Communiqué de presse
Paris, le jeudi 24 octobre 2024

Rapport Hiscox sur la gestion des cyber-risques 2024 – 8e édition
Une hausse des cyberattaques enregistrées par 67 % des entreprises, avec un risque majeur pour leur réputation

Paris, 24 octobre 2024 – Hiscox dévoile aujourd'hui les résultats de la 8e édition de son rapport annuel sur la gestion des cyber-risques, marqué par une hausse du nombre de cyberattaques enregistrées par 67 % des entreprises au cours de l'année écoulée.

En voici les principaux enseignements :

- **Le salarié, 1er point d'entrée pour 46 % des entreprises ayant subi au-moins une cyberattaque au cours des 12 dernier mois.**
- **L'utilisation d'appareils personnels par un plus grand nombre de salariés est perçue comme un facteur de risque élevé pour 44 % des entreprises au profil de risque élevé.**
- **Près de la moitié des entreprises touchées par des cyberattaques (47 %) font état de difficultés majeures pour attirer de nouveaux clients, soit plus du double par rapport à l'an dernier (+27 points).**
- **Seulement 56 % des entreprises utilisant l'IA générative sont conscientes que cela impacte de façon considérable leur profil de risque.**

Les TPE/PME dans le viseur des cyberpirates

Dans un contexte de hausse du nombre de cyberattaques, où le risque cyber reste une menace prédominante au sein des entreprises, les attaques touchent plus les PME (entre 20 et 249 salariés) et les TPE (entre 0 et 19 salariés) qu'auparavant. En effet, tandis que les grandes entreprises perfectionnent leur système de protection, la menace se tourne de plus en plus vers leurs partenaires de plus petite taille. Plus vulnérables et moins équipées, elles sont la porte d'entrée des pirates vers les systèmes d'information des sociétés de tailles plus importantes.

État des lieux de la cyber protection : une prise de conscience est amorcée au sein des entreprises, mais il reste encore du chemin à parcourir, notamment face aux nouveaux risques.

Des dirigeants lucides sur leur capacité à gérer le risque cyber
La prise de conscience accrue de la menace des cyberattaques amène les entreprises à souscrire davantage des polices de cyber assurances. Malgré cela, **un tiers des professionnels en charge de la stratégie de cybersécurité de leur entreprise (34 %) pense que leur entreprise n'est pas préparée à affronter des cyberattaques**. Plus d'un quart des dirigeants (26 %) déclarent que leur entreprise ne dispose pas des ressources suffisantes pour gérer le risque financier associé à une menace de

cybersécurité. Un tiers (32%) indique même être en retard dans l'adoption des technologies de cybersécurité nécessaires.

Inquiets des risques pour la réputation de leur entreprise

Bien que les risques financiers demeurent centraux dans le cadre d'une cyberattaque, le risque réputationnel se fait de plus en plus prégnant. **Près d'une entreprise sur deux (47 %) a connu des difficultés pour attirer de nouveaux clients à la suite d'une cyberattaque, soit plus du double de l'édition précédente de ce rapport.** Par conséquent, ils sont 43 % à avoir perdu des clients (contre 21 % en 2023), 38 % à avoir subi une mauvaise publicité (25 % en 2023). Conscients de cette réalité, **61% des dirigeants estiment que l'atteinte à la réputation suite à une cyberattaque porte un préjudice majeur à leur entreprise.**

Et faisant face à de nouveaux types de menaces liées à l'IA

Quelle que soit leur taille, les entreprises doivent également faire face à de nouveaux types de menaces, en particulier celles liées l'IA générative. En effet, si **70 % des entreprises ont déjà intégré cette technologie au sein de leur structure, près de la moitié (44 %) ne se doute pas que celle-ci modifie profondément leur profil de risques**. Elles ne considèrent donc pas qu'il est important de souscrire une couverture spécifique.

Pour autant, **près de deux décideurs interrogés sur trois (64 %) estiment que l'IA générative jouera un rôle essentiel dans l'élaboration de leur stratégie de cybersécurité d'ici à 2030** : si elle peut être utilisée de manière malveillante, l'IA peut également constituer un allié de poids face aux cyberattaques.

« Il est important de rappeler que l'intégration de nouvelles solutions technologiques n'est pas sans risques pour les entreprises. Ces dernières doivent en avoir conscience et adopter une approche résiliente de la cybersécurité, associant des systèmes robustes, des salariés informés et proactifs ainsi qu'une cyber assurance complète. C'est la condition sine qua non *pour réduire au maximum les risques et préserver leur précieuse capacité d'adaptation, propice à l'innovation. »* **précise Nicolas Kaddeche, Directeur Technique chez Hiscox France**

Travailler sa cyber-résilience et prévenir l'« erreur humaine »

Il existe plusieurs leviers pour optimiser sa cyber-résilience et de réduire les risques de cyberattaques :

La formation, la solution clé face au « facteur humain »

Le premier levier concerne une défaillance vieille comme le monde : l'erreur humaine. **Un salarié était le premier point d'entrée de la cyberattaque dans près d'une entreprise sur deux (46 %) ayant subi au-moins une attaque au cours des 12 derniers mois**. **Par ailleurs, l'utilisation accrue d'appareils personnels par leurs salariés est un facteur clé d'exposition pour 44 % des entreprises à haut risque de cyberattaque.** En réponse, deux tiers des dirigeants (65 %) rapportent que leur entreprise a investi dans des formations supplémentaires en matière de cybersécurité pour les salariés travaillant à distance, afin de limiter le risque. C'est pourquoi Hiscox a choisi d'accompagner ses assurés en leur mettant à disposition la CyberClear Academy, plateforme de formation en ligne en matière de sécurité des systèmes d'information.

Hausse des budgets dédiés à la cybersécurité

Un autre levier, plus évident mais néanmoins fondamental, est d'investir pour sa sécurité. **En moyenne, les entreprises ont alloué 11 % de leur budget informatique à la cybersécurité en 2023.**

Les petites entreprises y consacrent même une part plus importante. Fruit du travail de sensibilisation mené depuis plusieurs années par les acteurs de la cybersécurité, trois quarts des entreprises de 1 à 10 salariés et 73 % des entreprises de 11 à 49 salariés ont consacré 11 % à 20 % de leur budget informatique annuel à la cybersécurité.

Anticiper et instaurer une culture de la cyber-conscience

Quelle qu'en soit leur motivation principale, les entreprises doivent adopter une démarche proactive pour limiter les risques. 31 % des entreprises affirment que protéger leur réputation a été l'une des principales raisons pour mettre en place un plan de gestion des cyber-risques. C'est pourquoi Hiscox inclut dans son offre CyberClear une garantie dédiée et une assistance réputationnelle.

« L'erreur humaine reste l'un des grands facteurs de risques, en particulier à l'ère du télétravail. Mais elle est loin d'être une fatalité. Afin de se prémunir des cyberattaques autant que possible, en complément de l'investissement dans les moyens matériels et de couverture, les entreprises doivent instaurer une culture de la cyber-conscience, en reconnaissant que la défense contre les cyber-risques est une responsabilité commune et non une simple préoccupation exécutive ou opérationnelle. » **commente Benjamin Langlet, Responsable Marché Cyber chez Hiscox France.**

Le rapport est accessible sur la page de l'Observatoire Hiscox.

Contacts presse :
Olga Tess - olga.tess@insign.fr - 06 73 46 90 76
Baptiste Romeuf - baptiste.romeuf@insign.fr - 06 63 80 87 54

___

Notes aux rédacteurs : Hiscox, en partenariat avec Man Bites Dog, a réalisé une enquête d'opinion auprès de 2 150 professionnels en charge de la stratégie de cybersécurité de leur entreprise. Pour les besoins de cette enquête, 400 personnes ont été sondées aux États-Unis et 250 dans chacun des pays suivants : Royaume-Uni, République d'Irlande, France, Allemagne, Espagne, Belgique et Pays-Bas. Les entretiens ont été menés entre le 12 août et le 2 septembre 2024.

Ce rapport inclut une comparaison avec les études des années précédentes, en premier lieu le Rapport sur la gestion des cyber-risques 2023. Le panel de 2023, composé de 5 005 professionnels, comprenait plus de 900 personnes basées aux États-Unis, au Royaume-Uni, en France et en Allemagne, plus de 400 en Espagne et plus de 200 en Belgique, en République d'Irlande et aux Pays-Bas.

Le Rapport sur la gestion des cyber-risques 2024 repose sur un panel d'étude plus spécialisé composé de dirigeants d'entreprise et de décideurs dans le domaine informatique. Les participants comprenaient également une plus grande proportion de grandes entreprises (plus de 1 000 salariés) que les années précédentes.

****À propos du groupe Hiscox****

Fondé en 1901, Hiscox est un assureur spécialiste qui assure près de 160 000 particuliers et professionnels en France depuis 30 ans. Pour accompagner au mieux ses clients, Hiscox distribue ses assurances via des courtiers, des partenaires banquiers ou assureurs mais aussi directement en ligne pour les TPE et indépendants.

Assureur historique reconnu de l’Art, des biens d’exception pour la clientèle privée et des assurances de Kidnapping et Extorsion, Hiscox a su développer son expertise dans le domaine des assurances professionnelles, avec désormais plus de 1 500 métiers de services couverts. Grâce à sa connaissance approfondie des métiers de ses clients et de leurs risques, Hiscox propose des couvertures adaptées à leurs besoins et les accompagne avec ses experts avant, pendant et après un sinistre.

Chez Hiscox, l'humain fait la différence. Parce que tout part de l’histoire de ses clients. Assurer une histoire, ce n’est pas seulement protéger des biens : c’est protéger des parcours de vie, des entreprises et des projets qui l’écrivent. Et pour comprendre celle qui se cache derrière chaque contrat Hiscox, nos équipes prennent le temps d’écouter ce qui la rend unique.

En complément, Hiscox met à la disposition des particuliers et des professionnels ses rapports et baromètres, reconnus sur le marché, dans son Observatoire, afin de les tenir informés au sujet de 6 thématiques : la tech, le cyber, l’art, les véhicules de collection, les entrepreneurs et les tendances sociétales.

****À propos de Man Bites Dog****

Man Bites Dog est un cabinet de conseil en marketing stratégique et en leadership éclairé, primé à l'échelle mondiale, dans le secteur B2B. Nous combinons la culture créative et les grandes idées d'une agence, avec les capacités d'intelligence économique et de recherche d'un groupe de réflexion, ainsi que la stratégie et le pouvoir d'activation des médias et du marketing. Nous créons des plates-formes de leadership éclairé qui impliquent le comité de direction, aidant les marques à construire leur réputation, à approfondir leurs relations, à générer des revenus et à réaliser des changements dans le monde réel.