
**RAPPORT 2025
SUR LA GESTION DES RISQUES-CYBER**

Les PME agissent contre
les cyber-menaces
actuelles et futures



Sommaire

- 03 Introduction
- 04 Résumé
- 05 Principales conclusions
- 06 État des attaques
- 09 Les entreprises agissent
- 10 Cyber-résilience
- 11 L'IA et les menaces futures
- 13 Divulgations obligatoires
- 14 Comparaison par pays
- 15 Conseils aux PME en matière de cybersécurité

Le Rapport Hiscox sur la gestion des risques-cyber repose sur une étude menée auprès de 5 750 entreprises par Wakefield Research, qui a interrogé les personnes en charge de la cybersécurité au sein de leur entreprise, à savoir les chefs d'entreprise, dirigeants ou associés pour les entreprises de moins de 50 salariés, et les DSI, RSSI, directeurs de la sécurité ou directeurs informatique pour les sociétés de 50-249 salariés.

L'étude a été réalisée entre le 29 juillet et le 8 août 2025 au moyen d'une enquête en ligne proposée par email. Les participants se répartissent géographiquement de la façon suivante : 1 000 participants aux États-Unis, au Royaume-Uni, en France, en Allemagne et en Espagne, respectivement, 500 participants en Irlande et 250 au Portugal.

Ces données d'étude constituent un échantillon représentatif d'entreprises assurées et non assurées, qui ont déclaré ou non un sinistre après un incident. Elles ne sont pas nécessairement représentatives de nos propres chiffres en matière de déclaration de sinistres, ni mêmes de ceux du secteur de l'assurance dans son ensemble.

Introduction



Eddie Lamb
Directeur de la
Cybersécurité Monde
Hiscox

L'essor du commerce électronique a ouvert un monde de possibilités aux petites entreprises, leur donnant les moyens d'innover, d'accéder à de nouveaux marchés et de jouer un rôle de plus en plus important dans l'économie mondiale. La plus puissante de ces évolutions récentes est sans doute l'intelligence artificielle (IA), qui permet aux PME de développer des outils et des ressources auxquelles elles n'auraient pas pu avoir accès auparavant.

Mais ces opportunités présentent également des défis. À mesure que les entreprises adoptent les nouvelles technologies, elles doivent également naviguer dans un environnement où les cyber-menaces en constante mutation peuvent compromettre leurs chances de succès de bien des manières. Cette neuvième édition du Rapport Hiscox sur la gestion des risques-cyber est conçue pour aider les petites et moyennes entreprises (PME) à mieux comprendre les risques qu'elles rencontrent dans notre monde dominé par la technologie qui se transforme rapidement, ainsi que les mesures qu'elles peuvent mettre en place pour minimiser leur exposition à ces risques. Ayant moi-même créé et développé ma propre petite entreprise, c'est un sujet qui me tient particulièrement à cœur.

Nous avons interrogé 5 750 entreprises au Royaume-Uni, aux États-Unis, en France, en Allemagne, en Espagne, en Irlande et au Portugal pour comprendre l'impact que les cyber-attaques ont sur leur entreprise, et les risques les plus courants auxquels elles sont exposées. Plus de la moitié de ces entreprises nous ont déclaré avoir subi une cyber-attaque au cours des 12 derniers mois, et un tiers d'entre elles ont dû verser une amende réglementaire en raison d'une fuite de données, dont le montant a eu une incidence sur leur santé financière.

Cela souligne l'importance pour les PME d'adopter les mesures nécessaires pour protéger les données de leurs clients, en conformité avec les exigences réglementaires, telles que le Règlement général sur la protection des données (RGPD) en Europe ou les lois sur la protection des consommateurs appliquées aux États-Unis par la *Federal Trade Commission* (Commission fédérale du commerce, FTC).

Les attaques par ransomware demeurent une menace particulièrement persistante pour de nombreuses entreprises. Les PME que nous avons interrogées nous ont fait part de leur expérience d'attaques par ransomware, certaines ayant payé à plusieurs reprises afin de protéger leurs données sensibles, quand bien même le versement d'une rançon ne garantit pas la récupération des données. Parmi les PME qui ont versé une rançon, trois sur cinq ont rapporté avoir récupéré l'ensemble

de leurs données, mais pour près d'un tiers d'entre elles, les pirates ont continué à exiger davantage d'argent.

Notre rapport s'intéresse par ailleurs à l'impact de l'IA sur les petites entreprises, pour lesquelles elle peut s'avérer à la fois bénéfique et préjudiciable. Si l'IA offre de nouvelles possibilités et de nouveaux outils pour détecter les menaces et y répondre, elle introduit également de nouvelles vulnérabilités, créant des points d'entrée non protégés et exposant des failles dans la sécurité des données, que les pirates peuvent exploiter de la même manière qu'ils le faisaient il y a dix ou quinze ans. L'IA étant de plus en plus intégrée dans nos activités professionnelles quotidiennes, nos équipes spécialisées chez Hiscox s'attachent à définir les risques associés, à mettre en place des couvertures et à développer les connaissances et les formations nécessaires pour soutenir les dirigeants de petites entreprises à travers le monde.

Et pourtant, même si les risques-cyber sont en perpétuelle mutation, les PME y font face de manière proactive et pragmatique. La grande majorité des PME (94 %) prévoient d'augmenter leurs investissements dans la cybersécurité et la protection des données au cours des 12 prochains mois. Cela comprend l'embauche de spécialistes de la cybersécurité, l'actualisation des programmes de formations, l'analyse régulière des vulnérabilités et l'évaluation des risques liés à leur chaîne d'approvisionnement.

Chez Hiscox, nous sommes fiers d'accompagner ces entreprises, en leur offrant non seulement une couverture d'assurance, mais également des réflexions, une expertise et un appui. Nous comptons plus de vingt années d'expérience dans la protection des données et la cyber-assurance et fournissons une cyber-assurance à plus de 80 000 clients dans le monde, aidant ainsi quotidiennement des entreprises à se rétablir après un incident, à renforcer leurs défenses et à bâtir une résilience de long-terme.

En matière de cybersécurité et de résilience des entreprises, nous ne pouvons pas nous reposer sur nos lauriers et considérer notre travail comme achevé. Au contraire, nous devons maintenir notre détermination collective à combattre la cybercriminalité et faire une priorité de la gestion continue des risques-cyber.

Nous espérons que ce rapport incitera davantage d'entreprises à évaluer leurs capacités de gestion des risques-cyber à l'aide de notre outil de modélisation de la cyber-maturité, qu'il nourrira des discussions et qu'il contribuera à la mise en place de stratégies de cybersécurité encore plus élaborées.

Résumé

83 %

des entreprises ont fait état d'une amélioration de leur cyber-résilience

Personne n'a jamais dit que garantir la sécurité des PME (petites et moyennes entreprises) était une tâche aisée. Cette catégorie majeure d'entreprises représente 50 % de l'économie mondiale, et leurs dirigeants doivent relever un grand nombre de défis, en jonglant souvent avec des responsabilités transversales : opérations, ventes, marketing, image de marque, technologie, RH, etc.

L'un de leurs rôles les plus délicats est celui d'évaluateur des risques, qui requiert de leur part une compréhension de l'évolution constante des menaces auxquelles leur entreprise est confrontée. La complexité de ces menaces ne cesse de s'accroître à mesure que les avancées technologiques, telles que l'intelligence artificielle agentique, transforment le monde qui nous entoure.

Dans cette neuvième édition du rapport annuel d'Hiscox sur la gestion des risques-cyber, nous nous penchons sur l'impact de ces risques numériques en mutation rapide, leur signification et les mesures que les petites entreprises peuvent mettre en place pour limiter leur exposition.

Presque toutes les PME (94 %) prévoient d'augmenter leurs investissements dans la cybersécurité et la protection des données au cours des 12 prochains mois, en actualisant la formation de leurs salariés en matière de cybersécurité (70 %) et en embauchant du personnel supplémentaire pour renforcer leur cyber-résilience (60 %).

Le rapport de cette année met en lumière une détermination globale des PME à investir non seulement dans des logiciels et formations, mais également à rester vigilantes en évaluant régulièrement leurs risques et vulnérabilités, et en souscrivant des polices de cyber-assurance pour les protéger en cas de problème.

Grâce à cette approche proactive, les entreprises affichent une confiance accrue, et 83 % d'entre elles font état d'une amélioration

de leur cyber-résilience au cours des 12 derniers mois.

La complexité des risques numériques ne cesse de croître. Les entreprises sont confrontées au dilemme de savoir comment gérer les conséquences des attaques par ransomware, y compris au regard des évolutions réglementaires, comme l'illustre une nouvelle loi australienne qui oblige les entreprises à divulguer le montant des rançons versées. D'autres pays pourraient adopter une réglementation semblable. Une grande majorité des entreprises (71 %) estiment que de telles divulgations devraient être obligatoires.

Malgré ce soutien, les opinions divergent sur la question de savoir si ces exigences devraient s'appliquer aux entreprises privées. 53 % des participants considèrent que les entreprises privées ne devraient pas être tenues de divulguer publiquement le montant des rançons qu'elles ont versées.

En France, depuis la loi LOPMI du 24/01/2023, les victimes de ransomware (rançongiciel) ont l'obligation de déposer plainte dans un délai de 48h après le versement de la rançon, afin de pouvoir mobiliser les garanties du contrat d'assurance.

Il n'a jamais été aussi difficile de mener ses affaires en raison des menaces en ligne (60 % des personnes interrogées considèrent que l'ingénierie sociale via l'IA, les logiciels malveillants créés par l'IA et les attaques par phishing constitueront les principales menaces émergentes liées à l'intelligence artificielle dans les cinq prochaines années). Les experts en cybersécurité et les décideurs travaillent d'arrache-pied pour protéger leur entreprise, leurs salariés et leurs clients.

Au cours des 12 derniers mois, 59 % des PME ont subi une cyber-attaque, mais au lieu de rester les bras croisés, elles investissent, forment leurs salariés et mettent à jour leurs systèmes pour s'adapter à l'environnement en constante évolution.

Principales conclusions

59 %

des participants ont subi une cyber-attaque au cours des 12 derniers mois.



33 %

ont dû verser une amende importante après un cyber-incident.



94 %

augmentent leurs investissements dans la cybersécurité et la protection des données.



60 %

recrutent du personnel supplémentaire pour renforcer leur cyber-résilience.



88 %

effectuent une évaluation trimestrielle des risques liés à leurs fournisseurs et partenaires.



91 %

réalisent une analyse de leur cyber-vulnérabilité au moins une fois par trimestre.



27 %

ont subi une attaque par ransomware au cours des 12 derniers mois.



71 %

sont favorables à une obligation de divulgation des montants de rançon versés.



État des attaques

60 %

des entreprises qui ont versé une rançon ont récupéré l'intégralité ou une partie de leurs données.

Les entreprises qui ont subi une cyber-attaque l'année passée n'ont pas été confrontées à un incident isolé, elles ont souvent été touchées à plusieurs reprises. Près de trois entreprises sur cinq (59 %) ont enregistré au moins une cyber-attaque au cours des 12 derniers mois.

Parmi celles-ci, les grandes entreprises ou celles dont le chiffre d'affaires est plus élevé ont été plus nombreuses à faire face de multiples incidents. À titre d'exemple, les entreprises victimes d'une attaque l'an dernier, qui réalisent un chiffre d'affaires annuel de 10 millions \$ ou plus et celles dont le chiffre d'affaires est compris entre 1 million \$ et 10 millions \$, ont subi en moyenne davantage d'attaques (environ six) que celles dont le chiffre d'affaires est inférieur à 1 million \$ (environ quatre).

De même, parmi les entreprises qui ont subi une attaque, les entreprises de 50-249 salariés ont enregistré en moyenne sept attaques l'an dernier contre environ cinq attaques en moyenne pour les entreprises de 11-49 salariés et quatre attaques en moyenne pour les entreprises de 1-10 salariés.

Parmi les entreprises ayant rapporté des incidents, le nombre moyen d'attaques varie d'environ trois attaques dans les secteurs tels que la chimie, l'immobilier et les médias à environ huit attaques pour les organismes à but non lucratif. Une cyber-attaque réussie peut infliger des dommages immédiats et importants : perturbation des opérations, augmentation des coûts et exposition des données sensibles.

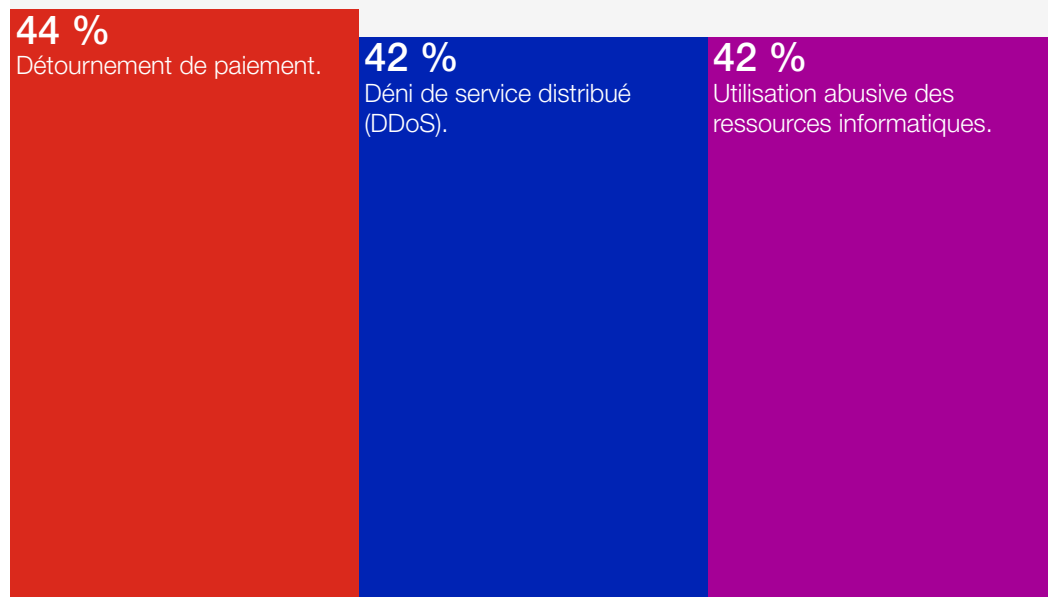
Les entreprises constatent que les pirates exploitent les vulnérabilités de leur propre matériel informatique et celles de leurs partenaires. Les appareils connectés appartenant aux entreprises - l'Internet des objets (IdO) - ont constitué le point d'entrée le plus courant des cyber-attaques l'an dernier (33 %), suivi des vulnérabilités de la chaîne d'approvisionnement, telles que les sites web des fournisseurs (28 %), ainsi que les serveurs d'entreprise dans le cloud (27 %). Les outils et logiciels IA ont été le point d'entrée pour 15 % des entreprises.

Aucune entreprise n'aime verser de l'argent à des malfaiteurs qui ont piraté leurs données, mais s'agissant d'attaques par ransomware, il est fréquent que les entreprises fassent tout leur possible pour récupérer ce qui a été perdu. Cela comprend le versement d'une rançon, lorsqu'elle est exigée. De toutes celles qui ont versé une rançon, 60 % ont récupéré l'intégralité ou une partie de leurs données et deux entreprises sur cinq (41 %) ont reçu une clé de récupération mais ont tout de même dû reconstruire leur système.

Le versement d'une rançon ne résout pas toujours le problème. En effet, 31 % des entreprises qui ont versé une rançon ont reçu une demande d'argent supplémentaire, et 27 % ont subi une autre attaque, bien que ne provenant pas nécessairement de la même source.

État des attaques

Typologie des attaques subies par les entreprises au cours des 12 derniers mois.



État des attaques suite

71 %

La majorité des entreprises disposent d'une forme de cyber-assurance.

Les conséquences d'une cyber-attaque peuvent être graves et durables, allant parfois jusqu'à menacer la survie d'une entreprise. Un tiers des entreprises touchées (33 %) ont dû payer des amendes suffisamment élevées pour mettre en péril leur santé financière, et beaucoup ont par ailleurs fait état d'une baisse de leurs indicateurs de performance commerciale (30 %), d'une augmentation de leurs coûts liés à la notification des clients (29 %) et d'une plus grande difficulté à attirer de nouveaux clients (29 %).

Pour celles qui doivent s'acquitter d'une amende, la situation est complexe. Les entreprises ayant des activités à l'étranger peuvent encourir non seulement des amendes dans leur pays, mais également dans les pays ou régions où elles mènent leurs activités. Une fuite de données peut entraîner des amendes pour non-respect des règles en matière de protection des données des clients dans des territoires comme la Californie, le Canada, l'UE ou autres, et les amendes réglementaires peuvent se chiffrer en milliers voire en millions de dollars ou d'euros.

L'assurance est un levier que les entreprises utilisent pour atténuer les effets de ces attaques. La majorité des entreprises interrogées (71 %) sont dotées d'une police de cyber-assurance ou d'une couverture cyber dans le cadre d'une autre police.

Les entreprises de 1 à 10 salariés sont moins nombreuses à avoir souscrit une cyber-assurance (65 %) que celles de 11-49 salariés (49 %) ou celles de 50-249 salariés (82 %).

L'impact des cyber-attaques sur les collaborateurs de l'entreprise est considérable. Les cyber-incidents sont une source de stress important pour les salariés (39 %) et peuvent mener à l'épuisement professionnel (burn-out) (32 %) ou entraîner une augmentation des congés maladie (31 %).

Si de tels événements peuvent aussi renforcer l'esprit d'équipe (38 %) et la loyauté envers l'entreprise (43 %), ils contraignent les entreprises à apporter un soutien nécessaire à leurs collaborateurs pendant et après une attaque.



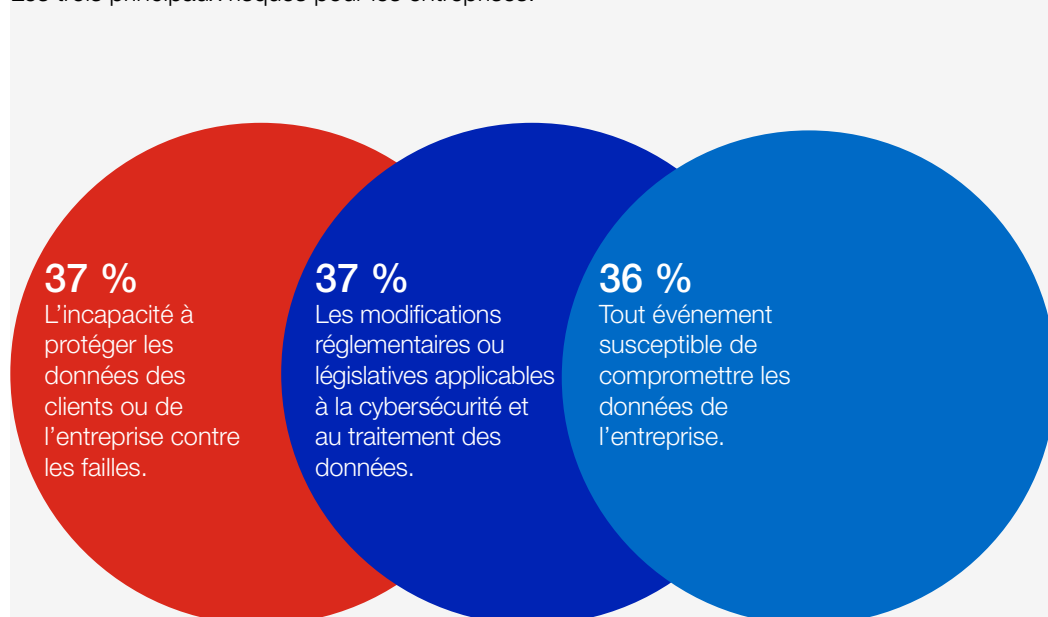
Le rapport de cette année révèle à quel point l'intelligence artificielle transforme le paysage des cyber-menaces. Mais plus encore, il met en lumière la dualité de cette technologie : alors qu'elle apparaît comme un atout stratégique pour renforcer la cyber-résilience d'une entreprise, elle est également devenue un outil pour les pirates informatiques, augmentant la sophistication et la complexité des cyber-attaques.

Ana Silva

Directrice Risques Professionnels (PSC)
Hiscox Iberia

Principaux risques-cyber

Les trois principaux risques pour les entreprises.





L'impact humain d'une cyber-attaque ne devrait jamais être sous-estimé. Les salariés subissent un stress immense, qui peut entraîner une augmentation des absences ou mener au burn-out. Soutenir les salariés après une cyber-attaque n'est pas seulement la bonne chose à faire, cela aide également l'entreprise à se rétablir et à renforcer sa résilience pour l'avenir.

Mike Maletsky

VP Technology & Cyber
Hiscox USA



Les entreprises agissent

79 %

Investir dans des mesures de cybersécurité supplémentaires pour les salariés en télétravail.

Presque toutes les entreprises consacrent des ressources à la prévention des attaques et 94 % prévoient d'augmenter leurs investissements dans la cybersécurité et la protection des données l'année prochaine. Le Portugal (45 %) et l'Espagne (40 %) sont en tête des pays où les investissements devraient augmenter significativement.

Plus de la moitié des entreprises du secteur automobile dans le monde (54 %) prévoient d'accroître considérablement leurs investissements dans la cybersécurité et la protection des données. Viennent ensuite les organismes publics (49 %), les entreprises du secteur des télécommunications (47 %) et celles du secteur de la chimie (45 %).

La conformité réglementaire joue également un rôle important : 81 % des entreprises mettent en place des mesures pour s'adapter aux exigences réglementaires en matière de cybersécurité. Les entreprises qui ont subi une cyber-attaque l'an dernier sont plus nombreuses (87 %) à déclarer s'être adaptées à la réglementation que les autres (72 %).

Le télétravail représente un autre défi en matière de sécurité pour les entreprises, 79 % d'entre elles ayant investi dans de nouvelles formations à la cybersécurité pour les salariés travaillant à distance, afin de prévenir les attaques.

Des contrôles de sécurité fréquents sont un autre moyen de limiter les cyber-menaces pour les entreprises. 91 % des entreprises réalisent au moins une fois par trimestre des analyses de leur cyber-vulnérabilité, telles que des simulations ou des tests d'intrusion.

Par ailleurs, lorsqu'elles cherchent à identifier l'origine des menaces, les entreprises mènent des investigations au-delà de leurs propres systèmes et de leurs salariés. En ce sens, 88 % des entreprises réalisent au moins une fois par trimestre une évaluation des risques-cyber liés à leurs fournisseurs et partenaires.

L'expérience incite les entreprises à agir

Les entreprises attaquées au cours des 12 derniers mois sont plus enclines à investir dans la formation que les autres.

87 %

des entreprises qui ont subi une attaque investissent dans la formation.

68 %

des entreprises qui n'ont pas subi d'attaque investissent dans la formation.

Cyber-résilience



Notre modélisation de la cyber-maturité est un outil gratuit qui aide les entreprises à comprendre leurs forces et leurs faiblesses en matière de cybersécurité.

Les entreprises estiment que malgré la persistance des menaces et les conséquences qu'elles induisent, elles ont fait des progrès : la grande majorité (83 %) ont amélioré leur cyber-résilience au cours des 12 derniers mois. Ces améliorations reposent sur une combinaison de facteurs, notamment le renforcement des effectifs en charge de la sécurité, l'investissement dans des logiciels et une meilleure formation des salariés à la cybersécurité.

Malgré leur confiance affichée dans la résilience de leur entreprise, les équipes en charge de la cybersécurité ne se reposent pas sur leurs acquis : elles sont bien conscientes des nouvelles menaces, très largement induites par l'IA, qui nécessiteront toujours plus de vigilance et de travail.

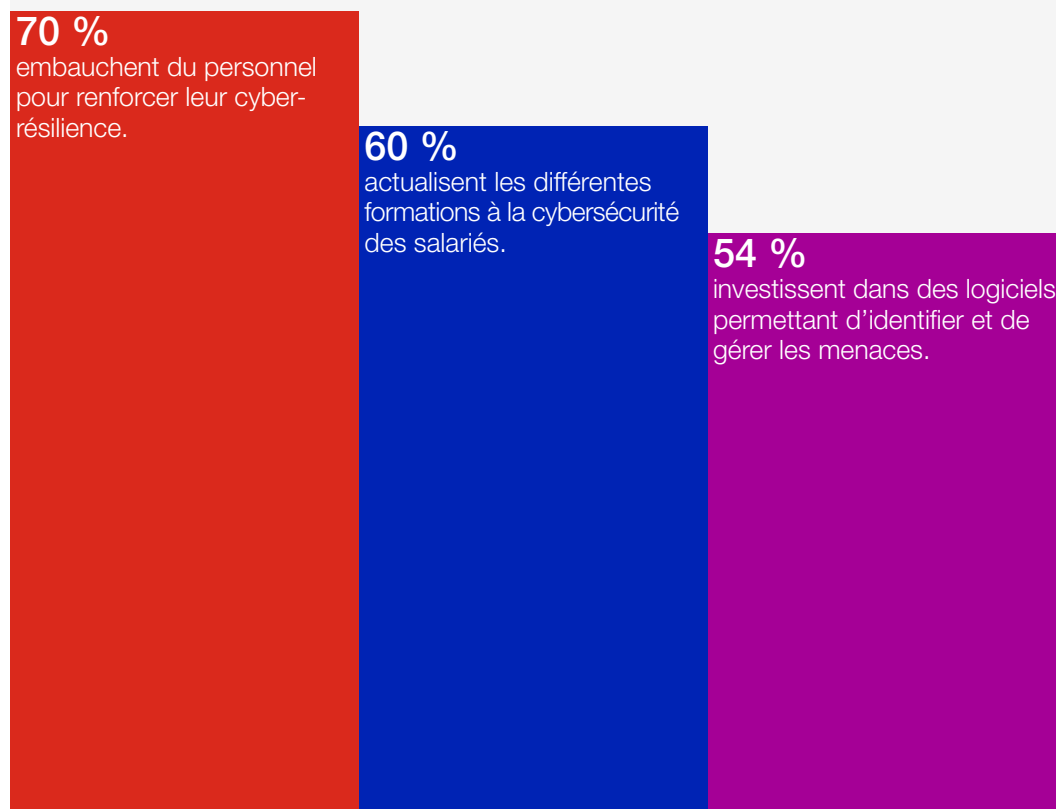


Les risques-cyber sont autant liés aux personnes qu'aux technologies. Nous travaillons avec des milliers de micro et de nano-entreprises sur leur protection contre les risques-cyber et le plus grand facteur de risques reste encore et toujours le facteur humain. Lorsque vous créez une entreprise, vous devez souvent jongler avec de nombreuses casquettes. Il est donc essentiel d'obtenir de l'aide pour protéger votre entreprise contre tous les risques-cyber auxquels elle est peut être confrontée, tels que le piratage de messagerie professionnelle, le détournement de paiement et l'ingénierie sociale. C'est pourquoi, chez Hiscox, nous travaillons avec nos clients en proposant des formations et des simulations de phishing pour renforcer leur résilience face aux escrocs et aux acteurs malveillants qu'ils rencontrent quotidiennement, pour les aider à se concentrer sur ce qu'ils font de mieux.

Diva Aoun
Directrice Cyber
Hiscox Europe

Améliorer la cyber-résilience

Les entreprises se prémunissent contre les futures menaces.





L'IA est un outil qui change la donne pour les entreprises de toute forme et de toute taille, mais elle augmente leur vulnérabilité aux risques-cyber si celles-ci ne disposent pas de l'expertise ou de la protection adéquates. Nos produits d'assurance de responsabilité civile professionnelle et de cyber-assurance protègent contre les sinistres découlant de l'utilisation de l'IA, y compris dans des situations où le piratage implique l'IA.

Nicolas Kaddeche

Directeur Technique et du
canal Direct
Hiscox France



L'IA et les menaces futures

L'essor rapide des services intégrés d'IA générative offre de nouveaux moyens de combattre les menaces, même si les acteurs malveillants utilisent la technologie pour créer de nouvelles attaques.

Près de deux-tiers des responsables de la sécurité dans leur PME (65 %) considèrent que l'IA constitue davantage un atout qu'une vulnérabilité pour leur entreprise. Les entreprises portugaises sont particulièrement enclines à considérer l'IA comme une aide à la sécurité (86 %), ce qui est moins le cas pour les entreprises aux États-Unis et au Royaume-Uni (58 % et 59 %, respectivement).

Les trois principales nouvelles menaces liées à l'IA dans les cinq prochaines années sont les attaques par ingénierie sociale (60 %), les logiciels malveillants créés par l'IA et les attaques de phishing (60 %) et la prise de contrôle des données de leur entreprise par l'IA (60 %).

Pour 22 % des entreprises, les installations (via une attaque physique ou par proxy sur les infrastructures) et les salariés (via l'ingénierie sociale ou le phishing) sont les points d'entrée les plus probables pour les fuites de données ou les attaques par ransomware. Les logiciels et les systèmes (20 %) et les tiers partenaires (20 %) sont également considérés comme des points d'entrée courants.

Les entreprises peuvent lutter plus efficacement contre les cyber-menaces si les salariés sont mieux informés sur la nature de

ces menaces et la façon de réagir en cas d'attaque.

Presque toutes les entreprises ayant subi une attaque (96 %) estiment qu'une meilleure information eu égard aux cyber-attaques et procédures, ou une meilleure compréhension de celles-ci, permettrait de réduire les délais de réponse lors de futurs incidents.

Il est essentiel d'optimiser le temps nécessaire pour évaluer une attaque qui s'est produite ou qui est en cours, afin d'y répondre de manière appropriée et de limiter les dommages. Parmi les entreprises victimes d'une attaque, beaucoup estiment qu'une meilleure connaissance des menaces potentielles avant leur survenance permettrait d'améliorer les délais de réponse (57 %).

Une meilleure compréhension des éléments à prendre en compte lors d'une attaque est un autre moyen d'accélérer la réponse (56 %). En ce qui concerne les mesures à prendre ensuite, près de la moitié des entreprises interrogées (49 %) suggèrent qu'il serait utile d'informer en amont sur les personnes auprès de qui signaler une attaque. De même, pour 49 % des entreprises, les délais de réponse pourraient être réduits si le processus de décision en cas d'attaque était plus efficace.

49 %

estiment qu'un processus de décision plus efficace est nécessaire pendant une attaque.

Se préparer à la menace liée à l'IA

Les entreprises agissent pour se protéger contre les menaces en constante évolution et prévoient de mettre en œuvre les mesures suivantes au cours des trois prochaines années.

37 %

Veiller à ce que les polices d'assurance intègrent les risques liés à l'IA.

36 %

Sensibiliser les salariés à la menace liée à l'IA par le biais de formations.

36 %

Réaliser des audits réguliers de l'utilisation de l'IA.

33 %

Embaucher des salariés spécialisés dans l'IA.

33 %

Mandater des consultants spécialisés dans la sécurité de l'IA.

Divulgations obligatoires

71 %

sont favorables à la divulgation du montant des rançons versées.

Une loi australienne unique en son genre est entrée en vigueur il y a quelques mois, obligeant toutes les entreprises à divulguer aux autorités, dans un délai de 72 heures, le montant de toute rançon versée à la suite d'une attaque par ransomware.

Si la plupart des entreprises participantes (71 %) se sont déclarées favorables à la divulgation du montant des rançons, les avantages et les inconvénients de cette réglementation continuent de faire débat.

Les chefs d'entreprise, DSI, RSSI et directeurs informatique sont largement d'accord (entre 71 % et 77 %), mais, selon nos observations, les directeurs de la sécurité partagent moins souvent cet avis (50 %).

Les entreprises qui n'ont pas subi de cyber-attaque l'an dernier étaient plus nombreuses (85 %) à approuver l'obligation de divulgation, que celles qui ont subi une attaque (61 %).

54 % des entreprises déclarent que les divulgations peuvent aider les clients et les

parties prenantes à évaluer la santé financière, et 52 % estiment qu'elles aident les autorités à combattre les ransomwares. La majorité des personnes interrogées au Portugal (52 %) et en Espagne (52 %) considèrent également qu'il s'agit d'un moyen d'éviter de stigmatiser les entreprises qui ont payé pour protéger leurs données.

Pourtant, des préoccupations demeurent : 49 % craignent que les divulgations obligatoires encouragent les pirates et 53 % considèrent que les entreprises privées ne devraient pas avoir l'obligation de divulguer publiquement leurs finances.

S'il est vraisemblable que des rançons continueront d'être versées, avec des résultats variables, le débat entourant la divulgation du montant des rançons, en particulier s'agissant des sociétés privées, devrait prendre de l'ampleur, notamment si de nouvelles lois ou réglementations imposent cette obligation.



L'introduction d'une obligation de déclaration se heurtera inévitablement à une certaine résistance, mais la nécessité de démanteler le modèle économique de la cybercriminalité fait universellement consensus. Alors que le Royaume-Uni prend des mesures ambitieuses pour lutter contre les ransomwares et renforcer la sécurité dans le pays, les petites entreprises doivent continuer à prendre en main leur cybersécurité et à investir dans leurs salariés et leurs moyens de défense.

Alana Muir

Directrice Cyber
Hiscox UK

Le débat de la divulgation

Raisons pour lesquelles les entreprises devraient ou non être tenues de divulguer le montant des rançons en cas d'attaque par ransomware.

Favorables à la divulgation

54 %

déclarent que les divulgations permettent aux clients et aux parties prenantes d'avoir une image plus claire de la santé financière d'une entreprise.

52 %

pensent que davantage de transparence pourrait aider les autorités à apporter une réponse lors de futurs incidents impliquant des ransomwares.

Opposés à la divulgation

53 %

estiment que les entreprises privées ne devraient pas être obligées de révéler leurs informations financières.

49 %

craignent que les divulgations puissent inciter des acteurs malveillants à lancer des attaques par ransomware.

Comparaison par pays



Cyber-vulnérabilité

L'Irlande a enregistré le taux le plus faible de cyber-attaques au cours des 12 derniers mois (42 %), tandis qu'en Allemagne (67 %) et au Royaume-Uni (65 %) les entreprises ont été plus nombreuses à subir au moins une attaque.



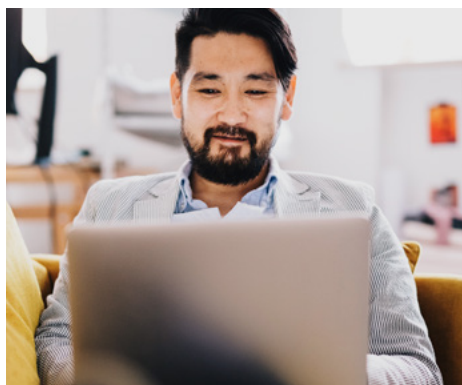
Récupération de données

Pour celles qui ont versé une rançon après une attaque par ransomware, les États-Unis ont enregistré le taux le plus élevé de récupération de données (74 %), et l'Irlande le plus faible (53 %*).



Réglementation

Le Portugal (86 %) et l'Irlande (85 %) ont davantage confiance dans la capacité des entreprises à s'adapter aux nouvelles exigences réglementaires en matière de cybersécurité, contrairement aux États-Unis (76 %).



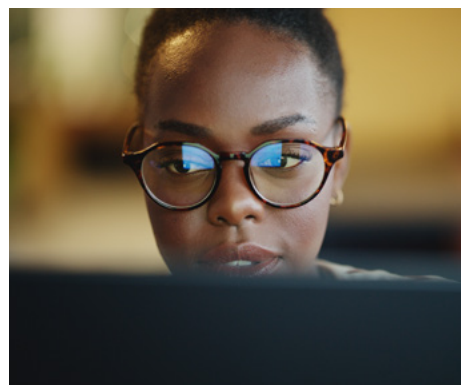
IA

Le Portugal (86 %) a davantage tendance à considérer l'IA comme un atout en matière de sécurité plutôt que comme une vulnérabilité. Les États-Unis (58 %) et le Royaume-Uni (59 %) sont moins enclins à partager cet avis.



Divulgation obligatoire

C'est aux États-Unis (80 %) qu'on trouve le plus d'entreprises favorables à la divulgation obligatoire des montants de rançon versés. Ce soutien est plus faible en Allemagne (65 %), au Portugal (65 %) et en Espagne (62 %).



Assurance

La couverture de cyber-assurance, au titre d'une police dédiée ou dans le cadre d'une autre police, varie selon les pays, le taux de souscription le plus faible étant en France (61 %).



Conseils aux PME en matière de cybersécurité



Installez un logiciel de sécurité de bonne réputation.

L'un des moyens les plus efficaces de limiter les cyber-menaces les plus récentes est d'installer un logiciel de sécurité sur tous vos appareils. Ces logiciels combinent plusieurs outils et fonctionnalités qui permettent d'identifier et de bloquer automatiquement les activités suspectes, puis de prendre des mesures pour supprimer la cause de la menace. La dernière génération de logiciels de sécurité est nourrie par l'IA et associe souvent plusieurs fonctionnalités essentielles, telles qu'un antivirus, un pare-feu de réseau, des gestionnaires de mots de passe et des sauvegardes de données, offrant un ensemble complet de contrôles complémentaires pour protéger contre les menaces comme les ransomwares.



Utilisez un gestionnaire de mots de passe et une authentification robuste.

Les mots de passe faibles ou réutilisés sont les premières cibles des pirates lorsqu'ils cherchent à accéder aux systèmes d'une entreprise. Un bon gestionnaire de mots de passe peut vous aider à créer des mots de passe complexes et à les stocker de façon sécurisée. Beaucoup de ces gestionnaires peuvent désormais surveiller les violations de mots de passe et vous informer lorsqu'il est nécessaire de les modifier. Associés à l'utilisation de la biométrie et à l'authentification à plusieurs facteurs (MFA), ils offrent des niveaux de sécurité renforcés pour vos identités numériques. Non seulement les gestionnaires de mots de passe contribuent à réduire les risques-cyber, mais ils sont également plus pratiques pour les utilisateurs et améliorent l'expérience numérique globale.



Maintenez vos systèmes et logiciels à jour.

Les systèmes d'exploitation et les applications obsolètes contiennent souvent des vulnérabilités que les pirates informatiques peuvent exploiter. Mettez en place une procédure pour installer régulièrement les mises à jour sur l'ensemble des appareils et plateformes logicielles de votre entreprise. Envisagez d'activer les mises à jour automatiques des logiciels pour faciliter l'application des correctifs de sécurité, car cela permet de s'assurer que les mises à jour critiques sont installées rapidement et proviennent uniquement du fournisseur authentique. Les mises à jour de routine sont non seulement bénéfiques pour la sécurité, mais elles permettent également de garantir que vos appareils et logiciels fonctionnent de façon optimale avec toutes les dernières fonctionnalités.



Sauvegardez les données de votre entreprise de façon sécurisée et testez régulièrement ces procédures.

Même avec des défenses solides, il existe toujours un risque de perte de données ou d'attaques par ransomware. Des sauvegardes fréquentes et sécurisées, stockées hors ligne ou dans le cloud, garantissent un rétablissement rapide des entreprises si le pire se produit. Aujourd'hui, les sauvegardes de données peuvent souvent être automatisées à l'aide de logiciels qui assurent leur bonne acquisition et un stockage sécurisé, mais il est toujours utile de tester vos sauvegardes régulièrement pour confirmer que les données peuvent être restaurées de façon effective et minimiser les coûts liés au temps d'indisponibilité.



Déterminez les personnes qui peuvent accéder aux données.

Tous les salariés n'ont pas besoin d'accéder à l'ensemble des données de l'entreprise. En limitant les autorisations, de sorte à ce que les salariés aient accès uniquement aux informations et systèmes nécessaires à l'exercice de leurs fonctions, vous réduisez les risques de menaces internes et de fuites de données accidentelles. Vérifiez et mettez à jour régulièrement ces autorisations, en particulier après un changement de poste ou le départ d'un salarié, afin de maintenir votre niveau de sécurité. Si vous utilisez l'IA, il est également important de gérer les autorisations d'accès associées aux agents et aux applications d'IA. Si elles sont mal configurées, elles peuvent souvent mettre en évidence des faiblesses non souhaitables dans les contrôles d'accès aux données et entraîner une fuite accidentelle de données.

Hiscox SA
49 avenue de l'Opéra
75002 Paris

T 01 53 21 82 82

E hiscox.asspro@hiscox.fr

www.hiscox.fr