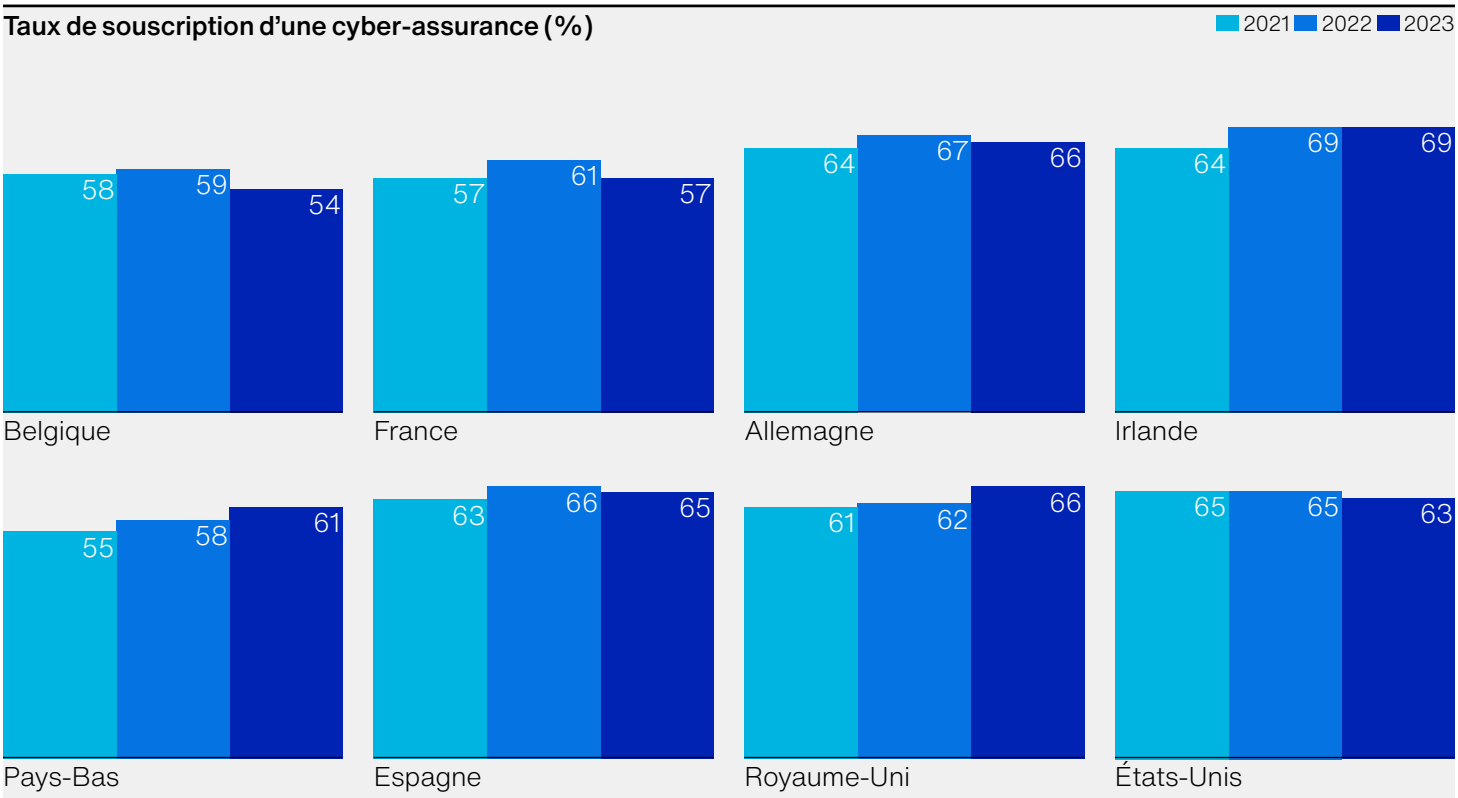
A fait l'expérience d'au moins une attaque de rancongiciel (%)



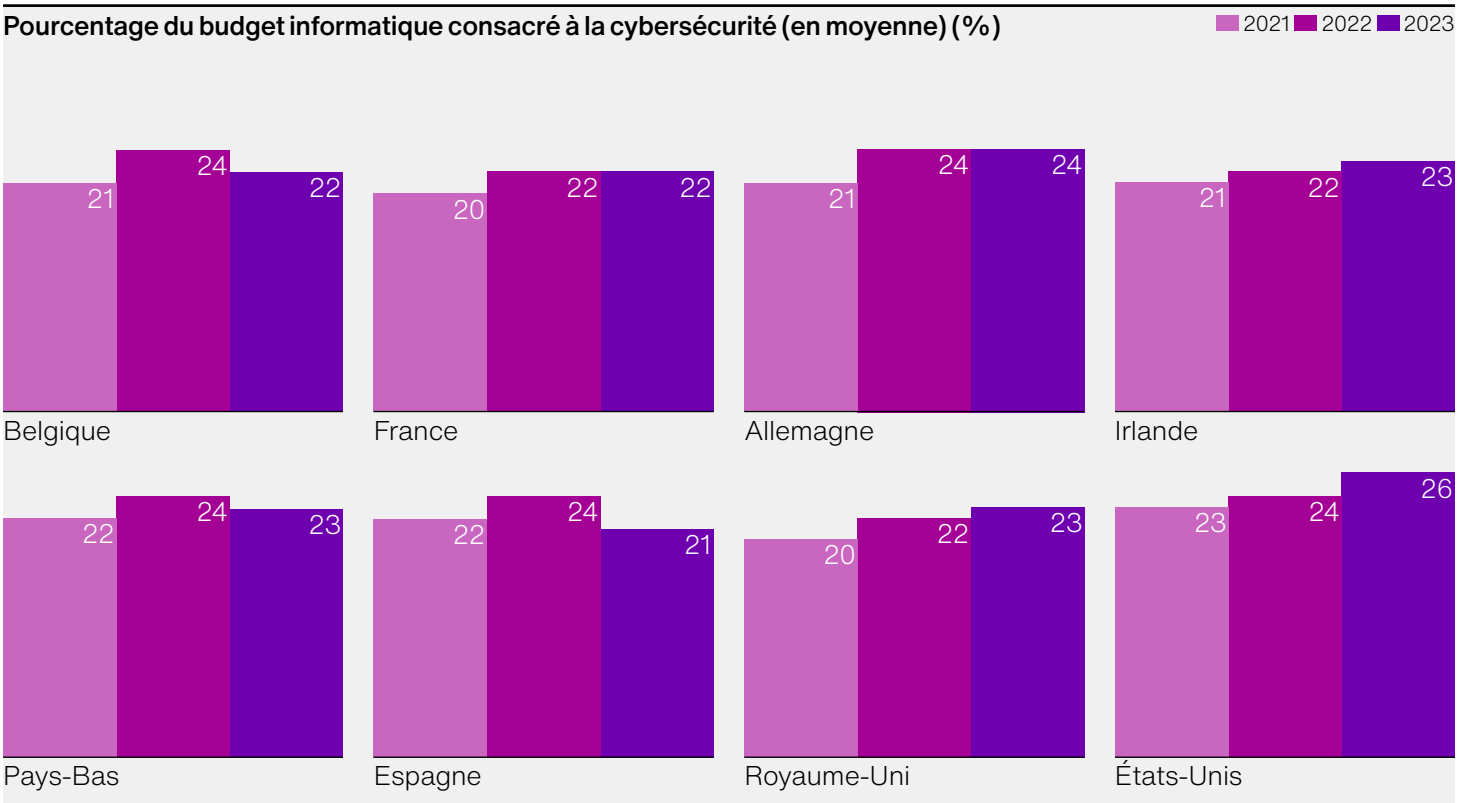
Victimes d'un rancongiciel payé (%)



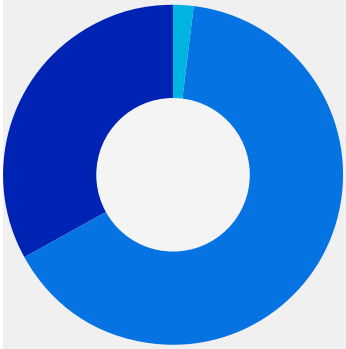
Taux de souscription d'une cyber-assurance (%)



Pourcentage du budget informatique consacré à la cybersécurité (en moyenne) (%)



Belgique

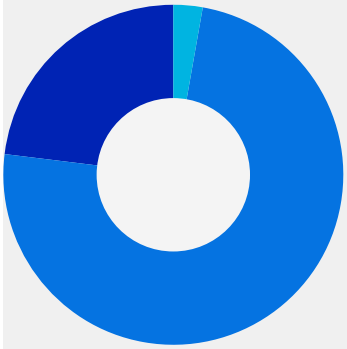


Cyber maturité	%
Expertes	2
Intermédiaires	65
Novices	33

Seul pays du groupe d'étude où le cyber n'est pas l'un des trois principaux risques pour les entreprises.

Les dépenses consacrées à la formation cyber des employés et au changement de culture ont presque doublé en trois ans.

France

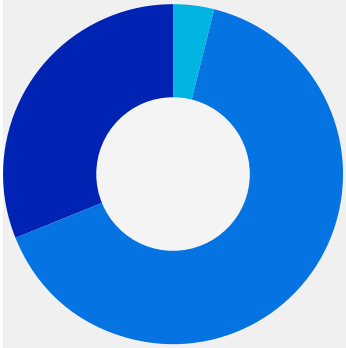


Cyber maturité	%
Expertes	3
Intermédiaires	74
Novices	23

41% ont été victimes d'une fraude par détournement de paiement à la suite d'une cyberattaque.

Principale raison de souscrire une assurance: être concerné par la sécurité des données.

Allemagne

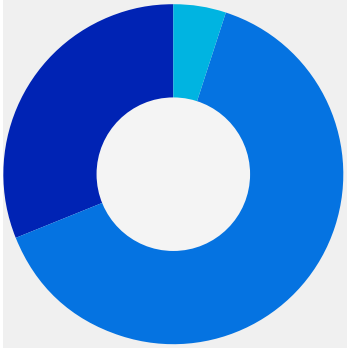


Cyber maturité	%
Expertes	4
Intermédiaires	65
Novices	31

Augmentation de 26% des cas de cyberattaques comparé à l'année dernière.

Hausse de 40% de la fraude par détournement de paiement suite à une cyberattaque.

Irlande

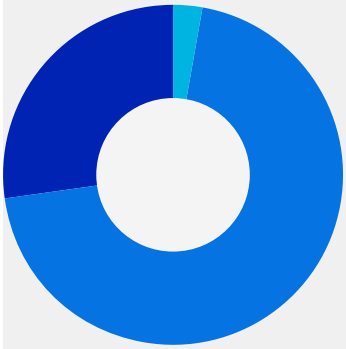


Cyber maturité	%
Expertes	5
Intermédiaires	64
Novices	31

69% des répondants irlandais interrogées ont souscrit une cyber-assurance, le taux le plus élevé de l'étude.

Augmentation de 50% des demandes d'argent après le paiement d'une rançon.

Pays-Bas

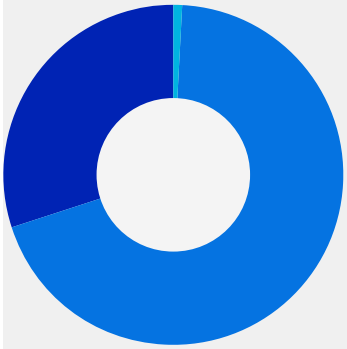


Cyber maturité	%
Expertes	3
Intermédiaires	70
Novices	27

Seul pays de l'étude à avoir augmenté son score de préparation cyber.

Diminution de 50% des rançongiciel par rapport à l'année dernière.

Espagne

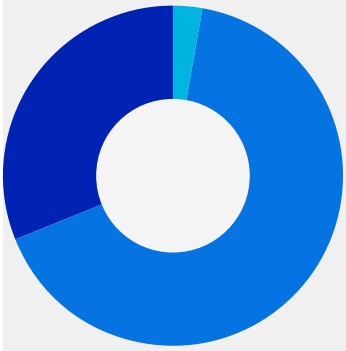


Cyber maturité	%
Expertes	1
Intermédiaires	69
Novices	30

Le point d'entrée le plus courant est le serveur Cloud d'entreprise.

L'augmentation des budgets cyber est selon 25% des repondants la raison de la chute des risques cyber.

Royaume-Uni

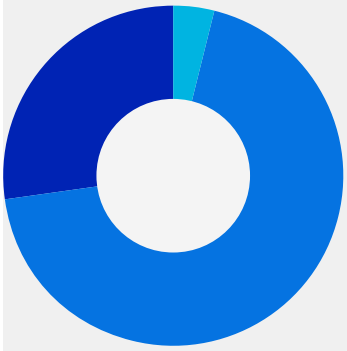


Cyber maturité	%
Expertes	3
Intermédiaires	66
Novices	31

Près de trois quarts des entreprises pensent que leur marque sera endommagée si les données des clients ne sont pas traitées en toute sécurité.

Le Royaume-Uni est le second pays (48%) le moins touché par une cyberattaque.

États-Unis



Cyber maturité	%
Expertes	4
Intermédiaires	69
Novices	27

Plus d'une entreprise sur cinq voit sa solvabilité menacée après une cyberattaque.

La première raison de gérer proactivement le risque cyber: réassurer les clients.

Méthodologie

Au total, 5 005 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 l'Espagne et plus de 200 pour la Belgique, la République d'Irlande et les Pays-Bas). Les participants ont rempli le questionnaire en ligne entre le lundi 9 janvier 2023 et le jeudi 2 février 2023.

Le profil complet des participants est détaillé ci-dessous.

Répondants

Nombre de salariés	%	Niveau	%
1–9	26	Cadre de niveau C	29
10–49	19	Vice-président	24
50–249	15	Directeur	32
250–999	15	Manager	15
1 000-plus	25		

Secteur	%	Département	%
Services aux entreprises	7	Haute direction	9
Construction	8	E-Commerce	4
Énergie	4	Finance	9
Services financiers	10	Direction juridique	4
Agro-alimentaire	4	Ressources humaines	7
Administration et organismes à but non lucratif	5	Informatique et technologie	18
Fabrication	8	Marketing et communications	5
Pharmacie et santé	9	Opérations	10
Services professionnels	8	Chef d'entreprise	14
Dommages aux biens	3	Achats	4
Commerce de gros et de détail	8	Gestion de produit	5
Technologie, médias et télécommunications	18	Gestion des risques	5
Transport et distribution	5	Ventes	5
Voyages et loisirs	4		

Les faits du sinistre d'un client d'Hiscox ont été utilisés en page 15.

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 déclarations de sinistre 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.

Notre nouvelle génération de produits d'assurance comprend un ensemble d'outils et de services
Au-delà du classique transfert de risque, la cyber-assurance d'Hiscox 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 aux salariés de l'ensemble des petites et moyennes entreprises qu'elle assure, partout dans le monde, en collaborant avec divers prestataires.

Nous partageons ainsi notre expertise et développons les consciences
Nous avons développé des outils gratuits, comme notre modélisation d'auto-évaluation de la cyber-maturité pour permettre aux entreprises de comprendre leurs forces et faiblesses en matière de cybersécurité. Grâce à notre outil de modélisation de la maturité, vous pouvez comparer la performance de votre entreprise à celle de plus de 16 000 autres entreprises.

Nous vous tenons informés sur l'univers de la cybersécurité
Pour la septième année consécutive, nous avons élaboré le Rapport Hiscox sur la gestion des cyber-risques. Chaque année, ce rapport dresse un panorama rapide des capacités de gestion des cyber-risques des entreprises et propose également un tableau des meilleures pratiques pour lutter contre une menace en perpétuelle évolution. Sur la base d'un échantillon représentatif d'entreprises de huit pays classés par taille et par secteur, il reflète l'expérience directe des acteurs se trouvant en première ligne dans la lutte contre la cybercriminalité.

Quel est votre score de maturité Cyber?
Notre modèle de cybermaturité est un outil gratuit et interactif qui aide à l'évaluation de votre entreprise en termes de cybersécurité grâce à des outils sécurisés acceptés par l'ensemble du secteur.

www.hiscoxgroup.com/cyber-maturity

Hiscox Assurances
38 avenue de l'Opéra
75002 Paris France

+33 (0)1 53 21 82 82
info.france@hiscox.com
hiscox.fr

22594 10/23