QBE
At the heart of it

Temps nuageux sur le cyber :

le cloud et l'IA amènent des perturbations

Trois points à retenir :

1. L'intelligence artificielle et le cloud renforcent l'efficacité des entreprises mais exacerbent aussi leurs risques.

2. Les pirates informatiques utilisent des tactiques bien rodées mais aussi des outils dernier cri pour extorquer de l'argent.

3. Les entreprises doivent placer la gestion des risques au cœur de leurs opérations pour garantir leur résilience.

La migration vers des plateformes de cloud public, privé ou hybride génère des gains d'efficacité, ce qui favorise l'automatisation et l'adoption de l'intelligence artificielle (IA). Ces avancées créent des avantages concurrentiels, mais les menaces évoluent tout aussi rapidement.

Tandis que les entreprises s'en remettent de plus en plus aux services cloud, les cybercriminels exploitent les faiblesses qui peuvent y être liées, comme les contrôles d'identité défaillants, les erreurs de configuration ou encore la sécurisation insuffisante des données.

L'IA générative (GenAI) amplifie les risques, puisqu'elle réduit les obstacles techniques pour les hackeurs débutants et qu'elle décuple la rapidité et la précision des attaques. Les acteurs malveillants peuvent utiliser la GenAI pour contourner les systèmes de sécurité des entreprises et perturber leurs opérations, avec des répercussions financières, une atteinte à leur image et de potentielles conséquences réglementaires. Ces menaces prennent la forme de deepfakes±, d'usurpations d'identité et d'attaques d'hameçonnage†. Ainsi, les attaques par rançongiciels continuent d'augmenter (IT-ISAC a enregistré 1 537 attaques par rançongiciels au premier trimestre 2025, contre 572 au premier trimestre 2024). Les perturbations qu'elles provoquent représentent désormais un risque majeur pour les entreprises, notamment celles qui utilisent le cloud.

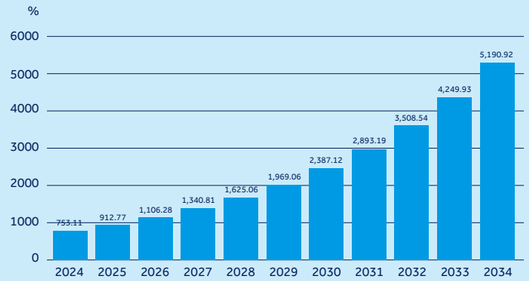
Glossaire

± **Deepfake:** technologie qui utilise l'IA pour produire du contenu vidéo ou audio qui semble très réaliste.

† **Hameçonnage :** tentative d'obtention d'informations privées et confidentielles auprès d'internautes (nom d'utilisateur, mot de passe ou numéro de carte bancaire). Généralement, les cybercriminels se font passer pour des correspondants légitimes et envoient des e-mails ou des messages instantanés qui contiennent des liens infectés par des logiciels malveillants.

Une approche préventive, qui fait la part belle à la résilience, est donc essentielle. Les entreprises doivent intégrer la gestion des risques à leurs systèmes informatiques, anticiper les vulnérabilités de leurs fournisseurs et partenaires, et planifier la continuité de leurs activités.

Figure 1: Valeur du marché mondial du cloud computing (en milliards $)



Control Risks Source: Precedence Research[1]

L'exposition au risque grandit à mesure que s'étend l'adoption du cloud. Le marché mondial qui représente 912 milliards de dollars en 2025 devrait dépasser les 5 000 milliards de dollars d'ici 2034.[2] De plus en plus d'entreprises déplacent leurs infrastructures et leurs données vers des serveurs cloud, qui deviennent donc des cibles privilégiées. Les alertes cloud de haute gravité ont augmenté de 235 % en 2024 par rapport à l'année précédente,[3] signe que l'adoption de cette technologie progresse et que les capacités des cybercriminels augmentent.

La plupart des attaques dans le cloud visent à compromettre les e-mails professionnels (Business Email Compromise, BEC).[4] Les cybercriminels exploitent des plateformes comme Microsoft 365 pour lancer des campagnes de phishing BEC afin de prendre le contrôle de comptes ou de récupérer des identifiants. Ils utilisent une plateforme cloud de confiance plutôt que via le typosquattage‡ ou le spoofing** d'e-mail pour mener des attaques sans déclencher les mécanismes de sécurité les plus courants.[5] De plus, les groupes de cybercriminels sophistiqués ou les hackeurs liés à un État privilégient le cloud pour cibler les infrastructures numériques.

1 precedenceresearch.com/cloud-computing-market
2 precedenceresearch.com/cloud-computing-market
3 unit42.paloaltonetworks.com/2025-cloud-security-alert-trends
4 ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index
5 guardz.com/blog/sophisticated-phishing-campaign-exploiting-microsoft-365-infrastructure

Glossaire

‡ **Typosquattage:** enregistrement d'un nom de domaine ressemblant à un site légitime afin de propager des logiciels malveillants via des liens contenus dans des e-mails d'hameçonnage ou des téléchargements furtifs. Par exemple, des acteurs malveillants pourraient enregistrer une variante du domaine légitime exemple.fr sous le nom exxemple.fr.

** **Spoofing d'e-mail :** stratagème par lequel un cybercriminel falsifie l'adresse de l'expéditeur d'un e-mail afin d'en masquer la véritable origine, pour faire croire qu'il provient d'une source fiable.

Double exposition : rançongiciels et hameçonnage

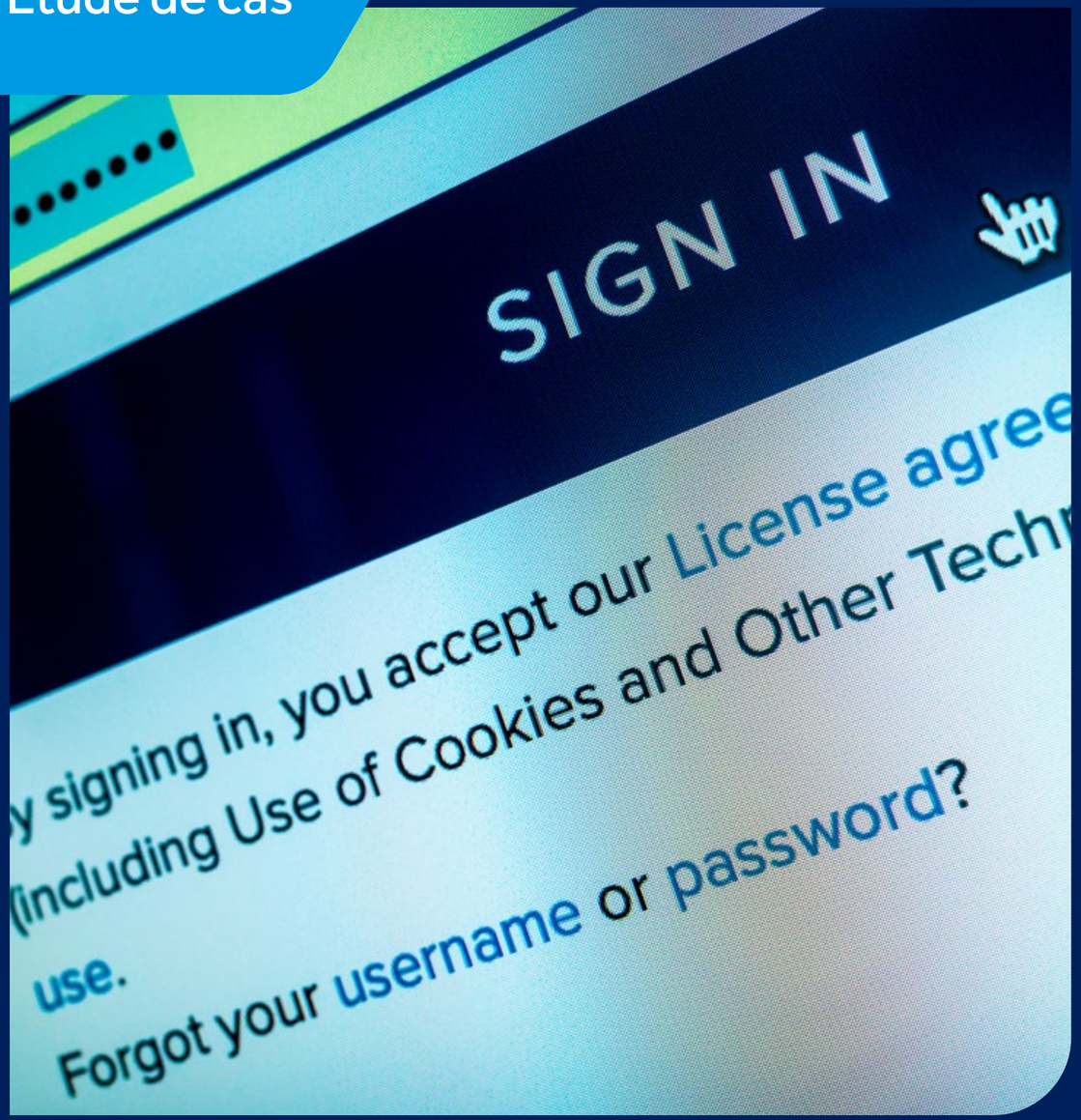
Près de la moitié des données des entreprises stockées sur des serveurs cloud sont classées sensibles,[6] ce qui en fait une cible privilégiée pour les opérateurs de rançongiciels. De nouveaux rançongiciels analysent les outils de collaboration basés sur le cloud, et les cybercriminels sont désormais capables d'évoluer entre les systèmes sur site et sur cloud, chiffrant ou exfiltrant les données au passage.[7]

L'hameçonnage reste le principal point d'accès pour les attaques dans le cloud ; il représentait un tiers des intrusions en 2023 et 2024.[8] Les cybercriminels utilisent souvent des tactiques d'hameçonnage pour voler des identifiants par le biais d'attaques de l'homme du milieu (MITM)‡. Les acteurs de la menace peuvent également exploiter des failles dans des applications cloud, en utilisant des identifiants légitimes volés et en accédant à des comptes administrateurs.

6 cpl.thalesgroup.com/resources/webinars?commid=615147&bt_tok=%7b%7bRecipient.ID%7d%7d
7 microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments
8 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glossaire

‡ **Attaque de l'homme du milieu** (Man-In-The-Middle, MITM) : cette attaque consiste pour un acteur de la menace à s'immiscer dans une conversation entre l'utilisateur (victime) et le système. La position du cybercriminel lui permet d'intercepter, d'envoyer et de recevoir des données destinées à un destinataire légitime.



Okta, 2023

Des cybercriminels ont volé des identifiants d'Okta, un fournisseur d'authentification unique (SSO), et accédé au système de gestion des dossiers d'assistance. En dérobant ces données sensibles, notamment des cookies et des jetons de session, ils ont pu usurpé l'identité d'utilisateurs légitimes.

L'un de ses clients, 1Password, un gestionnaire de mots de passe comptant plus de 100 000 utilisateurs professionnels, a détecté une activité suspecte sur son compte Okta (utilisé pour les applications destinées aux employés) le 29 septembre. L'entreprise a alors suspendu toute activité et enquêté.[9] Okta n'a informé 1Password de la compromission que le 19 octobre, soit 16 jours plus tard, malgré l'alerte donnée par un autre client spécialisé en cybersécurité, BeyondTrust, le 2 octobre.[10]

Au total, 134 entreprises ont été touchées, et la valeur d'Okta en bourse a dégringolé de 2 milliards de dollars.[11,12]

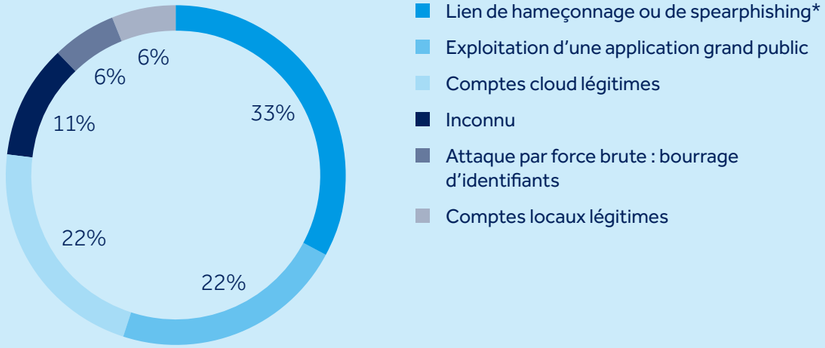
9 arstechnica.com/security/2023/10/1password-detects-suspicious-activity-in-its-internal-okta-account
10 portnox.com/blog/cyber-attacks/unpacking-the-okta-data-breach
11 nightfall.ai/blog/okta-data-breach-what-happened-impact-and-security-lessons-learned
12 cnbc.com/2023/10/23/okta-hack-wipes-out-more-than-2-billion-in-market-cap.html

Chaîne d'approvisionnement : le maillon faible

Les fournisseurs qui hébergent et gèrent des données sont devenus une cible de choix pour les cybercriminels. Une attaque contre un seul fournisseur peut avoir des répercussions sur de nombreuses entreprises, qui se comptent parfois par centaines. Quelles que soient leurs capacités, les acteurs malveillants considèrent le cloud comme une cible potentielle car la valeur marchande des données ne cesse de croître.

D'ici 2025, le volume de données dans le monde entier devrait atteindre les 200 zettaoctets (200 000 milliards de gigaoctets), qu'elles soient stockées dans les réseaux informatiques, les infrastructures publiques, les centres de données, les appareils personnels ou encore les objets connectés.[13] La moitié de ces données seront stockées dans le cloud, contre 43 % en 2024[14], 15 % en 2020[15] et 10 % en 2015.[16] Les services de cloud et de stockage concentrent tant de données précieuses qu'ils suscitent la convoitise parmi les cybercriminels.

Figure 2: Attaques ciblant les environnements cloud, par vecteur d'accès initial (2022-24)



Control Risks – Source: IBM[17]

13 cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
14 storagenewsletter.com/2023/01/25/43-of-data-to-be-stored-in-public-cloud-by-2024-on-average/
15 gartner.com/en/documents/3989101
16 statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/
17 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glossaire

* **Spearphishing:** forme d'hameçonnage qui cible un groupe de personnes partageant une caractéristique commune, par exemple les employés d'une entreprise, les étudiants d'une université, les clients d'une banque ou d'un site Internet.

MURKY PANDA, 2023-2025

MURKY PANDA, un prolifique acteur de la menace lié à l'État chinois, a été observé en train d'exploiter des vulnérabilités zero-day chez des fournisseurs de logiciels en tant que service (SaaS) pour accéder à leur réseau. Le groupe peut contourner les défenses pour rester longtemps indétectable dans les systèmes de clients, ce qui lui permet d'accéder à des données privées pendant de longues périodes. MURKY PANDA a également ciblé un fournisseur de solutions cloud Microsoft en détournant des droits d'accès administrateur.[18]

Ce groupe représente une menace sérieuse pour le secteur public et le secteur privé en Amérique du Nord, notamment les services professionnels et informatiques. Il passe par les fournisseurs ayant accès à des informations sensibles et les environnements cloud sont particulièrement vulnérables à ses attaques. En effet, MURKY PANDA comprend la logique des applications personnalisées et exploite leurs fonctionnalités plutôt que leurs vulnérabilités.

18 crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud

Acteurs liés à un État

Les groupes de cybercriminels liés à des États exploitent de plus en plus les faiblesses des systèmes cloud.

GenAI : bouclier ou arme ?

La GenAI transforme l'environnement des cybermenaces. Son utilisation devrait connaître une forte croissance au cours des cinq prochaines années en Amérique du Nord et en Europe, à mesure que les outils GenAI apportent des gains de productivité dans la plupart des secteurs, si ce n'est tous.

- En 2025, ChatGPT compte 755 millions d'utilisateurs actifs et Microsoft Copilot 88 millions.[19]
- Le nombre d'utilisateurs de ChatGPT a augmenté de 33 % entre décembre 2024 et février 2025.[20]
- 78 % des entreprises déploient l'IA dans au moins une fonction en 2025, contre 55 % en 2024.[21]
- 20 à 40 % des employés utilisent activement l'IA dans le cadre de leurs fonctions, notamment dans la programmation.[22]

Mais le détournement de cette technologie à des fins de fraude et d'extorsion est devenu une menace très répandue. La fraude par deepfake augmente de façon particulièrement alarmante : des cybercriminels se font passer pour des cadres dirigeants, des administrateurs et des personnalités publiques en utilisant des voix, des images et des vidéos de synthèse.

Ces stratagèmes ont pour but de tromper les employés pour qu'ils virent d'importantes sommes d'argent sur des comptes bancaires contrôlés par des réseaux criminels. En 2024, près de 10 % des cyberattaques réussies impliquaient des deepfakes, avec des pertes financières allant de 250 000 à plus de 20 millions de dollars.[23]

19 firstpagesage.com/seo-blog/chatgpt-usage-statistics
20 demandsage.com/chatgpt-statistics
21 sqmagazine.co.uk/ai-tools-usage-statistics
22 sqmagazine.co.uk/ai-tools-usage-statistics
23 Control Risks

Une entreprise de Singapour, 2024

Un escroc s'est fait passer pour le directeur financier d'une multinationale de Singapour. Croyant l'appel vidéo authentique, l'employé a autorisé un virement de près de 500 000 dollars.[24] Bien que les polices de Singapour et de Hong Kong aient retrouvé et intercepté l'argent, l'incident a probablement engendré des coûts considérables en termes de réaction et de rectification.

24 channelnewsasia.com/singapore/deepfake-scam-impersonate-ceo-company-finance-director-5048706

Des cybercriminels soutenus par des États utilisent également la GenAI : ils utilisent les grands modèles de langage (GML) pour développer des scripts malveillants, mener des opérations de reconnaissance ou déployer des attaques à grande échelle. Ils peuvent aussi cibler les GML en aval, à l'intérieur des entreprises, afin de provoquer des pannes ou des perturbations.

Les groupes de cybercriminels exploitent de plus en plus la GenAI et les technologies de deepfake pour mener des attaques à but lucratif dans tous les secteurs à travers le monde. La GenAI est capable de créer des modèles d'hameçonnage efficaces ou de lancer des campagnes d'ingénierie sociale sophistiquées très rapidement. Des cybercriminels aux capacités limitées s'aident de l'IA pour développer des scripts et des logiciels malveillants.[25] Les entreprises seront sans doute bientôt confrontées à davantage d'attaques provenant de groupes auparavant considérés comme inoffensifs par faute de moyens.[26] Les extorsions par rançongiciel rendues publiques ont augmenté de 54 % en janvier – avril 2025 par rapport à la même période l'année précédente.[27]

25 hp.com/us-en/newsroom/press-releases/2024/ai-generate-malware.html
26 anthropic.com/news/detecting-countering-misuse-aug-2025
27 Control Risks

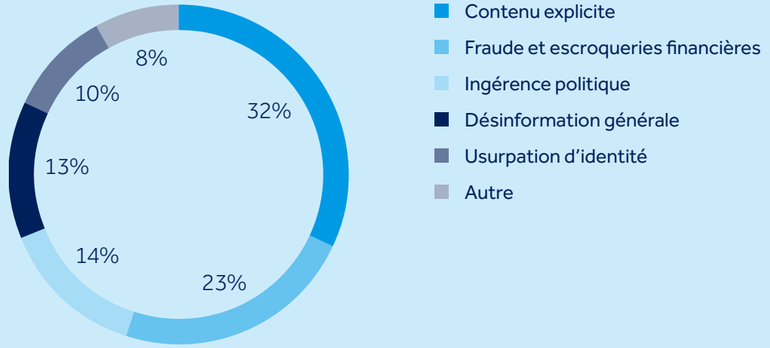
Étude de cas

Amazon, 2025

Un hackeur éthique a mis en évidence des faiblesses critiques dans l'extension Amazon Q pour Visual Studio Code en soumettant une pull request malveillante. En utilisant un simple compte GitHub sans privilèges, le hackeur s'est vu attribuer par inadvertance un accès administrateur. Cet accès lui a permis de demander à l'assistant de réinitialiser les paramètres d'usine, d'effacer le disque local et de supprimer des bases de données de ressources cloud. Le cybercriminel, qui a dit vouloir exposer une faille IA, n'a eu besoin d'aucun logiciel malveillant sophistiqué pour réussir son attaque. Ceci illustre les vulnérabilités qui peuvent apparaître lorsque l'architecture et les contrôles de sécurité sont contrôlés par des tiers.[28] Bien qu'aucune donnée sensible n'ait été détruite, l'incident pourrait inspirer des attaques similaires contre des services d'assistance IA et de sécurité.

28 404media.co/hacker-plants-computer-wiping-commands-in-amazons-ai-coding-agent

Figure 3: Type de contenu des attaques par deepfake, premier trimestre 2025



Control Risks – Source: Resemble AI[29]

Le coût des attaques

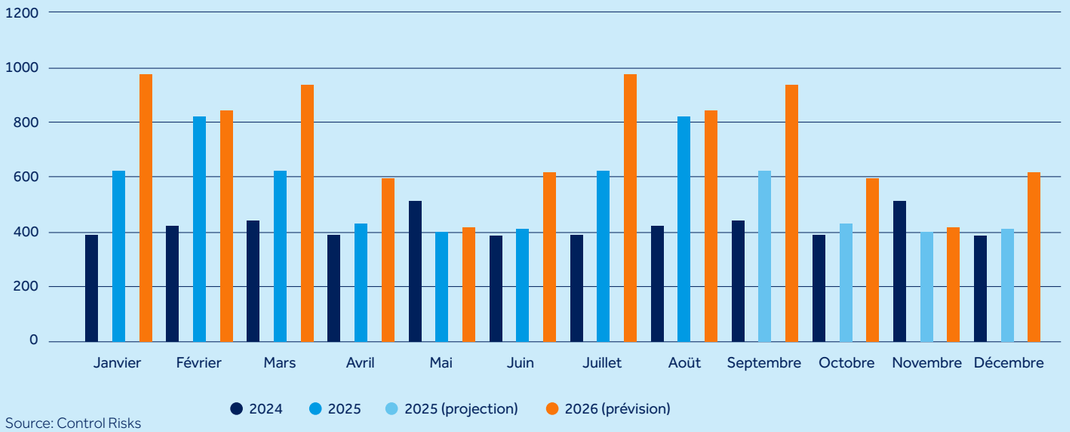
Les attaques par rançongiciel peuvent porter atteinte à la réputation et entraîner des pertes financières, voire des contentieux, non seulement pour l'entreprise ciblée, mais également pour les entreprises partenaires et leurs clients. Ces dernières années, l'adoption généralisée des services cloud et d'autres technologies émergentes est allée de pair avec une augmentation constante des attaques par rançongiciel. Des attaques d'envergure ont fait les titres de la presse britannique au printemps 2025 lorsque le groupe de cybercriminels Scattered Spider a ciblé des entreprises du commerce de détail et de la finance. Les hackeurs ont utilisé des techniques avancées d'ingénierie sociale et d'hameçonnage pour imiter des sites de confiance à l'aide de domaines typosquattés de fournisseurs SaaS tiers ; ils ont trompé les clients pour les amener à fournir leurs identifiants et leurs données de session.[30]

29 resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf
30 reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025

Partout dans le monde, les entreprises restent confrontées à d'importantes perturbations dues à des défaillances de tiers. Ces deux dernières années, des incidents et des pannes liés à des fournisseurs ont frappé de nombreux secteurs. L'un des plus retentissants a été la mise à jour défectueuse de CrowdStrike en 2024, qui a affecté environ 8,5 millions d'appareils Windows. Bien que cela représente moins de 1 % de toutes les machines Windows, la panne a eu des répercussions mondiales, touchant fortement les secteurs de la santé, de l'aviation et des autres transports.

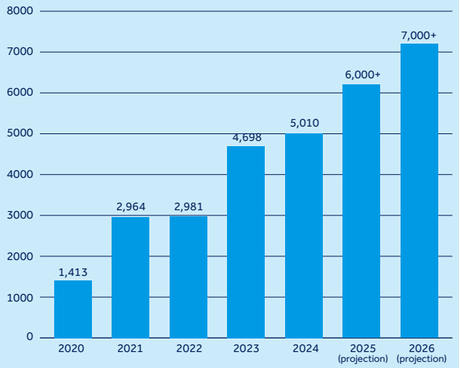
Des cybercriminels ont utilisé CrowdStrike comme leurre pour lancer des campagnes d'hameçonnage et compromettre des systèmes, voler des données et extorquer de l'argent. S'il ne s'agissait pas d'une attaque ciblée, cet incident a mis en évidence l'impact systémique que ces pannes peuvent avoir sur les entreprises dont les fonctions critiques reposent sur un SaaS. Avant cela, d'autres attaques ont perturbé des clients en aval bien au-delà du point de compromission initial, comme celle qui exploitait une faille dans le logiciel MOVEit ou encore la cyberattaque massive NotPetya.

Figure 4: Nombre de victimes de rançongiciels identifiées sur des sites de partage de données volées, par mois



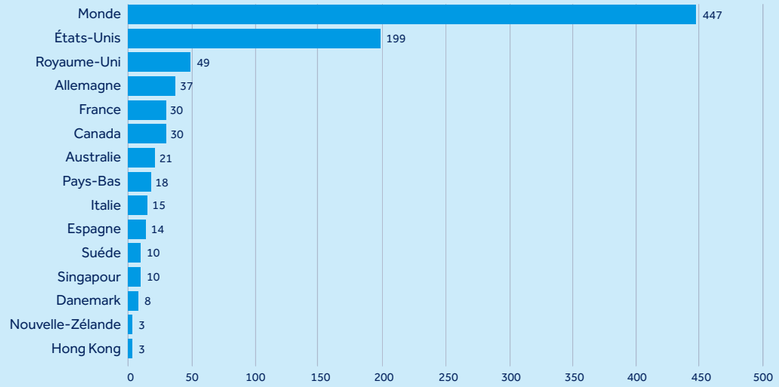
Source: Control Risks

Figure 5: Nombre total de victimes de rançongiciels identifiées sur des sites de partage de données volées (monde entier)



Source: Control Risks

Figure 6: Nombre de cyberincidents majeurs recensés par pays (août 2023-août 2025)



Source: Control Risks

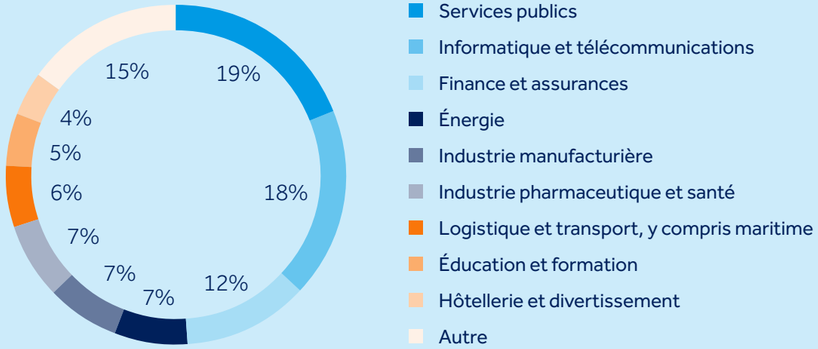
Étude de cas

Rackspace, 2022

En 2022, le groupe de cybercriminels Play a perturbé le service de messagerie Hosted Exchange de Rackspace en exploitant une vulnérabilité zero-day dans Microsoft Exchange. Cette attaque d'élévation de privilèges a touché au moins 27 clients d'Hosted Exchange : les cybercriminels ont obtenu un accès initial via des identifiants compromis, puis bloqué l'accès à la messagerie des entreprises.[31] Les répercussions ont été considérables : Rackspace a dû interrompre son service Hosted Exchange, a été poursuivi en justice par de nombreux clients et aurait subi des pertes d'environ 11 millions de dollars.[32]

31 ir.rackspace.com/news-releases/news-release-details/update-recent-cybersecurity-incident
32 msspalert.com/news/rackspace-taking-losses-of-roughly-11-million-for-hosted-exchange-ransom-attack

Figure 7: Cyberincidents, par secteur (août 2023 - août 2025)



Source: Control Risks

Comme les cybercriminels exploitent une surface d'attaque qui ne cesse d'augmenter, les entreprises du monde entier font face à des risques croissants d'interruptions, de pertes financières et d'atteinte à leur réputation. Leur utilisation de logiciels externes, d'outils d'IA ou d'hébergement cloud dans leurs opérations quotidiennes multiplie les possibilités d'attaque pour les acteurs malveillants.

La résilience dès le départ

Si l'adoption du cloud et l'intégration de l'IA s'accélèrent au rythme prévu, les cybercriminels continueront d'exploiter les nouvelles opportunités et les nouveaux points d'entrée, et les entreprises resteront vulnérables aux attaques. Une stratégie robuste est essentielle pour anticiper et surmonter les cyberincidents, en particulier ceux qui découlent de services tiers ou d'environnements cloud dont dépendent des fonctions critiques.

Renforcer la résilience implique de réfléchir, dès la mise en place de nouvelles technologies, à la gestion des cyberrisques. Cela passe par des protocoles robustes de gestion des identités et des accès (GIA), des audits de configuration réguliers et le chiffrement des données sensibles dans tous les environnements cloud. Pour détecter et contenir les menaces avant qu'elles ne s'aggravent, l'arsenal préventif comporte une veille continue – notamment sur les risques émergents – et des plans de réaction aux incidents.

Il convient également d'établir des protocoles pour gérer l'exposition de sa chaîne d'approvisionnement, mais aussi d'évaluer l'attitude de ses fournisseurs en matière de cybersécurité. En adoptant ces pratiques, les entreprises protégeront mieux leurs opérations, assureront la continuité de leurx activités et entretiendront la confiance de leurs clients dans un environnement numérique de plus en plus volatile.

Microsoft Azure, 2024

En juillet 2024, une attaque par déni de service distribué (DDoS) a frappé la plateforme cloud Azure de Microsoft. La panne, qui a atteint huit heures, a été causée par un fort afflux affectant Azure Front Door et Azure Content Delivery Network. Une défaillance des défenses a ensuite amplifié l'impact au lieu de le contenir.[33]

33 forbes.com/sites/kateoflahertyuk/2024/07/31/microsoft-confirms-new-outage-was-triggered-by-cyberattack

Mesures de renforcement de la cyberrésilience

Les organisations peuvent développer leur cyberrésilience en mettant en œuvre un éventail de mesures :

Comprendre et recenser les profils de risque pour identifier les menaces, les vulnérabilités et les actifs essentiels et dresser un tableau des expositions.

Définir le risque organisationnel acceptable afin que la direction fixe des limites pour l'exposition aux risques.

Donner la priorité aux stratégies d'atténuation qui concentrent les ressources là où elles auront le plus d'impact.

Se préparer aux scénarios les plus pessimistes avec des plans d'urgence et des protocoles de reprise d'activité éprouvés.

Mettre à l'épreuve les capacités de gestion de crise en testant les processus de réaction, de prise de décision et de communication.

Intégrer le soutien tiers à la stratégie de cybersécurité pour une gestion experte des risques résiduels.

Surveiller les tendances et adapter les cyberdéfenses pour garder une longueur d'avance sur l'évolution des menaces, des nouvelles technologies et des besoins de l'entreprise.

Au coeur de la souscription

Amanda Maréchal
Directrice Lignes Financières

Les entreprises françaises utilisent de plus en plus l'infrastructure cloud et les outils d'Intelligence Artificielle (IA) dans leurs opérations quotidiennes, ce qui modifie leur exposition aux risques cyber. Les tendances décrites dans ce rapport sont déjà à l'œuvre et correspondent à nos propres observations dans différents secteurs. De nombreux risk managers se retrouvent dès lors dans une course effrénée pour mitiger ces risques émergents en constante évolution.

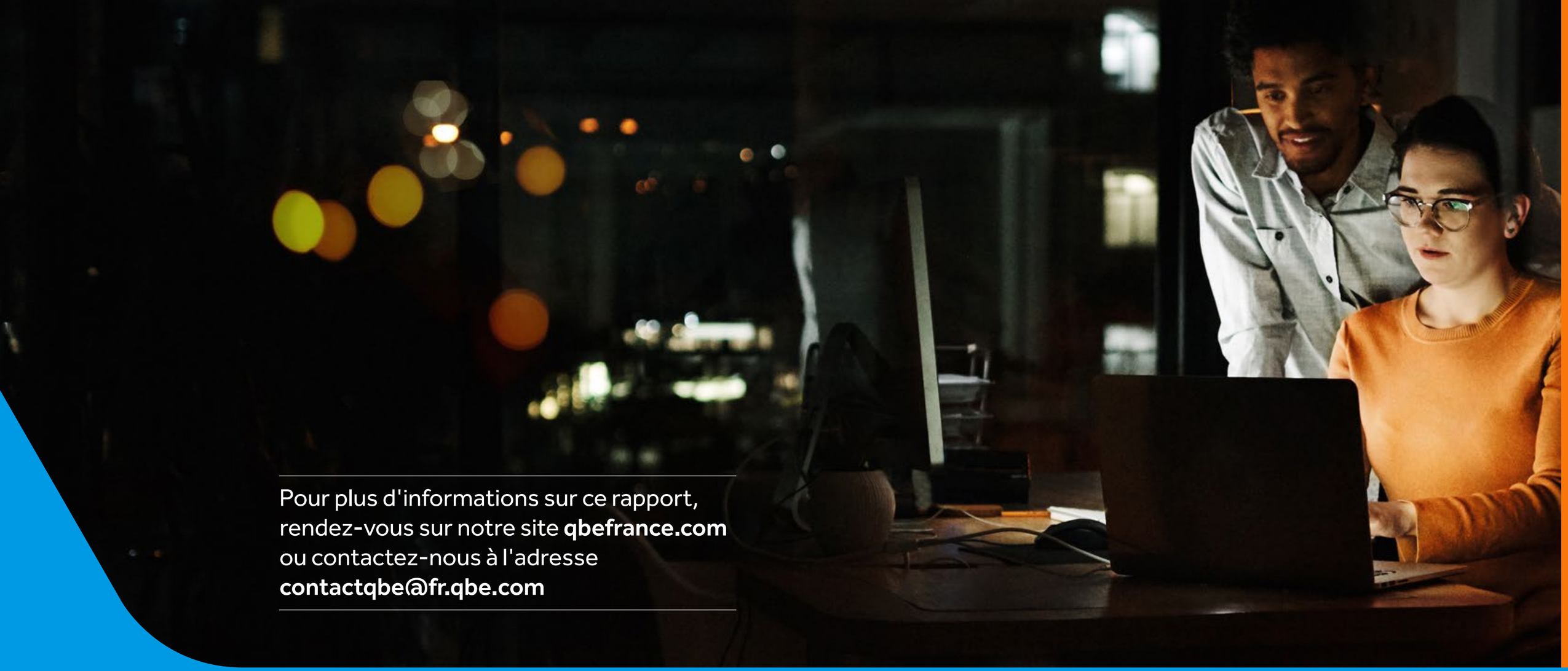
Les menaces planent sur les chaînes d'approvisionnement en France et à travers le monde. Bien sûr, les entreprises qui externalisent certaines fonctions réalisent des gains d'efficacité et des économies. Mais chaque élément externe, chaque niveau de sous-traitance ajoutent une couche supplémentaire au mille-feuille des risques informatiques et logistiques. Les liens multiples entre une entreprise et ses fournisseurs peuvent potentiellement transmettre des logiciels malveillants, mais plus généralement créent un tissu d'interdépendance opérationnelle. Chaque entreprise doit donc comprendre quelles sont ses fonctions qui reposent sur des services externes et, en cas d'interruption, quel sera l'impact.

Plusieurs incidents cyber ont récemment fait les gros titres ; les conséquences sur les entreprises touchées et leurs clients étaient considérables, tant sur le plan opérationnel que financier. Les plateformes cloud sont désormais tellement courantes que les vulnérabilités liées à une infrastructure tierce ne sont plus un problème marginal, mais un défi majeur. De même, la défaillance d'un seul fournisseur peut avoir des répercussions de grande ampleur. La mise à jour ratée de CrowdStrike en 2024 en est un exemple : seulement 8,5 millions d'appareils Windows ont planté mais des pans entiers de l'économie ont été touchés, notamment les transports.

En France, la panne a affecté des vols, des aéroports, des supermarchés, des chaines de télévision, des services de téléphonie mobile et même la préparation des Jeux Olympiques de Paris.

Dans ce contexte d'interconnexion numérique renforcée, l'Union européenne a adopté un schéma directeur pour une meilleure gestion des crises et incidents de cybersécurité. Autrement dit, l'environnement réglementaire se durcit. Les entreprises doivent effectuer les vérifications nécessaires lorsqu'elles sous-traitent des fonctions, les conditions contractuelles doivent être claires en ce qui concerne les risques, le signalement des incidents et la remédiation.

En matière d'assurance, les souscripteurs cyber qui analysent les risques d'une entreprise doivent aller au-delà des défenses périmétriques pour vérifier qu'elle a bien pris en compte les expositions de sa chaine d'approvisionnement. Outre une architecture solide, les entreprises qui adoptent une gestion des risques structurée et la testent régulièrement seront mieux à même de réagir et de récupérer en cas d'incident cyber. Le profil idéal est celui d'une entreprise qui opte pour la résilience dès le départ.



Pour plus d'informations sur ce rapport, rendez-vous sur notre site **qbefrance.com** ou contactez-nous à l'adresse **contactqbe@fr.qbe.com**

QBE European SA/NV
Tour CBX
1 passerelle des Reflets
92913 Paris La Défense Cedex
+33 (0) 1 80 04 33 00

QBEfrance.com

Ce rapport a été développé pour QBE par Control Risks

QBE
At the heart of it

994704/2510-FR