Cybersécurité, un levier de performance et de confiance pour les entreprises

01

Comprendre le risque cyber et **ses évolutions dans le monde**

02

Focus sur **la France**

03

Cyber-résilience : **adopter une démarche progressive pour faire face aux menaces**

04

AXA, un acteur au cœur de l'**écosystème cyber**

FRÉDÉRIC DE COURTOIS
Directeur Général Adjoint du Groupe AXA

« Dans un monde de plus en plus exposé à la **menace cyber**, notre responsabilité est claire : **anticiper les risques pour renforcer la résilience des entreprises et leur permettre de se développer de manière pérenne.** »

Dans un monde de plus en plus interconnecté, la cybersécurité s'impose comme un enjeu stratégique pour la pérennité des entreprises. L'édition 2024 du Future Risk Report d'AXA le confirme avec force : la menace cyber est désormais le troisième risque mondial selon le grand public – et le deuxième pour les experts. Avec l'essor de l'intelligence artificielle, les attaques se multiplient, s'intensifient, se complexifient. Elles touchent désormais tous les territoires, toutes les tailles d'entreprise, tous les secteurs d'activité.

Ce qui était autrefois perçu comme un risque technologique ponctuel est devenu une menace systémique. L'hyper-dépendance aux systèmes numériques et l'industrialisation de la cybercriminalité créent un terrain d'incertitude permanent, où l'anticipation devient vitale.

Dans ce contexte de polycrise, les entreprises ne peuvent plus considérer la cybersécurité comme une option. Se protéger est devenu une condition sine qua non de leur développement. Les conséquences d'une cyberattaque peuvent en effet être dévastatrices : paralysie de l'activité, destruction des données critiques, atteinte à la réputation, voire menace de la survie d'une organisation.

Or nous observons aujourd'hui partout dans le monde une véritable fracture en matière de cybersécurité. Les grandes entreprises ont, pour beaucoup, structuré leur défense. Mais les petites et moyennes entreprises, souvent moins préparées, se retrouvent en première ligne : elles représentent plus des deux tiers des organisations victimes de cyber-extorsion[1]. Ce chiffre est alarmant. Il appelle une réponse collective.

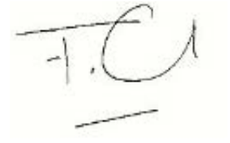
En tant qu'assureur, AXA a un rôle clé à jouer. Notre responsabilité ne se limite pas à l'indemnisation d'un sinistre. Elle commence bien en amont, avec une ambition claire : faire de la prévention un réflexe, et de la protection un levier de confiance pour l'avenir.

Nous mettons l'ensemble de nos expertises au service de cette ambition. En formant en continu et en mobilisant nos ingénieurs, souscripteurs, gestionnaires spécialisés et réseaux de distribution à travers le monde, nous aidons nos clients à évaluer, réduire et couvrir leurs risques cyber. En nous plaçant au cœur de l'écosystème cyber, nous contribuons à faire évoluer les pratiques et à anticiper les mutations d'une menace qui ne cesse d'évoluer.

Ce livre blanc s'inscrit dans cette dynamique. Il vise à éclairer, à sensibiliser, à guider. Il rappelle que la prévention est notre première ligne de défense, que la protection passe aussi par l'humain, et que l'assurabilité d'un risque cyber repose d'abord sur la capacité à agir en amont.

Chez AXA, nous croyons fermement qu'il est possible de concilier croissance économique, développement technologique et maîtrise des risques. Cela exige des entreprises une prise de conscience, un engagement durable, et des partenaires solides à leurs côtés.

Notre ambition est simple : permettre à chaque entreprise, quelle que soit sa taille, de se développer de manière pérenne.



(1) Security Navigator 2025, Orange Cyberdefense (petites et moyennes entreprises : moins de 250 salariés)

SOMMAIRE

JEAN-LUC MONTANÉ
Directeur Assurances IARD Professionnels et Entreprises d'AXA France

« AXA, en tant qu'assureur d'une PME sur trois en France, a le devoir d'accompagner les dirigeants pour **prévenir les risques et les soutenir en cas d'attaque**. »

Quelle est votre vision du risque cyber et du marché de la cybersécurité en France ?

Le risque cyber est devenu l'une des principales préoccupations des chefs d'entreprise. Avec l'explosion du nombre d'attaques – souvent très structurées et difficiles à détecter – la menace concerne aujourd'hui toutes les entreprises, quels que soient leur taille ou leur secteur d'activité.

L'intelligence artificielle joue un rôle ambivalent dans cette dynamique : elle permet de renforcer les dispositifs de défense, mais elle est aussi exploitée par les cybercriminels pour automatiser et cibler leurs attaques.

Par ailleurs, nous observons une forte disparité dans la couverture assurantielle : les grandes entreprises sont, pour la plupart, assurées contre les risques cyber. En revanche, les TPE, PME et ETI sont peu couvertes. C'est une vulnérabilité importante, ces structures étant fréquemment ciblées par les cybercriminels.

Quels sont les principaux freins à la souscription d'une assurance cyber dans les PME ?

Le premier frein est la faible prise de conscience du risque, à la différence des grandes entreprises qui sont davantage sensibilisées. Beaucoup de PME pensent être protégées en externalisant la gestion de leur informatique. Or, en cas d'attaque, la responsabilité juridique et les conséquences économiques pèsent bien souvent sur l'entreprise elle-même – et non sur le prestataire.

Par ailleurs, l'univers de la cybersécurité reste technique et abstrait pour bon nombre de dirigeants. Contrairement à un incendie, un sinistre cyber est difficile à visualiser et nécessite un effort de pédagogie renforcé.

Enfin, le coût peut apparaître comme un frein, alors que les primes d'assurance restent raisonnables au regard des pertes potentielles en cas d'attaque.

Comment AXA accompagne-t-elle les entreprises face à ces menaces ?

Notre approche ne se limite pas à une simple couverture d'assurance. Elle repose sur un accompagnement global structuré autour de trois piliers : prévention, assistance en cas d'incident et indemnisation. La priorité est d'agir avant que le sinistre ne survienne.

C'est pourquoi nous proposons des services inclus dans l'offre cyber, comme des scans de vulnérabilités, pour identifier les failles dans les systèmes d'information. Ils sont réalisés avant même la souscription du contrat et renouvelés tout au long de la relation.

Nous nous appuyons également sur des partenaires spécialisés pour proposer aux entreprises des dispositifs de sensibilisation et de formation de leurs collaborateurs – car dans de nombreux cas, c'est une faille humaine qui est à l'origine de l'attaque.

En cas d'incident, nos experts interviennent aux côtés de l'entreprise pour l'aider à gérer la crise rapidement, en complément de leur prestataire informatique.

Enfin, nous prenons en charge les conséquences financières des attaques : perte d'exploitation, frais de reconstitution des données…

En quoi l'engagement d'AXA face au risque cyber est-il stratégique ?

Face au risque cyber, qui peut compromettre la survie même d'une entreprise, notre rôle dépasse largement le champ assurantiel. En particulier pour les petites et moyennes entreprises, souvent plus vulnérables.
Nous sommes convaincus que la résilience des entreprises repose avant tout sur la prévention, la sensibilisation et l'anticipation. AXA est au cœur de l'écosystème cyber et mène de nombreuses actions sur le terrain, ce qui lui permet de disposer d'une vision fine des risques et de leurs évolutions. AXA est par exemple membre du Campus Cyber, lieu de référence de la cybersécurité en France.
Ces actions se déploient avec notre réseau d'Agents généraux et de courtiers, qui jouent un rôle central dans la sensibilisation et l'accompagnement des entreprises, partout sur le territoire.
Ce maillage unique nous permet d'agir dans la durée, avec des solutions conçues pour évoluer avec la menace.

Comment votre réseau d'Agents généraux et de courtiers participe-t-il à cette dynamique de prévention?

Ils sont en première ligne. Grâce à leur connaissance approfondie des besoins des entreprises et à leur formation continue sur les enjeux cyber, ils sont capables de proposer un diagnostic précis et d'offrir à leurs clients un accompagnement sur mesure.
À travers ses réseaux de distribution, AXA se tient aux côtés des chefs d'entreprise pour les soutenir dans la durée et leur proposer des solutions adaptées à leurs enjeux.

SOMMAIRE

Comprendre **le risque cyber** et ses évolutions dans le monde

01

État des lieux de la menace cyber : des **attaques toujours plus intenses et sophistiquées**, qui visent désormais toutes **les entreprises**

Chaque année, AXA publie un document de référence sur l'évolution des risques à l'échelle mondiale, le Future Risk Report. Le risque cyber figure, en 2024, au troisième rang des préoccupations majeures dans le monde, tous publics confondus, et au deuxième rang pour les experts[1].

4,44M$

C'est le coût moyen, pour une entreprise internationale, d'une violation de données en 2025, en baisse de 9% par rapport à 2024.[3]

+30%

C'est l'augmentation des attaques cyber dans le monde entre 2023 et 2024[2].

91%

C'est la part des experts en cybersécurité qui prévoient une forte augmentation des cybermenaces intégrant de l'intelligence artificielle dans les trois prochaines années[4].

*Les termes signalés par un astérisque sont définis dans le glossaire en fin de document.
(1) AXA Future Risk Report 2024 ; (2) Check Point Software Technologies; (3) IBM, Cost of a data breach report, 2025 ; (4) Sosafe, Tendances en cybercriminalité 2025

Aucune entreprise n'est aujourd'hui épargnée par la menace cyber, quels que soient sa localisation, sa taille ou son secteur d'activité

Une menace désormais mondiale.

Longtemps concentrées sur les pays les plus développés, les cyberattaques s'étendent aujourd'hui à toutes les régions du globe. Les pays émergents deviennent des cibles privilégiées, car ils sont moins matures sur le plan de la cybersécurité, facilitant l'infiltration des systèmes d'information.

34%

L'Asie Pacifique est la première zone touchée par les cyberattaques en 2024[1],

24%

et l'Europe

24%

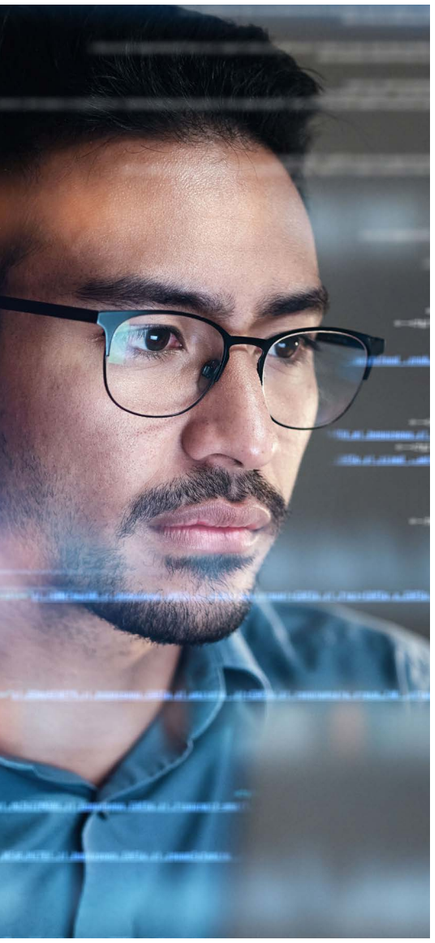
suivie par l'Amérique du Nord,

10%

puis le Moyen-Orient,

8%

et enfin l'Amérique Latine.



Toutes les industries sont exposées aux cyberattaques, mais certains secteurs stratégiques sont particulièrement sous pression.

Les attaquants exploitent en priorité les vulnérabilités identifiées pour compromettre la sécurité des organisations, sans épargner aucun secteur.

Les secteurs critiques comme l'énergie, la santé, l'industrie ou les transports sont particulièrement ciblés, en raison de la complexité de leurs systèmes opérationnels — difficiles à mettre à jour — et de niveaux de maturité hétérogènes en matière de cybersécurité, qui offrent un terrain favorable aux attaques. Les technologies opérationnelles (OT), qui pilotent les systèmes industriels et les infrastructures critiques, représentent un risque majeur : trois organisations sur quatre ont subi au moins une cyberattaque sur leur environnement OT en 2023[2].

Les industries manufacturières sont le premier secteur ciblé, avec

22%

des victimes de cyber-extorsion en 2024, une hausse de

25%

par rapport à 2023[3].

Les petites structures aussi exposées que les grandes entreprises.

Les très petites entreprises (TPE), les petites et moyennes entreprises (PME) ainsi que les entreprises de taille intermédiaire (ETI) font face à des risques de cybersécurité comparables à ceux des grandes entreprises. Souvent moins bien équipées et sans ressources dédiées à la cybersécurité, elles sont devenues des cibles attrayantes pour les cybercriminels. Elles peuvent également servir de points d'entrée pour des attaques visant des grandes organisations, via les chaînes de sous-traitance.

Les petites entreprises (1-49 employés) ont subi une hausse des cyber-extorsions de

53%

entre 2023 et 2024[3].

(1) IBM, X-Force 2025 Threat Intelligence Index ; (2) Palo Alto & ABI research, The state of ot security: A comprehensive guide to Trends, risks, & cyber resilience 2024 (3) Orange Cyberdefense, 2025 Navigator Report

Les groupes cybercriminels évoluent constamment

Malgré les efforts constants des forces de l'ordre – Interpol, le FBI, l'OFAC (Office anti-cybercriminalité), la National Crime Agency, entre autres — pour démanteler les groupes d'attaquants, de nouvelles structures apparaissent en permanence. Ces groupes se fragmentent après opération policière, donnant naissance à des entités plus petites, plus agiles et donc plus difficiles à identifier.

Parallèlement, le cybercrime se professionnalise. Les groupes se structurent comme des entreprises classiques avec des équipes dédiées au recrutement, au support technique et même au service client pour négocier les rançons. Leur modèle économique évolue en permanence pour contourner les mesures de sécurité et la surveillance policière, ce qui rend la lutte particulièrement complexe.

Trois facteurs déterminants derrière l'expansion de la menace cyber

1

Le rôle des technologies dans l'intensification et la sophistication de la menace.

Le rôle ambivalent de l'Intelligence Artificielle.

L'intelligence artificielle représente une avancée majeure pour les entreprises, en améliorant considérablement la détection et la prévention des menaces. Toutefois, elle constitue également une arme puissante pour les cybercriminels :

- automatisation des attaques ;
- ciblage plus précis des victimes ;
- création de deepfakes* : contenus audios ou vidéos malveillants, quasi-indétectables, dans toutes les langues ;
- exploitation facilitée des vulnérabilités*, élargissant ainsi la surface d'attaque disponible.

L'intelligence artificielle permet désormais à des acteurs peu expérimentés de mener des attaques sophistiquées, en détournant des outils dédiés de leur usage initial - par exemple WormGPT qui reprend le modèle de ChatGPT. Ces escroqueries parviennent à tromper tous les profils d'utilisateurs, quel que soit leur niveau de formation ou de sensibilisation à la cybercriminalité.

Cette évolution impose une vigilance accrue : les entreprises doivent intégrer ces nouvelles technologies dans leur stratégie de défense, tout en anticipant leurs usages malveillants.

En 2024 à Hong Kong, un employé a transféré

25 millions
de dollars

à des cybercriminels, trompé par une réunion Teams simulant les membres de son Comité Exécutif[1]. Un montant impressionnant, mais loin d'être un cas isolé.

La vente d'outils dédiés aux deepfakes sur le Dark Web a bondi de

223%

entre 2023 et 2024[2].

L'AVIS DE L'EXPERT

Et demain ?
Technologies quantiques* : un tournant majeur pour la cybersécurité de demain

Les technologies quantiques représentent une menace majeure pour les années à venir : elles ouvriront la voie à des attaques capables de briser certains systèmes de chiffrement actuellement considérés comme sûrs.
On estime que les premières démonstrations concrètes de cette menace pourraient survenir d'ici 2030. Il est essentiel d'anticiper en développant et en adoptant des algorithmes de chiffrement dits « post-quantiques ».
Cette transition s'annonce longue et complexe pour les entreprises, car elle implique une refonte en profondeur des architectures techniques.

MATHIEU COUSIN,
Cyber Risk Consulting & Threat Intelligence Strategist, AXA XL, a division of AXA

(1) Edition CNN, Sun February 4, 2024 ; (2) Accenture, Beyond the illusion—unmasking the real threats of deepfakes, 2024

2

Une interconnectivité croissante qui rend la menace imprédictible.

Les cybercriminels ciblent désormais davantage les Entreprises de Services du Numérique (ESN), non seulement pour voler leurs données, mais surtout pour atteindre celles de leurs clients. Cette stratégie d'attaque « par rebond* » leur permet de contourner les défenses des grandes organisations via leurs prestataires.

De plus en plus intégrés aux chaînes logistiques, les sous-traitants deviennent des cibles de choix. Souvent de plus petite taille, ils disposent de moyens de protection plus limités, servant parfois de point d'entrée vers des structures plus importantes.

L'incident majeur chez CrowdStrike en 2024 est une illustration frappante des impacts de l'interconnectivité croissante. À la suite d'une erreur interne, ce fournisseur de solutions de cybersécurité a déployé une mise à jour défectueuse qui a immédiatement paralysé des millions de postes Windows chez ses clients à travers le monde. Cet incident a entraîné plus d'**1 milliard** de dollars de pertes à l'échelle mondiale, démontrant comment un point de défaillance dans la chaîne numérique pouvait déclencher des perturbations massives[1].

3

Un contexte géopolitique instable qui démultiplie les menaces à l'échelle mondiale.

Les conflits dépassent désormais les champs de bataille traditionnels pour s'étendre au cyberespace. États et groupes affiliés exploitent les failles des systèmes numériques pour attaquer leurs adversaires… et parfois surveiller leurs alliés. On observe également des rapprochements entre groupes cybercriminels et hacktivistes*, qui unissent leurs forces pour mener des actions plus efficaces.

Parallèlement, l'espionnage industriel se banalise : des attaques ciblent les systèmes d'entreprises, d'infrastructures vitales ou d'institutions pour voler des données sensibles et tenter de déstabiliser les économies.

(1) Edition CNN, 2024

Panorama des principaux **risques cyber**

Les cyberattaques qui visent les entreprises sont multiples et évoluent au rythme des technologies. Comprendre les menaces les plus fréquentes permet d'en renforcer la prévention et la résilience.

36 000

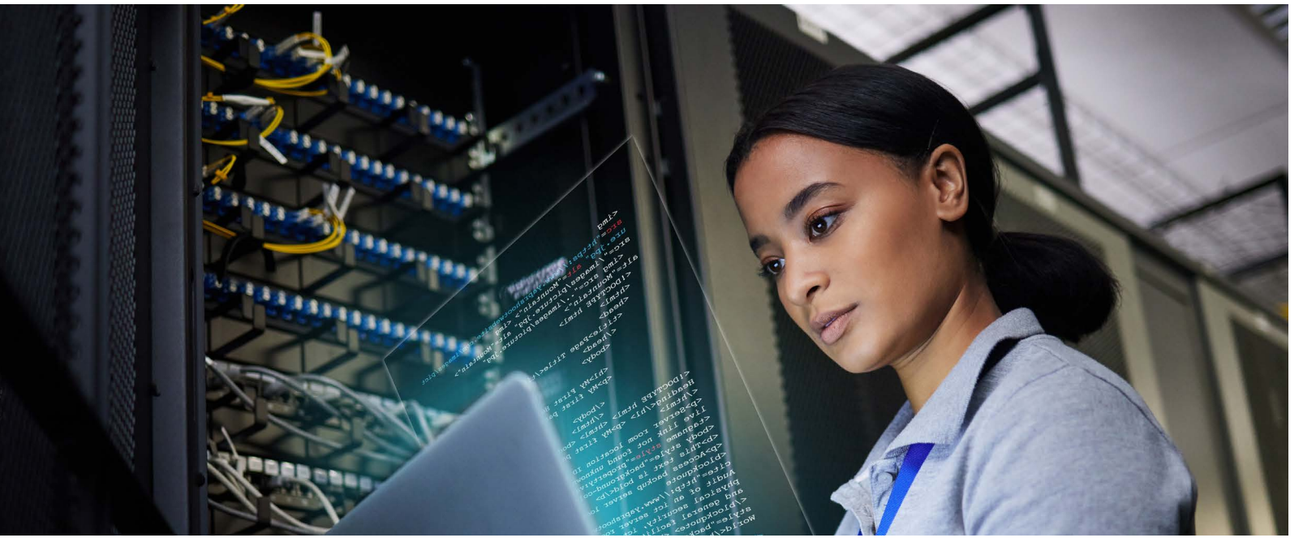
scans automatisés sont lancés par les cybercriminels chaque seconde dans le monde pour repérer des failles de sécurité à exploiter[1].

47%

des entreprises ont constaté au moins une cyberattaque en 2024 en France[2].

9 sur 10

proportion des cyberattaques opérées grâce à une erreur humaine[3].



(1) FortiGuard Labs, 2025 Global Threat Landscape Report ; (2) OpinionWay pour CESIN, Baromètre de la cybersécurité des entreprises, 2025 ; (3) IBM, Indice relatif à la veille stratégique en matière de sécurité

Sept grandes familles de menaces cyber

1

Hameçonnage
*(phishing)**

Fréquence : **Très élevée**

3.4Mds

d'e-mails de phishing sont envoyés chaque jour dans le monde en 2025[4].

MODE OPÉRATOIRE

Message incitant à réagir dans l'urgence pour provoquer une action - cliquer sur un lien frauduleux ou télécharger un fichier malveillant par exemple.

C'est l'attaque la plus courante. Les cybercriminels tentent de voler des informations sensibles telles que des identifiants de connexion ou des coordonnées bancaires. Les campagnes de phishing peuvent être massives et ciblent les employés et les clients par le biais d'e-mails frauduleux. C'est une des principales portes d'entrée des criminels.

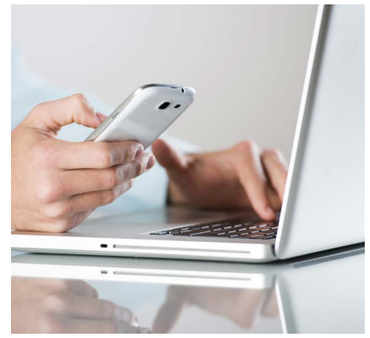
Le phishing évolue avec l'intelligence artificielle, donnant naissance à des variations de plus en plus sophistiquées et réalistes :

- **Vishing (voice phishing)** : appels téléphoniques usurpant la voix d'un tiers de confiance ;
- **Smishing (SMS phishing) :** piège tendu par SMS ;
- **Qishing (QR code phishing) :** attaque par un QR code piégé ;
- **Phishing sur messagerie instantanée :** ciblage des applications professionnelles (Teams, Slack) ou personnelles (WhatsApp, Messenger).

Les cybercriminels recourent de plus en plus aux attaques multivectorielles*, qui renforcent le sentiment d'urgence et poussent les victimes à agir sans réfléchir.

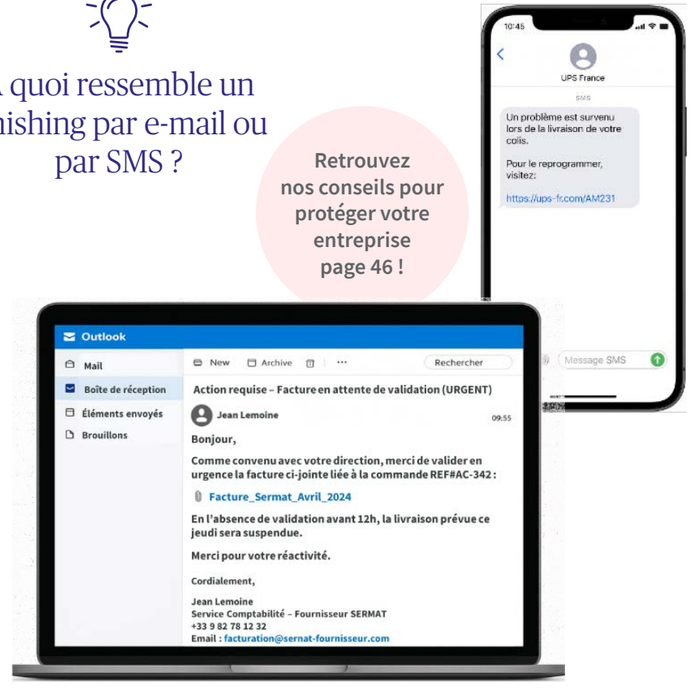
94%

des entreprises françaises constatent ainsi une hausse de ce type d'attaque, qui combine emails, applications de messagerie, réseaux sociaux et appels vocaux par deepfake[5].



À quoi ressemble un phishing par e-mail ou par SMS ?

Retrouvez nos conseils pour protéger votre entreprise page 46 !



(4) DeepStrike, Phishing statistics 2025 ; (5) Sosafe, Tendances en cybercriminalité 2025

2

Rançongiciels *(ransomware)**

Fréquence : **élevée**

59%

des entreprises dans le monde ont subi une attaque par ransomware[1] en 2024.

MODE OPÉRATOIRE

Intrusion, souvent réalisée via une pièce jointe piégée, ou une faille non corrigée. Le logiciel se propage discrètement puis chiffre les données, bloquant brutalement l'accès aux fichiers. Une rançon est alors exigée pour les déverrouiller.

Cette menace consiste à voler et/ou verrouiller les données d'une entreprise pour les rendre inaccessibles jusqu'au paiement d'une rançon. De plus en plus sophistiqués, ces logiciels malveillants ciblent parfois les sauvegardes informatiques et exfiltrent des données sensibles pour pratiquer une double extorsion. Dans certains cas, les cybercriminels vont jusqu'à solliciter les clients des entreprises compromises pour leur réclamer une rançon, réalisant une triple extorsion.

Ce type d'attaque s'est industrialisé avec l'apparition sur le Dark Web de rançongiciels-as-a-service* (Raas), facilement accessibles.
Les répercussions sont souvent dévastatrices : elles entraînent une paralysie opérationnelle, en plus d'autres impacts – comme des atteintes à la réputation ou des sanctions juridiques.

Le ransomware se classe ainsi parmi les cyberattaques les plus coûteuses.

3

Ingénierie sociale *(social engineering)**

Fréquence : **élevée**

98%

des cyberattaques utilisent des techniques d'ingénierie sociale en 2023[2].

MODE OPÉRATOIRE

Appel téléphonique ou message d'un individu usurpant l'identité d'un dirigeant, e-mail soigneusement conçu pour sembler provenir d'un partenaire… L'attaquant joue sur l'émotion, l'urgence et la confiance pour pousser sa cible à agir sans vérifier.

Ces attaques sophistiquées visent de plus en plus les entreprises. En exploitant une faille humaine plutôt que technique, les criminels manipulent un collaborateur pour l'inciter à réaliser une action critique : effectuer un virement, ouvrir un accès, télécharger un fichier piégé…. Ce levier psychologique est au cœur des campagnes de phishing.

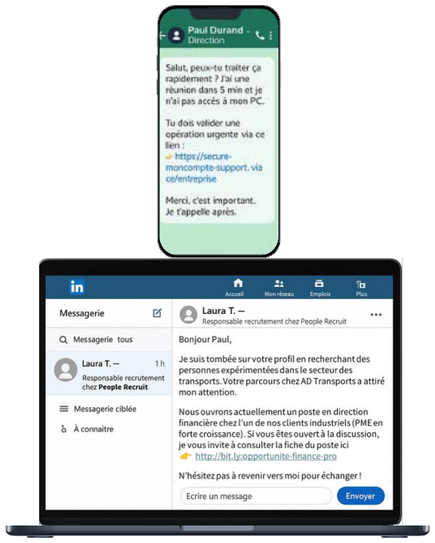
Aujourd'hui, les technologies de deepfake, qui consistent à créer de fausses vidéos ou de fausses voix, permettent de créer des escroqueries d'un réalisme saisissant, rendant ces attaques particulièrement difficiles à détecter.

Les attaques au président en sont une illustration typique : un cybercriminel se fait passer pour un dirigeant et incite par exemple un salarié à effectuer un virement frauduleux, en jouant sur la confiance hiérarchique.

Le cas Scattered Spider

Ce groupe de cybercriminels cible des entreprises en se faisant passer pour des collaborateurs ou des prestataires auprès des services d'assistance, par téléphone ou SMS. Il parvient ainsi à obtenir des accès et à infiltrer les systèmes d'information. Cette méthode d'ingénierie sociale, fondée sur des failles humaines, a déjà entraîné des fuites de données et des interruptions majeures dans de nombreuses grandes entreprises[3].

À quoi ressemble une ingénierie sociale par WhatsApp ou par Linkedin ?



(1) Sophos, The State of Ransomware 2025 (entreprises comptant 100 à 5000 employés); (2) Firewall Times, 2023 ; (3) AXA XL Cyber Risk Consulting Services, Threat Intelligence

4

Attaques par rebond

Fréquence : **élevée**

30%

des compromissions impliquent un tiers en 2024, deux fois plus qu'en 2023[1].

MODE OPÉRATOIRE

Intrusion dans le système d'un prestataire ou partenaire grâce à l'exploitation d'une vulnérabilité technique ou d'une faille humaine. Une fois l'accès obtenu, l'attaquant exploite les connexions ou les droits existants pour se propager vers la cible finale, souvent un grand donneur d'ordre.

Les attaquants ciblent parfois non pas directement une entreprise, mais l'un de ses partenaires disposant d'accès critiques aux systèmes et dont la cybersécurité est moins robuste.

Les prestataires ou fournisseurs ciblés sont par exemple un cabinet comptable, un prestataire informatique, un éditeur de logiciels ou encore une entreprise de transport. Une fois ce partenaire compromis, l'attaquant peut accéder de manière indirecte au système de l'entreprise.

La vulnérabilité d'un maillon de l'écosystème peut ainsi mettre en péril l'ensemble de l'organisation.

En 2025,

54%

des grandes entreprises considèrent leur chaîne d'approvisionnement comme le principal obstacle à leur cyber-résilience[2].

5

Attaques par déni de service distribué *(DDoS)**

Fréquence : **moyenne à élevée**

+53%

de DDoS observées dans le monde au premier trimestre 2024 par rapport à 2023[3].

MODE OPÉRATOIRE

Des réseaux d'ordinateurs infectés (« botnets *») inondent le serveur d'une entreprise de requêtes, provoquant sa saturation.

Ces attaques visent à ralentir ou à interrompre un site internet ou un service en ligne, en les submergeant de requêtes pour les saturer.

Elles ciblent généralement les institutions, lors de conflits géopolitiques ou les sites e-commerce, pour déstabiliser une entreprise.

En mai 2025, Cloudflare — spécialiste de la cybersécurité — a bloqué une attaque DDoS record visant un de ses clients, atteignant 7,3 térabits par seconde. En 45 secondes, plus de 120 000 adresses IP réparties dans 161 pays ont tenté de saturer les serveurs d'un fournisseur d'hébergement. C'est l'équivalent du téléchargement simultané de plus de 9 000 films en haute définition. Cette attaque éclair illustre la puissance croissante des attaques DDoS et l'importance de s'en prémunir avec des solutions adaptées[4].

(1) Verizon, Data Breach Investigations Report, 2025 ; (2) World Economic Forum in collaboration with Accenture, Global Cybersecurity Outlook 2025 ; (3) Cloudflare, Rapport sur les DDoS, 2024 ; (4) Le blog Cloudflare, juin 2025

6

Logiciels malveillants *(malware)**

Fréquence : **moyenne**

MODE OPÉRATOIRE

Logiciels installés via un support infecté (une clé USB par exemple), un téléchargement piégé, des pièces jointes d'e-mails ou encore des mises à jour compromises.

Ces programmes malveillants sont conçus pour collecter, endommager, détruire ou espionner des données informatiques à l'insu des utilisateurs.

Ils permettent d'enregistrer des frappes de clavier, d'intercepter des mots de passe ou de transmettre des données sensibles. Ils prennent la forme de virus, de chevaux de Troie ou encore de vers.

7

Attaques ciblées*

Fréquence : **faible**

MODE OPÉRATOIRE

L'attaquant s'introduit souvent par du phishing, puis installe un logiciel malveillant. Les intrusions peuvent durer plusieurs mois et combiner intrusion, surveillance et extraction de données.

Ces attaques ciblent des individus ou des organisations en raison de leur identité, de leur activité, ou pour accéder à des ressources spécifiques. Elles impliquent une intrusion discrète et prolongée dans le système informatique de l'entreprise sélectionnée afin de lui voler des données stratégiques ou de perturber durablement son activité.

Ce type d'attaque cible en général les entreprises critiques ou innovantes, et peut entraîner le vol de propriété intellectuelle.

En juin 2024, le prestataire de diagnostics médicaux britannique Synnovis a été ciblé par une attaque bloquant ses systèmes et volant les données de milliers de patients. L'incident a entraîné d'importants retards de soins, et le décès d'au moins un malade. Cette attaque illustre la capacité des cybercriminels à perturber durablement des infrastructures critiques et à mettre des vies en danger[1].

(1) Reuters, UK health officials say patient's death partially down to cyberattack, juin 2025

Certaines failles renforcent l'exposition aux cyberattaques

Deux failles critiques favorisent la réussite des cyberattaques, en permettant aux cybercriminels de contourner les protections classiques.

L'exploitation des vulnérabilités techniques

Les cybercriminels exploitent des failles techniques présentes dans les logiciels, les systèmes d'exploitation ou les équipements réseau pour conduire leurs attaques et compromettre les systèmes et les données des organisations. Ces vulnérabilités peuvent résulter de systèmes obsolètes, de logiciels non mis à jour (non patchés*) ou de mauvaises configurations.
Certaines sont connues, répertoriées et peuvent être corrigées par des mises à jour de sécurité. D'autres sont découvertes uniquement lorsqu'elles sont activement exploitées par les criminels. Ce sont les failles zero-day*, pour lesquelles aucun correctif n'existe encore au moment de leur utilisation.

Cas d'une société de services informatiques[1]

En novembre 2023, une entreprise d'une quinzaine de salariés et réalisant un chiffre d'affaires de 6M€ a été victime d'une attaque par ransomware.

L'attaquant a exploité une vulnérabilité Citrix pour se connecter à distance et compromettre la plateforme informatique de l'entreprise. Quinze serveurs dédiés à un client sont ainsi devenus inaccessibles. Une demande de rançon a ensuite été déposée.

La vulnérabilité Citrix était connue depuis juillet 2023. Bien qu'un correctif de sécurité ait été mis à disposition en septembre, l'entreprise n'avait pas mis à jour ses serveurs.

Le facteur humain, principal vecteur d'intrusion des cybercriminels

L'humain demeure le maillon le plus vulnérable de la chaîne de cybersécurité. La majorité des cyberattaques réussies trouvent leur origine dans des erreurs humaines ou des manipulations psychologiques.

- La mauvaise gestion des mots de passe – mots de passe trop simples, partagés ou réutilisés par exemple – offre aux cybercriminels des points d'accès privilégiés.
- Les criminels exploitent la confiance ou l'inattention des collaborateurs pour dérober des informations sensibles ou accéder aux systèmes. Ils jouent également sur la pression hiérarchique, en se faisant passer pour des supérieurs. Le phishing reste l'un des leviers les plus utilisés pour inciter les employés à cliquer sur des liens piégés, à divulguer leurs identifiants ou à exécuter des actions risquées sans en avoir conscience.

(1) AXA France

SOMMAIRE

Impacts des attaques cyber **sur les entreprises**

Les conséquences d'une attaque cyber peuvent être très lourdes pour les entreprises, voire menacer leur pérennité. L'interruption d'activité représente souvent le coût financier le plus important mais d'autres conséquences peuvent également fragiliser les organisations.

9 220 Mds$

coût lié à la cybercriminalité mondiale en 2024[1], l'équivalent du PIB de la troisième économie mondiale, derrière les États-Unis et la Chine.

(1) Statista, La cybercriminalité devrait monter en flèche dans les années à venir, 2024

1

Enjeu économique : l'interruption d'activité, première source de pertes financières

Une attaque cyber n'est pas seulement un incident technique : c'est avant tout une atteinte directe à la continuité de l'activité. Lorsque le système d'information est paralysé, l'entreprise se retrouve à l'arrêt, la production ou les ventes interrompues. L'entreprise subit une perte d'exploitation immédiate affectant sa marge brute.

Par ailleurs, une cyberattaque peut entraîner des frais importants pour les entreprises, par exemple :
- un détournement de fonds ;
- des frais d'expertise et d'assistance informatique ;
- des frais de reconstitution de données…

Cas d'une entreprise industrielle victime d'une attaque par rançongiciel[2]

Cette société de tôlerie industrielle, employant soixante-quinze personnes pour un chiffre d'affaires annuel de 15 millions d'euros, a été la cible d'une attaque par ransomware.

L'incident a entraîné l'arrêt complet de ses activités pendant quatre jours, avant une reprise progressive et un retour à la normale au bout de 10 jours.

Le coût total de l'attaque – incluant les pertes et les frais liés à la restauration du système d'information et des données – s'élève à 690 000€. Aucune rançon n'a été versée aux attaquants.

L'AVIS DE L'EXPERT

GUILLAUME BERCIER,
Agent général, AXA France

La perte d'exploitation constitue sans doute l'impact le plus grave pour une entreprise victime de cyberattaque. L'arrêt brutal de l'activité, même temporaire, peut engendrer des pertes financières majeures, voire compromettre la survie de l'entreprise. J'ai ainsi été témoin, il y a quelques années, des difficultés rencontrées par une structure libérale touchée par une attaque informatique qui l'a privée d'accès à son système pendant deux mois. Durant cette période, les six collaborateurs ont été dans l'incapacité d'exercer. L'impact économique a été considérable, d'autant que l'entreprise ne disposait pas, à l'époque, d'une assurance cyber pour couvrir ses pertes.

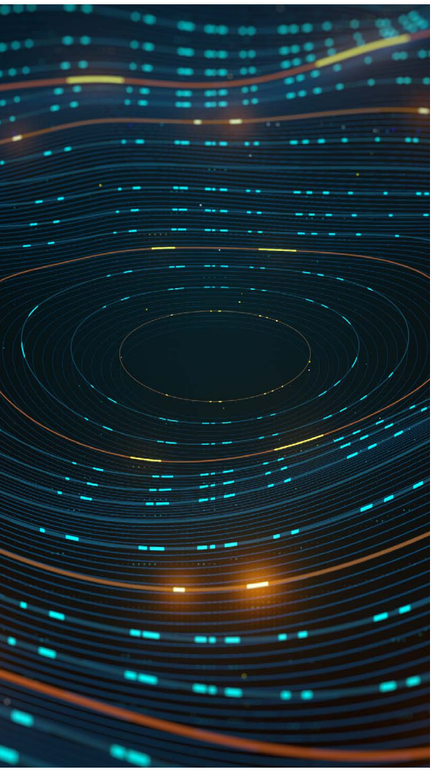
(2) AXA France

SOMMAIRE

2

Perte de données : un levier d'extorsion

Dans les attaques par ransomware, les cybercriminels exfiltrent souvent les données avant de les chiffrer, ouvrant la voie à une double, voire à une triple extorsion. D'une part, ils menacent l'entreprise de publier les données volées si la rançon n'est pas payée. D'autre part, ils peuvent faire pression sur les clients ou partenaires directement, voire revendre les informations sur le Dark Web. Les données ciblées sont souvent sensibles : médicales, financières, personnelles, etc. aggravant les conséquences juridiques et réputationnelles.



3

Atteinte à l'image de l'entreprise

Au-delà des pertes financières immédiates, une cyberattaque peut compromettre gravement la réputation d'une entreprise. La perte de confiance des clients, des partenaires ou des investisseurs peut avoir des effets durables, en particulier si des données sensibles sont exposées. Une mauvaise gestion de la communication de crise — silence, déni, informations floues — aggrave encore la perception. Dans certains secteurs (santé, finance, e-commerce…), la réputation constitue un actif stratégique : une entreprise perçue comme vulnérable ou opaque peut voir son image durablement détériorée, affectant sa croissance, sa valeur de marque et sa capacité à recruter ou fidéliser.

En avril 2025, Marks & Spencer a été ciblé par une cyberattaque sophistiquée. Les attaquants auraient accédé aux systèmes internes en usurpant l'identité de prestataires légitimes, exploitant des failles dans les processus d'authentification et les droits d'accès. Une fois infiltrés, ils ont paralysé les services numériques : site e-commerce, services de paiement, plateforme de click & collect — bloquant ainsi l'activité en ligne pendant six semaines. Certaines fonctionnalités en magasin comme le paiement sans contact ont également été suspendues.

Cette attaque de type multivectorielle, combinant ingénierie sociale, exploitation de vulnérabilités et interruption de services (DDoS), a provoqué un impact opérationnel immédiat, avec un manque à gagner estimé à plus de 350 millions d'euros[1].

Malgré cela, l'entreprise a mis en place une communication de crise exemplaire :

Dès les premières heures, l'entreprise a adopté une communication claire et transparente : excuses publiques du PDG, informations régulières aux clients, collaboration ouverte avec les autorités. Cela lui a permis de :

- Maintenir la confiance en assurant que les données financières n'étaient pas compromises ;
- Gérer les attentes clients en annonçant les délais de réouverture des services ;
- Renforcer sa crédibilité auprès des investisseurs, malgré un impact financier très important.

(1) L'Usine Digitale, 2025

Comprendre le risque cyber et ses évolutions dans le monde

4

Risques juridiques et de non-conformité associés aux attaques

Une cyberattaque peut engager la responsabilité juridique de l'entreprise à plusieurs niveaux :

En cas de négligence avérée — par exemple, l'absence de mesures de sécurité élémentaires ou la non-conformité à des normes en vigueur (RGPD, DORA, NIS2, etc.) — l'entreprise s'expose à des sanctions financières importantes infligées par les autorités de régulation. Dans certaines situations, la responsabilité pénale des dirigeants peut être engagée.

Une attaque ayant causé des préjudices à des clients ou partenaires peut entraîner des poursuites judiciaires pour manquement aux engagements contractuels.

La non-divulgation ou la mauvaise gestion d'un incident peut aggraver la situation en termes de réputation, mais aussi de contentieux avec les actionnaires ou les assureurs.

MATHIEU COUSIN,
Cyber Risk Consulting & Threat Intelligence Strategist, AXA XL, a division of AXA

L'AVIS DE L'EXPERT

En 2021 et 2022, des campagnes d'attaques par rançongiciel, menées par plusieurs groupes malveillants, ont affecté de nombreuses organisations dans tous les secteurs. Certaines compagnies affectées ont été contraintes de suspendre temporairement leurs opérations, avec des conséquences directes pour le public et des impacts économiques régionaux parfois importants.

Sur le plan juridique, ces attaques ont mis en lumière des manquements en matière de cybersécurité. Certaines organisations victimes ont dû répondre à des enquêtes, notamment de la part de la justice mais aussi des régulateurs, portant sur leurs protocoles de sécurité et de gestion de crise. Celles qui ont payé les rançons ont été critiquées pour ces faits, soulevant des débats sur la légalité et l'éthique de financer indirectement les cybercriminels.

Ces affaires ont contribué à l'évolution du cadre réglementaire, notamment en Europe et aux États-Unis, avec un renforcement des obligations de déclaration d'incidents pour les infrastructures critiques.

Cadre réglementaire

Une pression réglementaire en matière de gestion des risques cyber qui s'accroît partout, avec des intensités différentes selon les secteurs et tailles d'entreprise.

Comprendre le risque cyber et ses évolutions dans le monde

Une pression réglementaire croissante à l'échelle mondiale

Avec la multiplication des cyberattaques, les gouvernements ont pris conscience de l'importance d'encadrer la cybersécurité par la loi. Aujourd'hui, de nombreux pays adoptent des réglementations visant à protéger non seulement les infrastructures critiques (comme l'énergie, la santé, les transports, le secteur financier), mais aussi l'ensemble des entreprises et des collectivités, quelles que soient leur taille ou activité.

Un cadre réglementaire fragmenté et complexe

Europe
Densité réglementaire

• Le Règlement général de protection des données (RGPD) a posé un cadre important en matière de protection des données personnelles et de notification des violations de données.

• La directive NIS2[1] impose des obligations plus strictes en matière de gestion des risques et de déclaration des incidents pour les infrastructures critiques.

• La directive CER[2], qui se concentre sur la résilience opérationnelle, est le pendant physique de NIS2.

• Le règlement DORA[3] cible spécifiquement la résilience opérationnelle du secteur financier.

• Le Cyber Resilience Act (CRA) : c'est une réglementation qui fixe des exigences de cybersécurité pour les produits et services numériques commercialisés en Europe. Il vise à réduire les vulnérabilités et renforcer la sécurité dès la phase de conception.

En dehors de l'Union européenne, le nouveau Cyber Security and Resilience Bill au Royaume-Uni adopte une approche similaire à NIS2.

Amérique du Nord
« Patchwork » juridique

• Le cadre réglementaire américain repose principalement sur des lois sectorielles, telles que le GLBA* (Gramm-Leach Bliley Act) pour la finance ou le HIPAA* (Health Insurance Portability and Accountability Act) pour la santé.

• À cela s'ajoutent des réglementations propres à chaque État, comme le CCPA* (California Consumer Privacy Act) en Californie, qui impose, à l'instar du RGPD en Europe, des obligations en matière de protection des données personnelles. D'autres textes, comme la NY DFS 500, s'appliquent spécifiquement au secteur financier dans l'État de New York.

• Au Canada, le projet de loi C-8 vise à renforcer la cybersécurité des entreprises opérant dans des secteurs d'infrastructures critiques.

Asie-Pacifique
Des cadres stricts

• En Asie-Pacifique, les approches réglementaires en cybersécurité sont variées, mais souvent marquées par un haut niveau d'exigence.

• En Chine, les autorités imposent un contrôle strict des données et des mesures liées à la sécurité nationale.

• Singapour privilégie un cadre réglementaire clair et évolutif, axé sur la résilience numérique et la coopération entre acteurs publics et privés.

• L'Australie, de son côté, a récemment adopté le Cyber Security Act 2024, première loi dédiée à la cybersécurité applicable à l'échelle nationale.

(1) NIS2 : Directive Network Information and Security 2 ; (2) Directive Critical Entities Resilience ; (3) DORA : Règlement Digital Operational Resilience Act

Des obligations concrètes qui engagent la responsabilité des dirigeants

Malgré des approches différentes selon les régions, les cadres réglementaires se rejoignent sur le poids des sanctions en cas de non-conformité. Celles-ci peuvent inclure de lourdes amendes, mais également des interdictions temporaires d'exercer des fonctions de direction.
Quelques exemples :

Union européenne

Pour les entités dites « essentielles », la directive NIS2 prévoit des amendes d'au moins 10 M€ ou 2 % du chiffre d'affaires annuel mondial - le montant le plus élevé étant retenu.

États-Unis

En 2022, Morgan Stanley a écopé d'une amende de 35 M$ pour une mauvaise gestion du décommissionnement de serveurs contenant les données sensibles de millions de clients.

Chine

En 2022, Didi Global a écopé d'une amende de 1,2 milliard de dollars. Ses dirigeants ont également été personnellement sanctionnés, à hauteur de 147 000 $ chacun.

Un besoin de conformité complexe mais nécessaire

78%

des chefs d'entreprise à travers le monde estiment, en 2024, que les réglementations en cybersécurité réduisent efficacement les risques dans leur organisation(1).

2/3

de ces mêmes dirigeants considèrent la complexité et la prolifération des exigences réglementaires comme un défi(1).

L'AVIS DE L'EXPERT

Bien que la multiplication des réglementations soit complexe à gérer, elle présente des avantages significatifs : elle élève le niveau global de maturité en matière de cybersécurité, incite l'ensemble des acteurs à progresser et contribue ainsi à renforcer la résilience de l'économie à l'échelle mondiale.

JEAN-PIERRE MARBAIX,
Ingénierie Prévention Cyber, AXA France

(1) World Economic Forum in collaboration with Accenture, Global Cybersecurity Outlook 2025

Les exigences pour une conformité réussie

Les réglementations poussent les entreprises à agir sur deux fronts : d'une part en amont, en renforçant leurs dispositifs de prévention ; d'autre part en aval, en améliorant la remontée d'information en cas d'incident, afin de mieux protéger l'ensemble de l'écosystème.

EN AMONT

Organisation résiliente

Processus internes à même de détecter, d'évaluer et de contrer des menaces cyber potentielles.

Tests réguliers

Tests réguliers de l'infrastructure afin de vérifier sa résistance face aux menaces.

Gestion des tiers

Documentation des services TIC* confiés à des tiers et mise en place de règles de gestion.

INCIDENT

EN AVAL

Signalement

Remontée systématique, auprès des autorités de régulation compétentes, des cyber incidents importants.

Un défi pour les PME au cœur des chaînes d'approvisionnement

La surveillance accrue du régulateur porte sur les entités elles-mêmes et de plus en plus sur leurs chaînes d'approvisionnement. Les PME peuvent ainsi être amenées à rendre des comptes sur leur conformité, si elles opèrent pour des clients ou donneurs d'ordre directement visés par les textes. C'est par exemple le cas des PME dans l'Union européenne sous la directive NIS2.
Bien que ces cadres réglementaires soient nécessaires pour renforcer la cyber-résilience, ils posent un véritable défi pour les plus petites structures en particulier. Les besoins en matière d'investissement et d'organisation à mettre en place vont croissant, et certains dirigeants, ne disposant pas de ressources expertes en interne, peuvent être amenés à s'interroger sur les priorités à mettre en œuvre.

Complexité réglementaire et pénurie de talents : un double enjeu pour les grandes entreprises

Pour les grandes entreprises, le principal défi réside dans la coexistence de multiples réglementations non harmonisées. Être conforme à l'une ne garantit pas de l'être à une autre. Or, ces organisations ne disposent pas toujours des compétences locales nécessaires pour assurer une mise en œuvre efficace. À cela s'ajoute la pénurie de talents dans le domaine de la cybersécurité, qui accentue les tensions. D'autant que les ressources affectées à la conformité ne contribuent pas nécessairement à renforcer la sécurité de l'entreprise.

SOMMAIRE

Focus sur **la France**

02

Réglementation : **où en est-on ?**

La réglementation cyber se renforce et va s'appliquer à de plus en plus d'organisations. Un nombre croissant d'entreprises, y compris parmi les TPE et PME, va devoir s'y conformer.

79%

des entreprises françaises estiment qu'elles sont impactées par les réglementations cyber. La directive NIS2 est la plus fréquemment citée (74%)[1].

15 000

organisations françaises seront concernées par NIS2[2].

(1) OpinionWay pour CESIN, Baromètre de la cybersécurité des entreprises, 2025 ; (2) PWC, 2025

Les entreprises françaises doivent répondre à de nouvelles obligations pour renforcer leur cybersécurité

Si des réglementations spécifiques à certains secteurs d'activité existent déjà en France (NIS1 pour les opérateurs de services essentiels par exemple), on observe depuis quelques années une augmentation de la pression réglementaire afin d'inciter toutes les entreprises à se protéger contre la menace cyber.

NIS2

La directive européenne est en cours de transposition en droit français.
Les organisations concernées devront mettre en place des mesures relatives :

- à l'analyse et la gestion des risques, ainsi qu'à la sécurité des systèmes d'information ;
- à la gouvernance : responsabilisation des organes de direction et mise en place d'une politique de formation aux enjeux de sécurité ;
- au devoir d'information : obligation de prévenir l'ANSSI* en cas d'incident.

Au-delà des entités visées, NIS2 a un effet en cascade car les entreprises doivent évaluer et gérer les risques liés aux tiers.

La directive CER complète ce dispositif en imposant des exigences similaires, tout en se concentrant sur la sécurité physique des secteurs jugés critiques.

Quelles structures sont visées par NIS2 ?

Les acteurs dits « essentiels » ou « importants » :

- À partir de 50 salariés ou chiffre d'affaires supérieur à 10M€.
- 18 secteurs critiques : énergie, transports, santé, fournisseurs numériques, alimentation …

Mon entreprise est-elle concernée ?
Accéder au simulateur de l'ANSSI ici :
https://monespacenis2.cyber.gouv.fr/simulateur

Quels risques en cas de non-conformité ?
(sous réserve de transposition de la directive en l'état)

- Sanctions financières ;
- Responsabilité des dirigeants : interdictions temporaires d'exercer.

L'AVIS DE L'EXPERTE

La directive NIS2 va également concerner les sous-traitants. Les petites entreprises seront directement impactées et devront renforcer leur niveau de résilience au risque cyber. On observe déjà une évolution dans ce sens depuis quelques années, à travers les progrès réalisés en matière d'hygiène informatique - un prérequis indispensable pour accéder à une assurance cyber.

CHRISTINE SINIBARDY,
Directrice Risques Techniques et Cyber, AXA France

CRA

Le règlement européen Cyber Resilience Act vise à renforcer la sécurité des produits numériques mis sur le marché en imposant aux fabricants et aux distributeurs des exigences en matière de cybersécurité.
Pour les entreprises utilisatrices, cela représente une avancée importante pour réduire les risques cyber, en limitant les failles de sécurité dès la phase de conception des produits.

Exemples de produits concernés par le CRA

- Produits physiques (hardware) : ordinateurs, smartphones, cartes graphiques, imprimantes…
- Produits logiciels (software) : logiciel comptabilité, jeux vidéo, logiciel de traitement de texte…

LOPMI

La loi d'orientation et de programmation du ministère de l'intérieur impose, depuis avril 2023, aux entreprises françaises de déposer plainte dans les 72 heures suivant la détection d'une attaque afin de pouvoir être indemnisées au titre de leur assurance cyber. L'objectif est d'encourager le signalement des incidents pour améliorer la capacité d'action des autorités et renforcer la lutte contre la cybercriminalité.

L'AVIS DE L'EXPERTE

Il est essentiel de porter plainte dès les premières heures d'une attaque, auprès d'une brigade de gendarmerie ou d'un commissariat de police. Au-delà de l'obligation légale — déposer plainte dans les 72 heures pour pouvoir être indemnisé par son assureur —, cette démarche permet aussi de lutter contre la cybercriminalité en France, en donnant à nos services les moyens d'enquêter et de démanteler les organisations criminelles.

CÉCILE AUGERAUD,
Cheffe adjointe de l'Office anti-cybercriminalité (OFAC)

JONATHAN DRIKES,
Responsable Souscription Cyber, AXA XL France

L'AVIS DE L'EXPERT

Les grandes entreprises étaient déjà sensibilisées à la menace cyber avant l'arrivée de nouvelles réglementations comme NIS2 et ont mis en place des mesures de protection depuis plusieurs années. Ces réglementations devraient avoir un impact plus marqué sur les structures de plus petites tailles et/ou celles dont les secteurs d'activité n'étaient pas concernés par NIS1 telles que les activités de Production chimique et alimentaire, les administrations publiques ou de transports.

Focus sur les normes et certifications : un levier intéressant pour démontrer sa maturité en termes de cybersécurité.

Au-delà des obligations légales, adopter des normes reconnues comme celles de l'ISO ou de l'AFNOR reste une démarche volontaire susceptible de renforcer la confiance des clients et des partenaires.

Il peut être utile de se faire accompagner pour obtenir ces normes et certifications, qui peuvent sembler complexes au premier abord.

- **ISO 27001 :** norme internationale sur la mise en place d'un système de management de la sécurité de l'information ;
- **ISO 22301 :** norme internationale sur la mise en place d'un système de management de continuité d'activité ;
- **Certifications sur la cybersécurité proposées par l'AFNOR**, adaptées aux réalités françaises.

L'AVIS DE L'EXPERT

Si ces normes et certifications semblent incontournables pour les grandes entreprises, elles constituent également un levier stratégique pour les PME évoluant dans des environnements sensibles ou fortement interconnectés. Elles attestent d'un bon niveau de maturité en cybersécurité, renforcent la confiance des clients et partenaires et contribuent à répondre aux exigences croissantes des donneurs d'ordres.

JEAN-PIERRE MARBAIX,
Ingénierie Prévention Cyber, AXA France

En bref, ce qu'il faut retenir :

→ **La réglementation européenne se durcit et concerne de plus en plus d'entreprises** — directement ou via leurs relations commerciales — alors qu'elle ne visait auparavant que certains secteurs ou grandes structures.

→ **Se conformer à la réglementation permet :**
- d'être mieux préparé face aux attaques cyber ;
- d'éviter les sanctions ;
- de renforcer la confiance et la crédibilité auprès des clients et partenaires ;
- d'être indemnisé en cas d'attaque.

→ **Les normes et certifications** (ISO 27001, ISO 22301, AFNOR), bien que non obligatoires, constituent un gage de maturité et de sérieux.

État de la menace et préoccupations des chefs d'entreprise

La menace cyber progresse en France et cible de plus en plus les PME et les TPE, moins bien protégées que les grandes entreprises. Cette menace figure d'ailleurs en tête des principales préoccupations des dirigeants en France, selon le Baromètre AXA des chefs d'entreprise, paru en 2024.

À l'instar du reste du monde, la France connaît une intensification des cyberattaques. En 2024, près de la moitié des entreprises françaises ont été ciblées[1].

+15%

de cyberattaques en France en 2024[2].

37%

des attaques par rançongiciel visent les TPE, PME et ETI en 2024[2].

Les TPE et PME sont de plus en plus visées, avec une hausse des attaques de

+53%

en 2024[3].

L'AVIS DE L'EXPERT

Les attaques par rançongiciel figurent parmi les principales menaces pour les entreprises en France. Nous estimons que l'impact sur l'activité - c'est-à-dire la perte de marge brute - représente à lui seul environ 70% du coût total de ce type de sinistre.

JEAN-PIERRE MARBAIX,
Ingénierie Prévention Cyber, AXA France

(1) OpinionWay pour CESIN, Baromètre de la cybersécurité des entreprises, 2025 ; (2) ANSSI, Panorama des cybermenaces 2024 ; (3) Orange Cyberdefense, Security Navigator 2025

Certains facteurs renforcent l'exposition des entreprises au risque cyber.

Le recours à des prestataires externes, utilisés par

88%

des entreprises en 2024[1], expose davantage aux attaques.

Les petites structures qui hébergent leurs données dans le cloud pensent parfois que celles-ci sont automatiquement protégées, alors qu'elles sont de plus en plus ciblées par les cybercriminels. Cette perception s'explique notamment par le caractère récent de ces solutions et par le fait qu'elles ne les maîtrisent pas encore parfaitement.

LUC DECLERCK,
Directeur Général, Board of Cyber

L'AVIS DE L'EXPERT

Une attaque en 2025 contre un éditeur de logiciel a montré à quel point les entreprises peuvent être exposées via leurs prestataires. En quelques heures, des données sensibles ont été compromises et des milliers d'entreprises clientes ont vu leurs services paralysés, avec des répercussions pour des centaines de milliers de clients finaux.

En 2022,

79%

des entreprises ayant des informations hébergées dans le cloud ont subi au moins une violation de ces systèmes[2].

Malgré l'ampleur de la menace, les TPE et les PME françaises pensent être à l'abri des attaques.

62%

des TPE-PME pensent être faiblement exposées aux cyberattaques ou l'ignorent[3].

Les TPE et PME restent encore peu préparées face au risque cyber.

78%

des entreprises se disent insuffisamment préparées ou l'ignorent[3].

(1) SoSafe, Tendances en cybercriminalité, 2025 ; (2) Bessé & Stelliant, Risques cyber, Analyse de la sinistralité : quels enseignements ? Octobre 2022 ; (3) Cybermalveillance.gouv.fr, Etude de notoriété auprès de TPE & PME, Opinionway, 2024 Baromètre de la cybersécurité des entreprises, 2025

Les TPE et PME allouent des budgets très faibles à leur sécurité informatique. La quasi-totalité ne prévoit d'ailleurs pas de recrutement en cybersécurité pour 2025[1].

En 2024, 68% d'entre elles allouent moins de

2 000€

à leur sécurité informatique[1].

L'AVIS DE L'EXPERTE

Afin de répondre à l'intensification des menaces, l'ANSSI recommande aux entreprises d'allouer au moins 5 à 10% de leur budget informatique à la cybersécurité[2].

RÉBIAH BARDOT-GIRARD,
Chief Risk Consulting Officer, Cyber, AXA XL, a division of AXA

CHRISTINE SINIBARDY,
Directrice Risques Techniques et Cyber, AXA France

L'AVIS DE L'EXPERTE

Les petites entreprises sont encore très peu assurées contre le risque cyber. Elles se sentent peu concernées, estimant qu'elles sont trop petites pour intéresser les cybercriminels. Pourtant, elles sont de plus en plus victimes d'attaques de masse, qui ne ciblent plus une entreprise en particulier. Certaines sont même visées en tant que sous-traitantes, afin d'atteindre indirectement leur donneur d'ordres.

Très peu d'entreprises disposent aujourd'hui d'une assurance cyber, à l'exception des grandes entreprises, qui sont majoritairement couvertes.

Seules

10%

des ETI françaises étaient couvertes contre les cyberattaques en 2022, 3,2% des entreprises moyennes et 0,2% des petites et micro-entreprises[3].

On constate cependant des signaux positifs, avec une évolution de la couverture des entreprises de taille intermédiaire (+32% en 2024) et des entreprises de taille moyennes (+33%)[4].

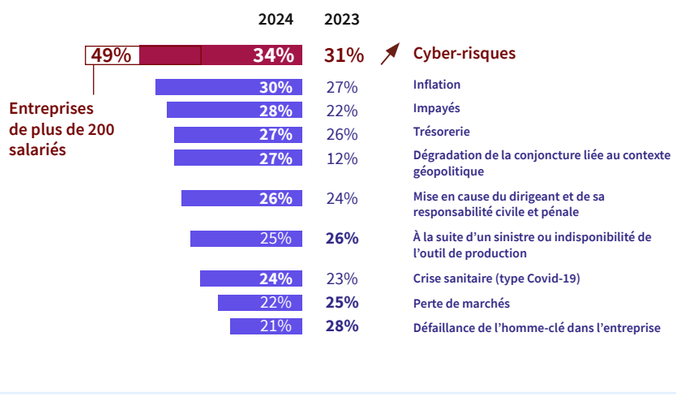
(1) Cybermalveillance.gouv.fr, Etude de notoriété auprès de TPE & PME, Opinionway, 2024 ; (2) Rapport ANSSI 2024 ; (3) AMRAE, étude Lucy 2023 ; (4) AMRAE, étude Lucy 2025
(Entreprises de taille intermédiaire : 50 millions < CA < 1 milliard € ; Entreprises de taille moyenne : 10 millions < CA > 50 millions € ; Petites et micro-entreprises : CA<10M€)

Baromètre des préoccupations des Chefs d'entreprise 2024[1]

Chaque année, AXA publie avec Kantar le Baromètre des préoccupations des chefs d'entreprise. Cette enquête, effectuée auprès de plus de 500 dirigeants d'entreprises de 10 à 500 salariés, évalue leurs préoccupations et leurs besoins en termes d'assurance.

En 2024, le risque cyber est la première préoccupation des chefs d'entreprise.

Quels risques vous inquiètent le plus ?



Le fait de détenir une assurance cyber rend les chefs d'entreprise plus sereins :

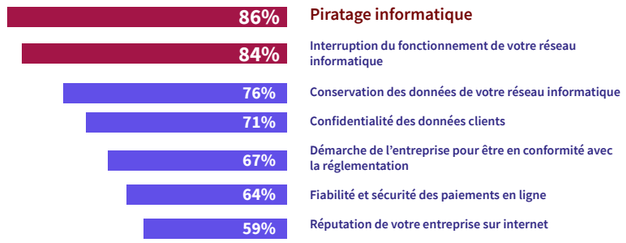
29% des clients AXA couverts sont préoccupés par les risques cyber, contre 34% des répondants au global.

58% **des entreprises souhaitent mieux maîtriser les risques cyber afin d'en réduire l'impact (vs 51% en 2023).**

Les risques cyber préoccupent davantage les chefs d'entreprise que les risques physiques, comme les risques d'accidents dans l'entreprise (52%) ou les risques routiers (51%).

Parmi les risques cyber, la menace la plus redoutée est le piratage informatique, suivi par l'interruption du réseau informatique.

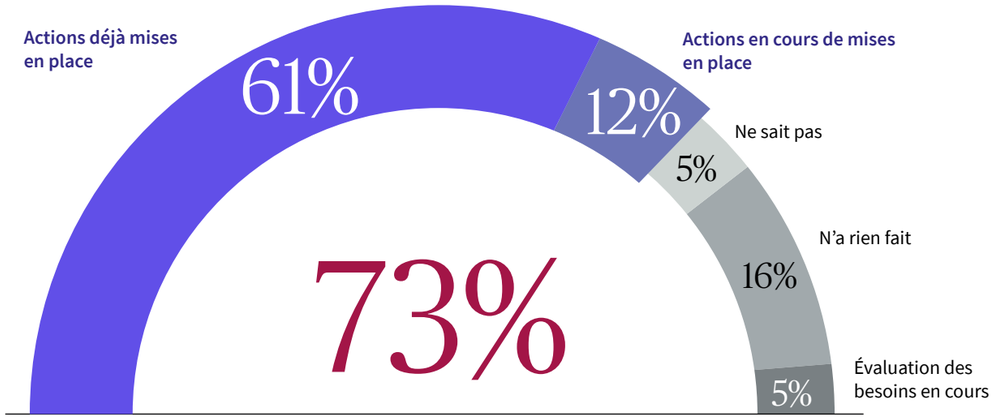
Quels sont les sujets liés aux risques cyber qui vous préoccupent le plus ?



(1) Baromètre AXA des préoccupations des chefs d'entreprise, Kantar, 2024

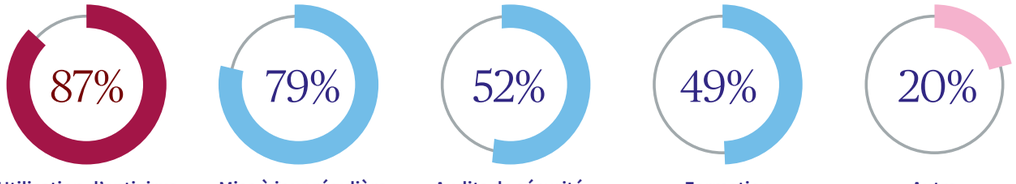
Les entreprises cherchent des solutions pour se protéger contre le risque cyber.

Dans quelle mesure votre entreprise est-elle préparée pour faire face aux risques cyber ?



des entreprises déclarent avoir renforcé leur sécurité informatique par des actions concrètes.

Si certaines actions de protection sont largement répandues, d'autres restent encore insuffisamment déployées…



37%

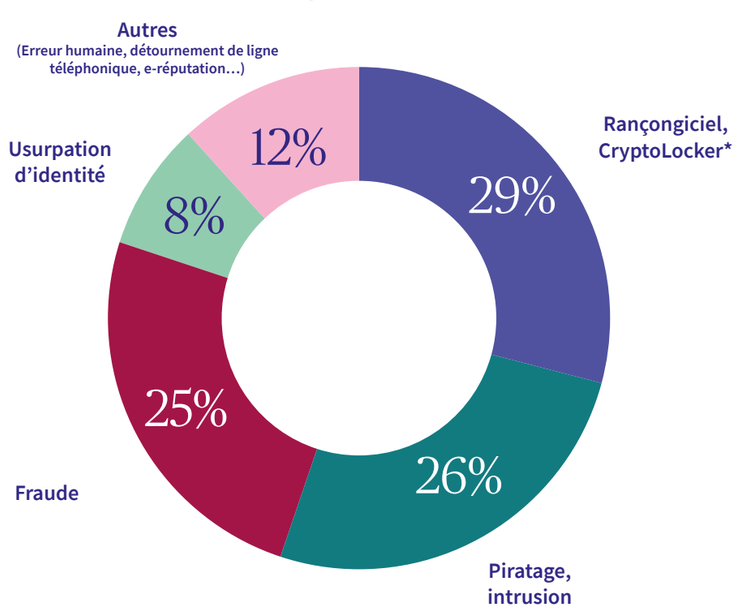
des chefs d'entreprise sont intéressés par un service offert par leur assureur pour tester la sécurité et l'inviolabilité de sites et outils internet.

Chiffres clés de la sinistralité cyber : l'observatoire d'AXA France

Mené par AXA France, l'observatoire des sinistres cyber analyse les incidents clos en 2024 au sein de son portefeuille client, quelle que soit l'année de survenance du sinistre. Cette étude offre un éclairage concret sur les attaques subies et les enseignements à tirer pour s'en prémunir.

1 Les rançongiciels arrivent en tête des sinistres enregistrés, suivis de près par les piratages / intrusions et la fraude.(1)

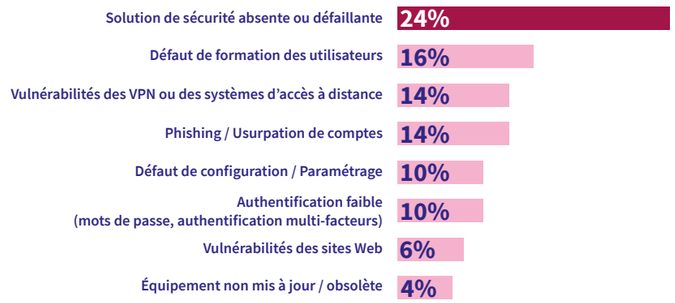
Typologie de sinistres (%)



(1) Base : sinistres clos en 2024, quelle que soit l'année de survenance de l'incident

2 L'absence ou la défaillance des solutions de sécurité constitue la principale vulnérabilité exploitée par les attaquants.(1)

Les principales vulnérabilités exploitées (%)



Dans près d'un quart des cas, les incidents sont liés à des solutions de sécurité absentes/défaillantes (pare-feu manquant ou mal configuré, mises à jour non effectuées…). Viennent ensuite le défaut de formation des utilisateurs, les accès distants non sécurisés et le phishing.

3 À la suite d'une attaque par rançongiciel, les délais de reprise de l'activité varient fortement selon la taille et le secteur de l'entreprise.

- La durée totale d'interruption d'activité atteint **6 jours en moyenne**, mais elle varie fortement – **de 1 à 43 jours** en fonction de la taille et du secteur d'activité de l'entreprise, ainsi que de la présence ou non d'une sauvegarde exploitable.
- Le délai de retour de l'activité à la normale est de **16 jours en moyenne**, avec de forts écarts - **1 à 111 jours**.

  Les délais de retour de l'activité à la normale varient selon le degré de maturité en termes de cybersécurité – généralement plus longs pour les petites structures, moins préparées aux attaques. Certains secteurs requièrent également plus de temps pour reprendre un rythme d'activité normal.

  Dans 17% des incidents observés suite à une attaque par rançongiciel, les sauvegardes ont été compromises, allongeant significativement le délai de retour à la normale.

En synthèse

Les rançongiciels, les piratages / intrusions et la fraude représentent 80% des sinistres enregistrés.

Les attaquants exploitent soit une vulnérabilité technique (absence d'une solution de sécurité, faille d'une solution de sécurité), soit les vulnérabilités humaines.

(1) Base : sinistres clos en 2024, quelle que soit l'année de survenance de l'incident

SOMMAIRE

Cyber-résilience : adopter une démarche **progressive** pour faire face aux **menaces**

03

Des différences de maturité **face au risque cyber**

Les niveaux de maturité en termes de cyber-résilience sont loin d'être homogènes et varient fortement selon la zone géographique, la taille et le secteur d'activité des entreprises.

35%

des petites entreprises considèrent leur cyber-résilience insuffisante en 2025, soit sept fois plus qu'en 2022[1].

7%

des grandes organisations jugent leur cyber-résilience insuffisante en 2025, soit deux fois moins qu'en 2022[1].

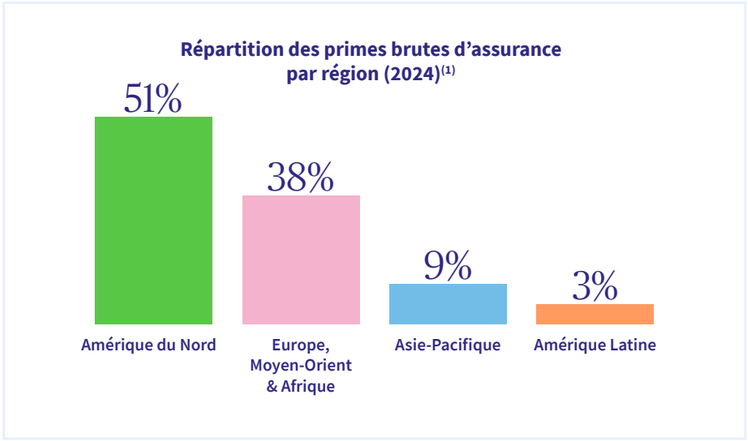
Cyber-résilience et cybersécurité : de quoi parle-t-on ?

Selon le National Institute of Standards and Technology (NIST), **la cyber-résilience désigne la capacité d'une organisation à anticiper, résister, récupérer et s'adapter** face à des conditions défavorables, de stress, des attaques ou des compromissions affectant des systèmes qui utilisent ou sont activés par des ressources cybernétiques.

Elle vise à garantir la continuité des activités, même dans un environnement numérique perturbé ou hostile. **La cybersécurité**, qui protège les systèmes et les données contre les attaques, **est une composante de la cyber-résilience**.

(1) World Economic Forum & Accenture, Global Cybersecurity Outlook 2025

Des niveaux de maturité différents selon les régions



Le volume des primes d'assurance cyber progresse significativement tout en restant concentré en Amérique du Nord et en Europe. Ces régions, plus matures, proposent en effet ce type de couverture depuis de nombreuses années.

Les régions Asie-Pacifique et Amérique latine, encore loin derrière, devraient toutefois enregistrer une progression rapide dans les prochaines années, portée par une amélioration progressive de leur maturité cyber.

Des grandes entreprises beaucoup mieux protégées que les TPE/PME

L'AVIS DE L'EXPERT

FRÉDÉRIC COPPIN,
Directeur Technique et Souscription Grands comptes, AXA France

Les grandes entreprises sont généralement mieux protégées face aux cyberattaques, grâce à une culture de la cybersécurité bien ancrée et des équipes dédiées. À l'inverse, les TPE et PME restent très vulnérables et ont subi une forte hausse des attaques en 2024 (+53 %)(3). Cette exposition s'explique en grande partie par la fragilité technique de leurs infrastructures. Plus préoccupant encore, de nombreuses PME se croient protégées parce qu'elles externalisent leurs systèmes informatiques. Or, cette externalisation ne garantit pas toujours une sécurité suffisante et ne les met pas à l'abri en cas d'attaque.

(1) Cyber Insurance Market Outlook 2025: Cycle Management Will Be Key To Sustaining Profits - SAP Global Ratings ; (3) Orange Cyberdefense, Security Navigator 2025

Cyber-résilience : adopter une démarche progressive pour faire face aux menaces

Des différences de maturité selon les secteurs d'activité

L'AVIS DE L'EXPERTE

VANESSA LEEMANS,
Head of Cyber, UK & Lloyd's, AXA XL, a division of AXA

Dans des secteurs fortement réglementés comme la finance ou la santé, les entreprises doivent répondre à des exigences strictes en matière de cybersécurité, en raison de la sensibilité des données qu'elles traitent et du caractère critique des services qu'elles fournissent, ce qui renforce leur niveau de cyber-résilience.

Certains secteurs, comme l'industrie manufacturière, font l'objet d'un contrôle accru et doivent mettre en place des mesures de sécurité renforcées pour protéger leurs technologies opérationnelles et leurs chaînes d'approvisionnement.

Au Royaume-Uni, les budgets consacrés à la cybersécurité sont globalement en hausse tous secteurs confondus, bien que certaines entreprises limitent leurs investissements dans un contexte économique contraint.

Les montants alloués dépendent de la taille de l'entreprise, de son niveau de maturité et de son évaluation des risques.

Celles dont la maturité cyber reste faible doivent aujourd'hui intensifier leurs investissements en matière de cybersécurité.

Pourquoi des entreprises restent-elles sous-protégées face au risque cyber ?

Les petites entreprises prennent peu à peu conscience du risque, mais en sous-estiment encore trop fréquemment les enjeux. Elles considèrent souvent qu'elles sont trop petites pour être ciblées et reconnaissent leur faible niveau de préparation.

1 Manque de temps

Les contraintes de temps sont régulièrement mises en avant par les petites entreprises lorsqu'elles évoquent les freins pour atteindre un bon niveau de cybersécurité.

2 Manque d'expertise

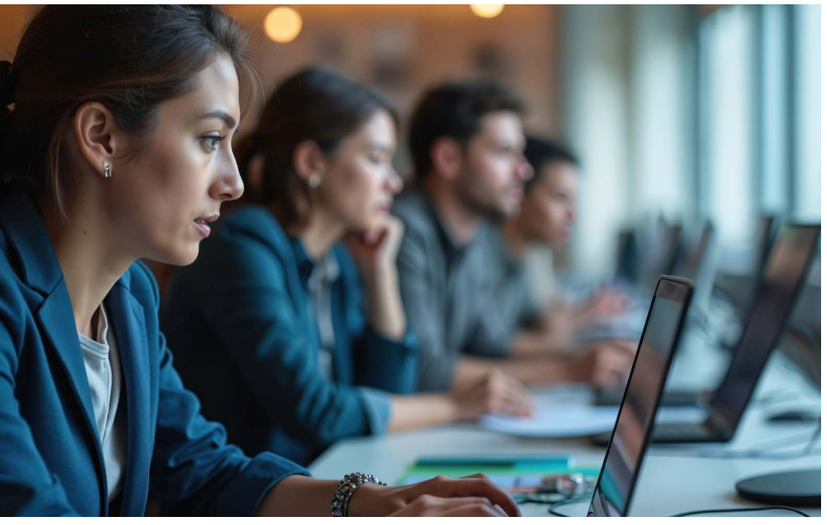
Les entreprises ne disposent pas toujours d'un niveau de connaissance et d'expertise suffisant pour identifier les risques et définir une stratégie de cybersécurité adaptée.

3 Manque de budget

Les investissements en cybersécurité sont parfois perçus comme des coûts additionnels, arbitrés au profit de dépenses jugées prioritaires.

4 Méconnaissance des systèmes de protection

De nombreux dirigeants pensent, à tort, être couverts dans le cadre d'autres contrats d'assurance, comme la Responsabilité Civile Professionnelle. De plus, il semble complexe d'identifier les outils de cybersécurité adéquats, souvent perçus comme inaccessibles ou inadaptés aux petites structures.



Le manque de compétences en cybersécurité demeure un défi pour la protection des entreprises. On estime qu'il manquerait environ 2,8 millions d'experts dans le monde. 59% des responsables de la cybersécurité considèrent cette pénurie de talents comme un obstacle majeur à la sécurité de leur organisation. La majorité des postes vacants se situent en Asie-Pacifique (plus de 1,5 million), suivie par l'Amérique et l'Europe[1].

(1) BCG & Global Cybersecurity Forum, 2024 Cybersecurity workforce report: Bridging the Workforce Shortage and Skills Gap

Cyber-résilience : adopter une démarche progressive pour faire face aux menaces

Des signaux positifs malgré tout, témoignant d'une dynamique encourageante

La médiatisation des attaques et le contexte géopolitique ont contribué à renforcer la prise de conscience des entreprises.

En France en 2024 les souscriptions d'assurance cyber ont progressé de 32% chez les ETI et de 33% chez les entreprises de taille moyenne[1].

Les dépenses mondiales en cybersécurité devraient atteindre 262 milliards en 2030, contre 196 milliards en 2025, augmentant de 33% en cinq ans[2].

L'AVIS DE L'EXPERTE

La cyber-résilience est un processus continu d'amélioration et d'adaptation, même pour les organisations matures. Cette exigence s'explique par l'évolution permanente des menaces, qui oblige les entreprises à investir sans relâche dans des outils et des ressources pour se protéger, réduire les risques et limiter les impacts des incidents.

MICHELLE CHIA,
Chief Underwriting Officer Cyber, Design & Select Professional, Americas, AXA XL, a division of AXA

(1) AMRAE, Etude LUCY, 2025 – ETI : chiffre d'affaires compris entre 50M et 1md€ et entreprises de taille moyenne : chiffre d'affaires compris entre 10M et 50M€ ; (2) Worldwide Security Spending, IDC, 2025

Construire un socle de sécurité : la cyber hygiène comme première ligne de défense

À l'heure où la plupart des cyberattaques exploitent des failles techniques ou humaines, la mise en œuvre de fondamentaux de sécurité constitue un prérequis indispensable pour initier une démarche de cybersécurité efficace.

200 000$

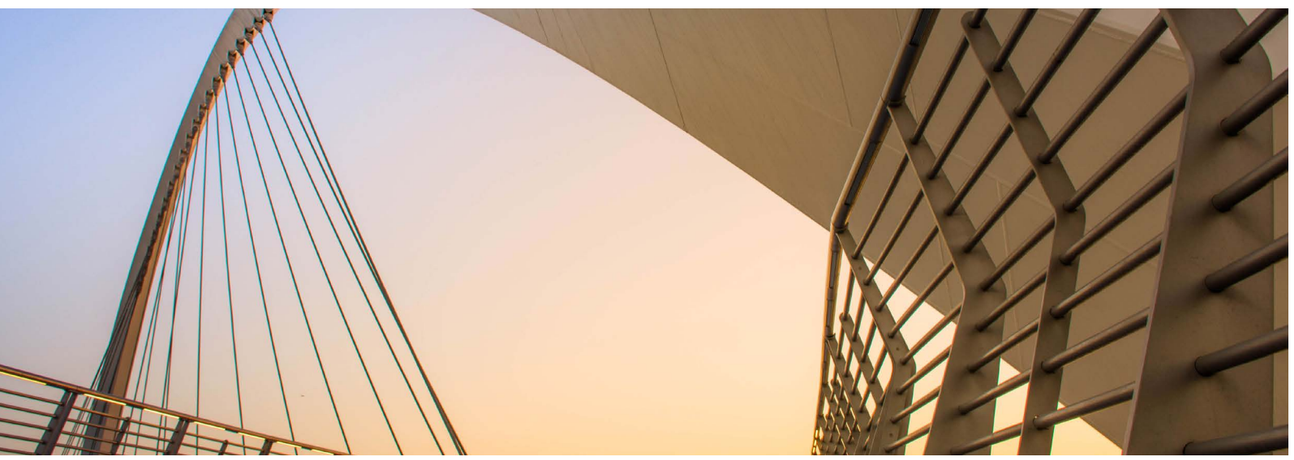
budget médian alloué à la cybersécurité par les PME dans le monde. Il atteint 5,7M$ pour les grandes entreprises. Cela représente un peu plus de 13% du budget informatique annuel[1].

35%

des violations de données en 2024 impliquent des ressources non surveillées ou non répertoriées, échappant aux contrôles de sécurité[2].

72%

des entreprises françaises estiment que l'usage massif par leurs salariés de services cloud non approuvés représente un risque élevé pour la sécurité[3].



(1) Rapport Kaspersky sur l'Économie de la Sécurité Informatique (IT Security Economics), 2024 ; (2) IBM, Cost of a data breach, 2024 ; (3) Baromètre de la cybersécurité des entreprises, Opinionway pour CESIN, 2025

Adopter une bonne hygiène informatique, c'est comme fermer les portes à clé : cela n'empêche pas toutes les intrusions, mais décourage la majorité des attaques opportunistes. **Des mesures simples et peu coûteuses réduisent considérablement l'exposition aux risques cyber et les impacts des incidents.** Pour être efficaces, les collaborateurs doivent y être sensibilisés.

1 Identifier les ressources exposées, pour savoir ce qui doit être protégé

De nombreuses entreprises ignorent qu'une partie de leurs outils est directement accessible sur Internet — et donc aux cybercriminels. Sites web, plateformes cloud, accès à distance pour les employés ou prestataires : chaque service exposé est une porte d'entrée potentielle. Pourtant, un simple inventaire permet de réduire considérablement les risques.

Que faire concrètement ?

Répertorier les systèmes connectés à Internet : sites internet, plateformes cloud, accès à distance, interfaces pour les prestataires, etc.

Recenser les équipements et outils utilisés : serveurs, postes de travail, logiciels, etc., sans oublier ceux qui ont été installés par les collaborateurs sans validation officielle, pour éviter le shadow IT*.

Mettre à jour régulièrement cet inventaire : réviser la cartographie au minimum une fois par an ainsi qu'à chaque changement organisationnel, lancement de projet ou arrivée de nouveaux prestataires.

En 2023, l'Atlantic General Hospital a subi une attaque par rançongiciel exploitant une application oubliée et mal sécurisée. L'incident a exposé les données personnelles de 137 000 patients et s'est soldé par un règlement judiciaire de 2,25 millions de dollars, à la suite d'un recours collectif[1].

Zoom sur le shadow IT, un risque souvent sous-estimé

Le shadow IT désigne tous les logiciels, services ou équipements utilisés sans l'approbation du service informatique. Il peut s'agir d'un collaborateur qui crée un compte sur une plateforme cloud pour partager des fichiers ou d'une équipe qui installe un outil SaaS* sans en informer personne. Bien que souvent motivé par un besoin de productivité, ce phénomène crée des failles de sécurité, car ces outils échappent aux mises à jour, contrôles et sauvegardes de l'entreprise.

(1) Bank Info Security, août 2024

2 — Sécuriser les accès et les systèmes critiques pour contrer les intrusions les plus fréquentes

Dans la majorité des attaques, les cybercriminels ne « forcent » pas l'entrée : ils exploitent des accès ouverts ou mal protégés. Identifiants compromis, mots de passe faibles, terminaux mal sécurisés ou serveurs exposés sont les points d'entrée privilégiés pour pénétrer un réseau. Pour une entreprise — quelle que soit sa taille — la priorité est donc de renforcer la protection des accès sensibles et de sécuriser les systèmes critiques.

Quels sont les fondamentaux à mettre en place ?

Adopter des mots de passe robustes et uniques pour chaque usage — ou recourir à un coffre-fort dédié — est une mesure de base indispensable pour protéger les accès sensibles tels que les emails, ERP*, VPN*.
Cette première barrière doit être complétée, dès que cela est possible, par une authentification renforcée* (MFA), qui combine au moins deux facteurs d'identification – par exemple un mot de passe et un code reçu sur mobile.
Pour des situations à haut risque il peut être utile de mettre en place une MFA avancée, incluant par exemple la vérification biométrique.

Qu'est-ce qu'un mot de passe robuste ?

- ✓ Il comporte au moins 12 signes ;
- ✓ Il mélange majuscules, minuscules, chiffres et caractères spéciaux ;
- ✓ Il est impossible à deviner : pas d'informations personnelles ni de suites logiques.
- ✓ Il est essentiel de sensibiliser les salariés à la gestion de leurs mots de passe.

Contrôler les droits d'accès en appliquant le principe du « moindre privilège »: limiter les droits d'accès au strict nécessaire pour chaque employé, et révoquer les accès des ex-collaborateurs.

Renforcer la protection des équipements:
- Installer un pare-feu ;
- Activer les protections intégrées aux systèmes d'information (par exemple l'antivirus de Windows ou macOS) ;
- Équiper les terminaux (PC, smartphones, tablettes) de solutions antivirus, et chiffrer les données.

En 2024, seules **45%** des TPE et PME françaises ont déployé des solutions de sécurité telles que des pare-feux ou des antivirus - des chiffres en recul par rapport à 2023(1).

Au Royaume-Uni, **61%** des entreprises utilisent un antivirus et **55%** ont mis en place un pare-feu(2).

Sauvegarder régulièrement les données stratégiques (commandes, contrats, etc), selon la règle du 3-2-1 :
- conserver **3 copies** des données
- sur **2 supports différents** (disque dur, cloud…)
- dont **au moins 1 copie hors ligne et isolée du réseau**

Les sauvegardes doivent faire l'objet de tests de restauration réguliers pour vérifier qu'elles sont bien exploitables.

(1) Afnic, Etude 2024 Réussir avec le web ; (2) Cyber magazine, Howden: How Cyber Attacks cost UK Companies $55bn in 5 Years, novembre 2024

L'AVIS DE L'EXPERTE

Pour être efficaces, les dispositifs de sécurité doivent rester discrets et fonctionner en arrière-plan de manière automatique, afin de ne pas alourdir le quotidien des collaborateurs.

GWENAËLLE MARTINET,
Directrice de l'offre cybersécurité, groupe Docaposte

Cas d'une entreprise lourdement pénalisée par l'absence de sauvegarde déconnectée(3)

Cette entreprise industrielle, réalisant un chiffre d'affaires annuel de 17 millions d'euros, a été victime d'une attaque par rançongiciel. L'attaquant a réussi à chiffrer l'unique sauvegarde hébergée sur un équipement NAS (serveur de stockage et de partage de fichiers) connecté en permanence au réseau.

Faute de sauvegarde déconnectée, l'entreprise a subi un arrêt total de ses activités pendant **10 jours**, suivi d'une reprise progressive en mode dégradé. Il a fallu **65 jours** pour rétablir l'ensemble des services informatiques.

Le montant du sinistre s'est élevé à **1,3 M€** comprenant les heures supplémentaires pour reconstituer les données, les frais de reconstruction du système d'information, les frais de gestion de crise et le coût lié à la perte d'exploitation.

(3) AXA France

SOMMAIRE

3 — Organiser la gestion préventive des mises à jour et de l'obsolescence du parc informatique

Fermer les brèches… avant qu'elles ne soient exploitées. Le parc informatique d'une entreprise - logiciels et équipements - peut comporter des vulnérabilités exploitées par les cybercriminels. Les logiciels présentent régulièrement des failles, qu'il faut corriger par des mises à jour de sécurité. Certains équipements, devenus obsolètes, ne bénéficient plus de correctifs, ce qui augmente le niveau de risque.

En 2024, seules **41%** des TPE et PME françaises procèdent régulièrement aux mises à jour des correctifs de sécurité[1].

Que faut-il faire concrètement ?

Mettre en place une procédure de patch management* pour organiser et suivre les mises à jour de sécurité ;
Désigner un responsable chargé de surveiller les mises à jour, les tester et déployer les correctifs dès leur publication.

Supprimer les logiciels et équipements obsolètes ou inutilisés ;
Ils ne sont plus maintenus par leurs éditeurs ou fabricants et constituent des portes ouvertes pour les attaquants.

Surveiller les bulletins d'alerte des éditeurs.
S'abonner aux notifications de sécurité pour être averti dès qu'une faille critique est signalée.

4 — Encadrer les prestataires pour éviter qu'ils ne servent de porte d'entrée aux cyberattaquants

Les prestataires informatiques et les sous-traitants jouent un rôle essentiel dans l'activité d'une entreprise, mais ils représentent aussi un risque. En effet, ils disposent souvent d'accès étendus aux systèmes, qui peuvent être ciblés par des cybercriminels pour atteindre l'entreprise. Il est donc impératif d'identifier les vulnérabilités qui peuvent en découler.

Quelles sont les bonnes pratiques à adopter ?

Vérifier les standards de sécurité des partenaires :
quelles mesures appliquent-ils (MFA, sauvegarde, surveillance, etc) ?

Limiter les droits d'accès au strict nécessaire :
ne donner accès qu'aux ressources indispensables pour leur mission, et révoquer immédiatement les accès en fin de contrat ou de mission.

Séparer les espaces de collaboration externes des systèmes critiques,
pour limiter l'impact en cas de compromission d'un prestataire.

(1) Afnic, Etude 2024 Réussir avec le web

5 — Surveiller les activités pour détecter à temps les signes d'intrusion

Une intrusion n'est pas toujours immédiate et visible. Dans de nombreux cas, les cybercriminels restent plusieurs jours — voire semaines — dans un système avant de déclencher leur attaque. Une surveillance continue permet de détecter ces comportements suspects et d'agir avant que des dégâts majeurs ne surviennent.

Les organisations qui utilisent largement l'intelligence artificielle et l'automatisation de la sécurité détectent et maîtrisent les incidents beaucoup plus rapidement que celles qui n'utilisent pas ces technologies, réduisant le temps moyen de gestion des violations de 80 jours et diminuant le coût moyen d'une violation de 1,9 million de dollars[1].

Activer la journalisation :
configurer les systèmes (serveurs, réseaux, applications) pour enregistrer les événements clés : connexions, transferts de fichiers, créations de comptes, élévations de privilèges… Ces journaux permettent de repérer des comportements anormaux ou d'analyser un incident a posteriori.

Mettre en place des alertes :
définir des seuils d'alerte sur les activités sensibles (connexion en dehors des horaires habituels, transfert massif de données, tentatives d'accès non autorisés, etc) pour être averti en temps réel d'une anomalie.

Pour aller plus loin, l'EDR*(Endpoint Detection & Response) managé, une surveillance renforcée

Une fois les bonnes pratiques de base en place, les entreprises peuvent renforcer leur protection grâce à un EDR managé.

L'EDR managé surveille en temps réel les terminaux (ordinateurs, serveurs, smartphones), détecte des comportements anormaux et déclenche des mesures pour limiter les impacts.

Cette solution est externalisée chez un prestataire spécialisé qui assure l'installation, la surveillance, l'analyse et le traitement des alertes pour l'entreprise.

(1) IBM, Cost of a data breach, 2025

Anticiper la menace : élaborer une stratégie de prévention sur le long terme

Une fois les fondamentaux de sécurité en place, il s'agit de définir une stratégie de prévention inscrite dans une démarche d'amélioration continue et ancrée dans la culture d'entreprise. Elle associe des mesures techniques, mais également organisationnelles, managériales, humaines et de conformité.

53%

des entreprises françaises de plus de 50 salariés ont désigné un référent cybersécurité en 2024[1].

62%

des entreprises françaises ont mis en place un programme d'entraînement à la crise cyber en 2024[2].

(1) Visiativ, Baromètre de la cybersécurité des entreprises françaises, 2024 ; (2) Baromètre de la cybersécurité des entreprises, Opinionway pour CESIN, 2025

La prévention s'appuie sur cinq piliers essentiels, à mettre en place progressivement pour renforcer durablement la cybersécurité de l'entreprise.

1 — Définir une gouvernance claire, soutenue par la direction, pour piloter la cybersécurité

Un pilotage structuré de la cybersécurité permet de prioriser les risques les plus critiques, d'allouer les moyens adéquats et d'assurer un suivi régulier. Il permet également de garantir la conformité réglementaire de l'entreprise.

- **Désigner un responsable cybersécurité**
  Même dans les petites structures, il est indispensable d'identifier un interlocuteur chargé de piloter les actions et d'agir comme référent en cas d'incident. Il peut être externalisé.

- **Formaliser les politiques et procédures**
  Définir les priorités, les objectifs et les règles de sécurité sur les bases d'une analyse des risques et les diffuser aux acteurs concernés.
  La Direction Générale et la Direction des Ressources Humaines doivent être impliquées.

- **Allouer un budget dédié**
  La cybersécurité requiert un budget adapté au niveau de risque et à la taille de l'entreprise.
  Cela inclut les équipes, la formation, les outils et le recours éventuel à des prestataires spécialisés.

- **Suivre et contrôler dans le temps**
  Les enjeux liés à la cybersécurité évoluent en permanence avec la menace et les évolutions technologiques. Mettre en place des indicateurs de suivi et planifier des audits réguliers est essentiel pour s'assurer que les mesures restent adaptées et efficaces.

L'AVIS DE L'EXPERT

La menace cyber n'est plus seulement un enjeu technique ou de sécurité, elle relève désormais de la responsabilité du conseil d'administration, qui doit intégrer la résilience dans sa stratégie à long terme. Les réglementations européennes récentes, telles que NIS2 ou DORA, mettent en lumière ce changement en plaçant la responsabilité de la cybersécurité au sommet de la hiérarchie. Elles impliquent directement le conseil d'administration et la direction générale pour définir l'impulsion stratégique, approuver les politiques internes, garantir le respect continu des exigences réglementaires, et superviser la mise en œuvre de stratégies de cybersécurité efficaces, de pratiques de gestion des risques et de dispositifs de continuité d'activité.

CARLOS RODRIGUEZ SANZ,
Cyber Regional Product Leader APAC & Europe, AXA XL, a division of AXA

2 Prioriser les actions en fonction de la menace et des enjeux de l'entreprise

Toutes les entreprises présentent des failles, mais elles ne sont pas toutes exposées au même niveau de danger. Certaines peuvent être exploitées par des attaques paralysant des activités critiques et provoquant des pertes majeures, tandis que d'autres n'auraient que des conséquences limitées. Il est donc essentiel d'évaluer les risques pour hiérarchiser les priorités et concentrer les efforts là où ils auront le plus d'impact.

Que faut-il faire concrètement ?

Cartographier les systèmes et les processus critiques
s'appuyer sur l'inventaire des ressources exposées aux risques cyber (systèmes connectés à internet, équipements, outils, logiciels y compris le Shadow IT) et prioriser ce qui est vital pour assurer la continuité des opérations.

Réaliser régulièrement des audits et des diagnostics techniques
scans des vulnérabilités, tests d'intrusion, audits des configurations systèmes – pour identifier les vulnérabilités dans la durée.

Évaluer les scénarios de risques
types d'attaques probables, conséquences économiques, réglementaires, réputationnelles, etc.

Définir un plan d'action concret
en priorisant les vulnérabilités selon leur niveau de gravité.

Suivre les menaces
mettre en place une veille sur les menaces émergentes (nouveaux types d'attaques, failles exploitées dans votre secteur) pour adapter la protection en permanence.

L'AVIS DE L'EXPERT

L'analyse des risques est essentielle : car chaque entreprise évolue dans un contexte spécifique, avec des enjeux et des priorités en termes de cybersécurité qui lui sont propres. C'est cette analyse qui permet de définir un niveau de protection et de prévention adapté face à la menace cyber.

JEAN-PIERRE MARBAIX,
Ingénierie Prévention Cyber, AXA France

L'AVIS DE L'EXPERTE

Le modèle Zero Trust, de plus en plus adopté par les entreprises, s'impose comme une référence pour renforcer la sécurité. Il repose sur un principe simple : accorder la confiance uniquement après vérification. Chaque utilisateur ou appareil doit prouver son identité à chaque étape, les accès sont limités à ce qui est strictement nécessaire, et les différents systèmes sont cloisonnés pour réduire les risques.

RÉBIAH BARDOT-GIRARD,
Chief Risk Consulting Officer, Cyber, AXA XL, a division of AXA

Cyber-résilience : adopter une démarche progressive pour faire face aux menaces

3 Sensibiliser et former les collaborateurs pour qu'ils deviennent un rempart face aux attaques

Environ 90% des cyberattaques trouvent leur origine dans une erreur humaine[1]. Sensibiliser et former les salariés — y compris la direction — reste donc un levier essentiel pour limiter les incidents et adopter les bons réflexes face aux menaces.
La sensibilisation ne doit pas se limiter à des sessions ponctuelles : elle doit s'inscrire dans la durée et être intégrée aux processus des ressources humaines, dès l'accueil des nouveaux arrivants, puis tout au long de la carrière. L'objectif est de créer une véritable culture de la cybersécurité, partagée par tous.

Pour être efficaces, les actions doivent être variées, interactives et régulières :

Campagnes de sensibilisation aux risques cyber notamment pour les petites entreprises.

Formations ciblées sur les principales menaces : phishing, ingénierie sociale, signalement d'incidents…

Simulations d'attaques et exercices de crise, pour s'assurer de l'efficacité des formations et améliorer la réactivité des équipes (tests de phishing par exemple).

La formation des collaborateurs ne doit pas se limiter à leur profil professionnel. Avec l'essor du télétravail, les salariés utilisent de plus en plus leurs comptes et équipements personnels pour travailler. Or ces dispositifs, souvent moins bien sécurisés, constituent une porte d'entrée pour les cybercriminels, qui s'en servent pour infiltrer les systèmes de l'entreprise.

L'AVIS DE L'EXPERTE

Des tests de phishing réguliers sont recommandés pour renforcer la vigilance des collaborateurs. Un de nos clients a pu réduire les clics de ses collaborateurs vers des liens malveillants de 70% après six mois de formation.

MICHELLE CHIA,
Chief Underwriting Officer Cyber, Design & Select Professional, Americas, AXA XL, a division of AXA

Conseils pratiques à partager avec les collaborateurs pour repérer une tentative de *phishing*

- **Ne jamais répondre à un courriel demandant des informations personnelles ou confidentielles** (mot de passe, code, numéro de carte bancaire…) : aucun site fiable ne le demandera.
- **Si un courriel semble suspect, ne pas cliquer sur les pièces jointes ni sur les liens.** Saisir directement l'adresse officielle dans la barre du navigateur.
- Pour un paiement en ligne, **vérifier que l'adresse du site est sécurisée et commence par « https »** (attention : condition nécessaire mais pas suffisante).
- En cas de doute sur l'identité d'un contact, **encourager les collaborateurs à vérifier son identité par un appel vocal ou un autre canal.**

(1) francenum.gouv.fr

4 Encadrer la chaîne de valeur pour maîtriser les risques sur le long terme

Les prestataires et sous-traitants représentent aujourd'hui un maillon critique de la sécurité des entreprises. D'abord, parce qu'ayant accès aux systèmes d'information de leurs clients, ils peuvent servir de porte d'entrée aux cyberattaquants. Ensuite, un prestataire paralysé par une attaque ne pourra plus honorer ses engagements, ce qui peut impacter l'activité de ses donneurs d'ordre. Enfin, les réglementations récentes, comme NIS2 en Europe, renforcent cette exigence de vigilance en étendant la responsabilité des entreprises donneuses d'ordre pour les failles présentes chez leurs sous-traitants. Il est donc essentiel d'encadrer et de contrôler la chaîne de valeur pour en garantir la fiabilité et limiter les risques qu'elle représente.

Comment encadrer efficacement la chaîne de valeur ?

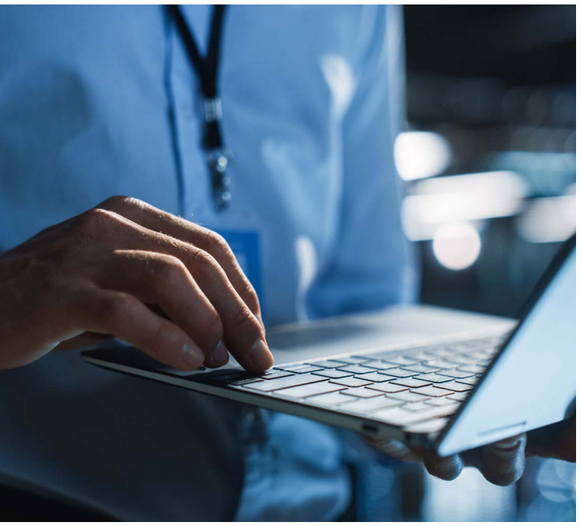
Sélectionner des partenaires fiables et audités : choisir des prestataires qui démontrent leur sérieux par des audits, certifications ou attestations de conformité (ISO 27001, SOC 2, …).

Diversifier la chaîne d'approvisionnement pour éviter de dépendre de quelques prestataires.

Intégrer des clauses contractuelles de sécurité : intégrer dans les contrats des obligations précises en matière de cybersécurité en détaillant les audits possibles, les niveaux attendus et les sanctions prévues en cas de manquement.

Maintenir à jour la liste de tous les partenaires externes qui travaillent avec l'entreprise pour disposer d'une vision à 360° en permanence.

En 2022, un prestataire de paie majeur aux Etats-Unis a été paralysé par une attaque par ransomware, laissant des centaines d'entreprises clientes incapables de verser les salaires de leurs salariés pendant deux semaines.



Cinq questions simples pour évaluer rapidement la cybersécurité d'un partenaire

Comment protégez-vous vos accès à nos systèmes ?
MFA activée, droits limités, surveillance des connexions, …

Mettez-vous régulièrement à jour vos systèmes et logiciels ?
Comment êtes-vous informés des vulnérabilités critiques ?

Quelles sont vos procédures en cas d'incident ?
Notification rapide, plan de réponse aux incidents, interlocuteur dédié.

Comment sauvegardez-vous vos données ? Pouvez-vous les restaurer ?
Fréquence des sauvegardes, stockage isolé, …

Pouvez-vous fournir des preuves de vos pratiques ?
Audits et certifications.

Cyber-résilience : adopter une démarche progressive pour faire face aux menaces

5 Souscrire un contrat d'assurance cyber

Une bonne hygiène informatique, l'externalisation des systèmes d'information et des mesures de prévention ne permettent pas d'empêcher 100% des attaques cyber, il subsiste toujours un risque que des cybercriminels parviennent à contourner les défenses. Une attaque peut alors menacer la continuité des activités et même la survie de l'entreprise.

L'assurance cyber vient ainsi compléter les mesures prises par les entreprises en interne ou par leurs prestataires informatiques, en apportant une double protection. Elle couvre les pertes financières en cas d'incident, par exemple en cas d'interruption d'activité, de vol ou de destruction de données. Elle permet aussi de mobiliser rapidement des experts en cybersécurité pour gérer la crise et relancer l'activité au plus vite.

Certains assureurs vont plus loin en proposant des services de conseil et des actions de prévention, pour aider les entreprises à mieux anticiper les risques et à réduire leur exposition aux attaques.

SOMMAIRE

Se préparer à l'incident : s'organiser pour limiter les impacts et améliorer sa résilience

Une hygiène informatique rigoureuse et une stratégie de prévention efficace ne suffisent pas à écarter totalement le risque d'une attaque cyber. Il est donc essentiel de préparer, en amont, la réponse de l'entreprise pour contenir la crise et relancer l'activité rapidement.

1M$

de perte évitée en moyenne par les entreprises victimes de ransomware ayant fait appel aux forces de l'ordre (hors rançon). Elles ont également identifié et contenu l'attaque plus rapidement[1].

62%

des entreprises françaises ont porté plainte à la suite d'une cyberattaque en 2024[2].

L'AVIS DE L'EXPERT

Pour les entreprises, une attaque cyber n'est plus une hypothèse, mais une réalité à anticiper. Se préparer - en construisant et en testant des scénarios de réponse – permet généralement de sortir plus vite de la crise, et d'en limiter les effets.

MATHIEU COUSIN,
Cyber Risk Consulting & Threat Intelligence Strategist, AXA XL, a division of AXA

(1) IBM, Cost of a data breach, 2024 ; (2) Baromètre de la cybersécurité des entreprises, Opinionway pour CESIN, 2025

Réagir efficacement en cas d'incident ne s'improvise pas. Cela requiert une préparation en amont, intégrée dans une démarche continue d'amélioration et fondée sur trois axes majeurs

1 — Préparer et activer l'organisation pour gérer la crise : anticiper, planifier et coordonner la réponse pour éviter la confusion lors d'un incident

En amont :

✓ **Elaborer un Plan de réponse aux incidents (PRI)**

Le PRI définit les étapes et les moyens pour réagir à un incident de cybersécurité.

Il est connu de tous les acteurs impliqués, régulièrement testé et mis à jour pour être opérationnel à tout moment.

Pendant l'incident

→ **Activer le PRI** dès la détection d'une attaque pour la contenir et protéger les actifs restants.

Qu'est-ce qu'un Plan de Réponse aux Incidents ?

Le PRI décrit comment détecter, analyser et contenir l'incident, en limiter les conséquences, restaurer les systèmes et tirer les enseignements de la crise. Il précise les rôles et responsabilités, les procédures à suivre et les contacts à mobiliser pour assurer une réponse rapide et coordonnée.

✓ **Définir une cellule de crise**

C'est une équipe pluridisciplinaire (direction, IT, juridique, communication) avec des responsables clairement désignés.

En fonction de l'organisation de l'entreprise, elle est composée d'interlocuteurs internes et/ou externes.

Elle est régulièrement formée à gérer différents scénarios d'incidents.

→ **Réunir la cellule de crise,** coordonner les décisions, suivre le plan tout en restant adaptable aux événements.

2 Assurer la continuité et la reprise des activités

En amont :

✓ **Mettre en place un Plan de Continuité d'Activité (PCA)***

Il permet de maintenir les services essentiels de l'entreprise, même en cas d'indisponibilité des ressources clés (systèmes d'information, systèmes industriels, prestataires, …).

Identifier les processus critiques et définir ce qu'il faut pour les maintenir en cas de crise (commandes, logistiques, etc).

Prévoir des modes alternatifs (« modes dégradés ») en cas d'indisponibilité prolongée des systèmes.

Pour être opérationnel, le PCA doit être testé régulièrement.

✓ **Définir un Plan de Reprise d'Activité (PRA)***

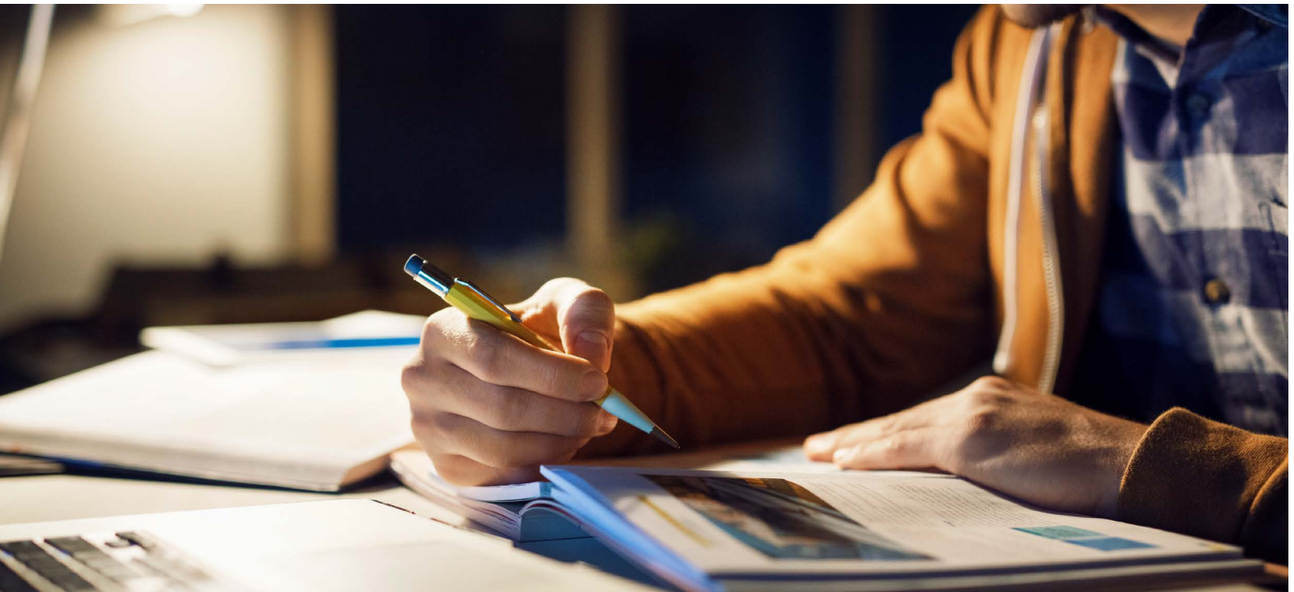
Il assure, en cas d'arrêt de l'activité ou d'un processus, la reconstruction de l'infrastructure numérique et la remise en route des applications stratégiques de l'entreprise.

Le PRA doit être testé et ajusté en continu pour s'adapter aux évolutions des infrastructures et des risques.

Pendant l'incident

→ **Déclencher les scénarios prévus par le PCA** pour assurer la continuité de l'activité pendant la crise.

→ **Activer le PRA** pour remettre progressivement en service les systèmes et valider leur intégrité.



3 Mobiliser les soutiens externes pour gérer la crise efficacement et communiquer de manière transparente pour préserver la confiance

En amont :

✓ **Souscrire une assurance cyber adaptée**

Le contrat permet de couvrir les frais et les pertes liées à l'incident (frais de remise en état, pertes d'exploitation, …).

Au-delà de l'indemnisation, privilégier un contrat d'assurance qui propose des services en amont (prévention) et dans la gestion de la crise (assistance).

✓ **Identifier les tiers à impliquer dans la gestion de l'incident**

Salariés, experts forensic*, experts en communication de crise, prestataires techniques, autorités, assureur… : autant d'intervenants clés qui doivent être mobilisables rapidement pour accompagner la gestion de la crise.

Certains contrats d'assurance identifient et coordonnent les tiers pour gérer l'incident.

✓ **Prévoir une communication transparente**

Clients, actionnaires, partenaires, autorités, … devront être informés en cas d'incident pour conserver leur confiance et être en conformité réglementaire.

Pendant l'incident

→ **Appeler son assureur pour bénéficier de son réseau d'expert** dans un premier temps, puis de l'indemnisation.

→ **Mobiliser les parties – internes et externes -** pour investiguer, contenir et réparer.

Effectuer les notifications légales : par exemple en France dépôt de plainte sous 72h suivant la détection de l'incident, information aux organismes compétents.

→ **Communiquer rapidement** pour limiter les risques judiciaires, réglementaires ou réputationnels.

L'AVIS DE L'EXPERT

Pour les organisations internationales qui opèrent dans de nombreux pays, l'un des principaux défis consiste à harmoniser la cybersécurité à l'échelle mondiale. Il s'agit de concilier des niveaux de maturité différents, des contextes réglementaires variés et des pratiques locales pour bâtir une protection cohérente et efficace.

JONATHAN DRIKES,
Responsable Souscription Cyber,
AXA XL France

En bref… **cinq réflexes à avoir** en cas d'attaque :

Immédiatement

1 — Activer le plan et la cellule de crise
Ne pas improviser : suivre le Plan de Réponse aux Incidents (PRI) et mobiliser l'équipe désignée.

2 — Contenir l'attaque
Identifier et isoler les systèmes affectés pour éviter la propagation et protéger les actifs restants.
Le système suspect doit être déconnecté du réseau sans l'éteindre ni le redémarrer, afin de préserver les preuves numériques.

3 — Mobiliser les experts
Faire intervenir les prestataires spécialisés (forensic, communication de crise, prestataires techniques) ; contacter son assureur pour déclarer le sinistre et déclencher les prestations prévues. Il sera en mesure d'aider à mobiliser les prestataires.

Premières heures

4 — Communiquer dès que possible
Porter plainte auprès des autorités compétentes (dans les 72h suivant la détection de l'attaque en France).
En cas d'atteinte aux données à caractère personnel, notifier les autorités locales compétentes (la CNIL en France par exemple), ainsi que les personnes concernées par la violation des données.
Informer la direction, les salariés, ainsi que les actionnaires, les clients et les partenaires.

Premières heures/jours

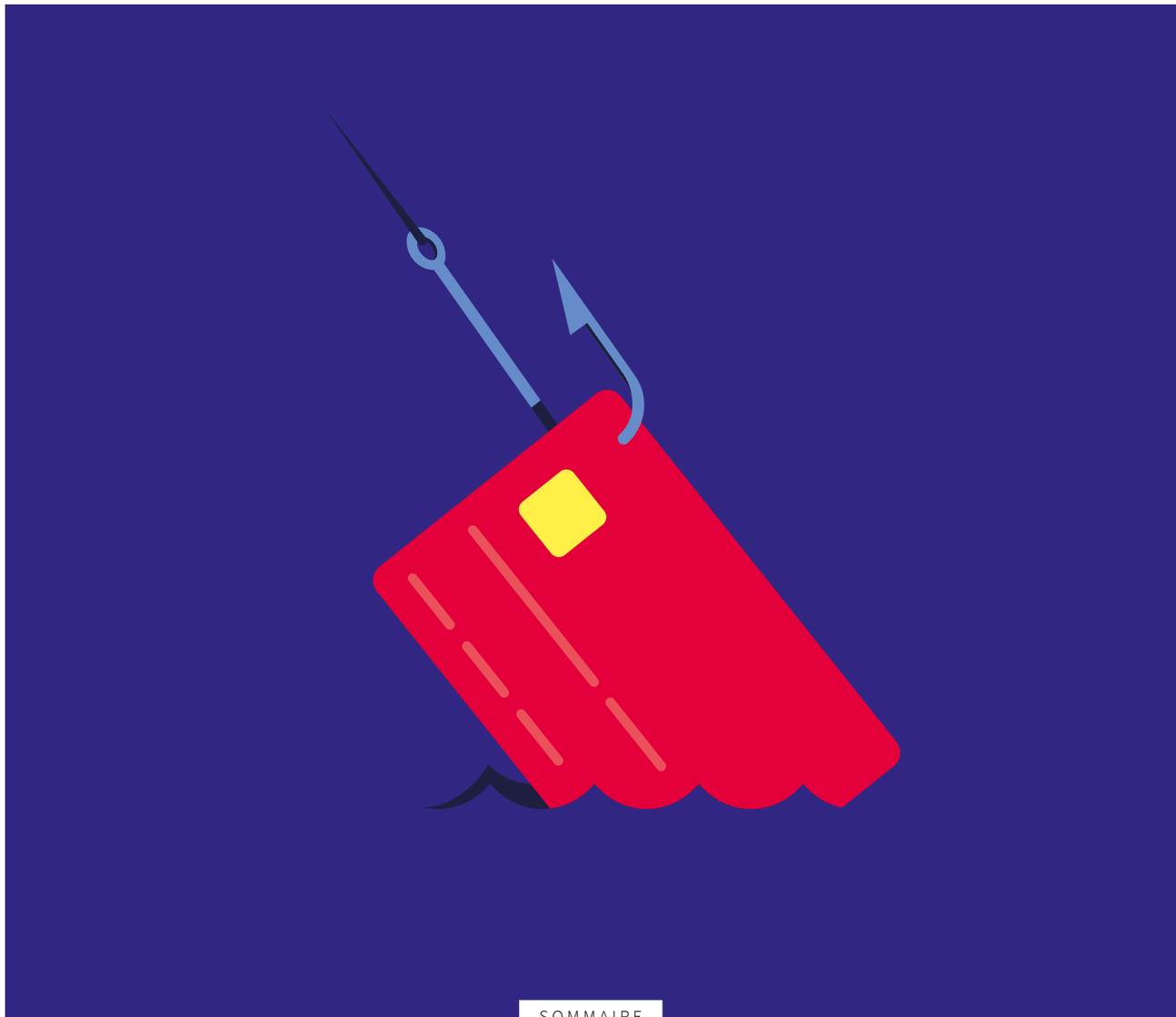
5 — Sécuriser l'activité
Déclencher le PCA pour assurer la continuité des activités.
Puis le PRA pour planifier la restauration progressive.

Se préparer à ces réflexes en amont, via des plans et des entraînements, permet de gagner un temps précieux et de limiter les impacts de l'incident.

Cyber-résilience : adopter une démarche progressive pour faire face aux menaces

Focus sur le phishing : quelques conseils pratiques pour réagir au plus vite

- Déconnecter immédiatement l'utilisateur ou le poste concerné ;
- Changer les mots de passe compromis ;
- Analyser les journaux pour identifier les accès non autorisés ;
- Informer les collaborateurs pour éviter d'autres clics sur le même message.



SOMMAIRE

AXA, un acteur au cœur de l'écosystème **cyber**

04

Sensibiliser les entreprises face **au risque cyber**

AXA France joue un rôle clé pour sensibiliser et mobiliser les entreprises face au risque cyber, à travers une politique de partenariats ciblés, des actions de sensibilisation sur le terrain et une veille internationale sur la menace.

plus de **1000** dirigeants sont sensibilisés chaque année en France à la menace cyber par AXA France[1].

Une responsabilité sociétale face à un risque majeur

Le risque cyber figure parmi les principales préoccupations des dirigeants, en raison des conséquences potentiellement lourdes des incidents sur l'activité de leur entreprise. Pour les TPE et PME, souvent moins bien préparées, il peut menacer la pérennité même de leur activité. Dans ce contexte, AXA France s'engage au-delà de son rôle d'assureur, en contribuant activement à la sensibilisation des entreprises afin qu'elles puissent mieux anticiper et se préparer à la menace.

L'AVIS DE L'EXPERT

Assurer une PME sur trois en France nous confère une responsabilité particulière. Derrière chaque entreprise, il y a un dirigeant qui peut être pris au dépourvu face à une attaque cyber. Nous avons le devoir de le sensibiliser et de l'aider à anticiper le risque pour protéger son activité.

THIERRY PITON,
Référent National Souscription Risques Cyber, AXA France
Réserviste à l'Office anti-cybercriminalité (OFAC)

(1) AXA France, 2025

Des liens stratégiques et une veille internationale pour anticiper une menace cyber en constante évolution

AXA France collabore activement avec des acteurs clés de l'écosystème cyber, favorisant un enrichissement mutuel des expertises et une compréhension fine de la menace.

Office anti-cybercriminalité de la Police judiciaire (OFAC)
Partenariat public-privé avec AXA France, inédit dans le secteur de l'assurance, visant à renforcer la protection des TPE et PME face aux cybermenaces. Ce partenariat se traduit par des actions de sensibilisation menées sur le terrain auprès des chefs d'entreprises.

Campus Cyber
AXA France est membre de Campus Cyber, un lieu d'innovation et de collaboration qui réunit entreprises, services de l'État, acteurs de la recherche et associations pour renforcer la protection de la société face au risque cyber.

AXA France s'appuie également sur la présence du Groupe AXA dans cinquante pays pour enrichir sa connaissance sur les tendances mondiales, telles que l'utilisation croissante de l'intelligence artificielle par les attaquants ou le rôle à venir des technologies quantiques.
Elle bénéficie en outre d'une ingénierie cyber internalisée, qui contribue activement à l'analyse des risques et à la veille sur l'évolution des menaces, en lien étroit avec des acteurs institutionnels tels que l'OFAC et la Gendarmerie nationale.
Cette approche itérative, nourrie par une veille internationale et des partenariats stratégiques, confère à AXA France une forte culture de la cybersécurité, lui permettant de sensibiliser les dirigeants aux risques, d'anticiper les actions de prévention et de rester en alerte face aux attaques émergentes.

L'AVIS DE L'EXPERT

AXA France a été l'un des premiers assureurs à se positionner sur le marché de l'assurance cyber, il y a dix ans. Cet engagement de long terme, renforcé par des liens étroits avec les acteurs clés de l'écosystème, place AXA France en première ligne pour comprendre les risques et sensibiliser les dirigeants de TPE et PME. Nous les aidons à mieux appréhender la menace et à prendre conscience des leviers de protection existants, notamment à travers des actions de prévention adaptées à leurs enjeux.

JEAN-PIERRE MARBAIX,
Ingénierie Prévention Cyber, AXA France
Réserviste à l'Unité Nationale Cyber de la Gendarmerie Nationale

"Le dépôt de plainte est indispensable pour faire avancer la lutte contre la cybercriminalité."

Pourquoi la menace cyber est-elle si préoccupante ?

Les attaques cyber sont menées par des groupes criminels organisés et structurés, difficiles à démanteler. En parallèle, nous observons le développement du crime-as-a-service*, facilité par l'intelligence artificielle, qui permet à des non-experts, voire à des novices, de lancer des attaques avec des outils clés en main. Le risque cyber explose et touche désormais toutes les entreprises, en particulier les PME et TPE, encore peu préparées. Face à ces évolutions, la sensibilisation des chefs d'entreprise est essentielle.

Que recommandez-vous aux entreprises ?

D'abord, anticiper. Il faut élaborer un plan de gestion de crise et s'entraîner pour être prêt à réagir en cas d'attaque.

Trop d'entreprises hésitent encore à déposer une plainte, par crainte pour leur réputation, par manque de préparation ou parce que la démarche peut sembler chronophage.

Enfin, en cas d'attaque par rançongiciel, il ne faut jamais payer : plus un pays paie, plus il attire les criminels.

Quelles sont les actions menées par l'OFAC pour sensibiliser les dirigeants de PME et TPE ?

Nous nous appuyons sur deux dispositifs complémentaires.

D'abord, le réseau des experts cybermenaces (RECYM), qui regroupe 110 réservistes issus des secteurs public et privé, répartis sur tout le territoire. Ils rencontrent des dirigeants de TPE et PME pour les sensibiliser à la menace et leur transmettre les bonnes pratiques. En 2024, 114 000 entreprises ont été sensibilisées à travers 157 actions, souvent organisées avec nos partenaires comme AXA.

Ensuite, le CSIRT-PJ, constitué d'ingénieurs en cybercriminalité, accompagne les entreprises victimes dans le dépôt de plainte.

Nous sommes reconnaissants vis-à-vis de l'ensemble de nos réservistes et partenaires pour leur engagement sans faille à nos côtés dans la sensibilisation du plus grand nombre.

CÉCILE AUGERAUD,
Cheffe adjointe de l'Office anti-cybercriminalité (OFAC)

Des actions de sensibilisation concrètes sur le terrain

Consciente que la première barrière contre une cyberattaque reste la vigilance des dirigeants et de leurs équipes, AXA France mène des actions de sensibilisation partout en France. Ces événements sont menés sous l'impulsion d'un accord entre AXA France et nos réseaux d'intermédiaires, en lien avec des experts en cybersécurité.
Ils visent à expliquer concrètement aux dirigeants de PME le niveau de risque auquel ils font face et à leur présenter les bonnes pratiques pour s'en prémunir.

L'AVIS DE L'EXPERT

Je mène des actions de sensibilisation auprès de chefs d'entreprise depuis 2018. À l'époque, il était difficile de susciter leur intérêt sur le sujet du risque cyber. Aujourd'hui, les mentalités évoluent : les dirigeants sont de plus en plus attentifs, conscients des enjeux pour leur activité et du risque réel lié à l'exposition croissante de leurs données.

GUILLAUME BERCIER,
Agent Général, AXA France

SOMMAIRE

AXA France : Global Cyber Secure, une solution complète et modulable pour protéger les entreprises de moins de 5 000 salariés

Des services de prévention et d'assistance couplés à un contrat d'assurance afin de répondre aux enjeux spécifiques des TPE, PME et ETI

Les dirigeants de TPE, PME et ETI ne disposent pas toujours de ressources dédiées à la cybersécurité. Ils doivent pouvoir s'appuyer sur des experts pour bénéficier d'un accompagnement complet, capable à la fois de réduire le risque de survenue d'une cyberattaque réussie, de limiter l'ampleur des conséquences et d'assurer une gestion optimale de l'incident. Conçue dans cette optique, l'offre Global Cyber Secure a déjà été adoptée par 5 000 entreprises en France.

L'AVIS DE L'EXPERT

Chez AXA France, nous sommes convaincus qu'agir avant l'incident est la meilleure protection. Une attaque cyber, même indemnisée, peut en effet fragiliser durablement une entreprise. Une approche proactive, axée sur la prévention, est donc essentielle.

FRÉDÉRIC COPPIN,
Directeur Technique et Souscription Grands comptes, AXA France

Les atouts de Global Cyber Secure :

Une solution **globale** qui combine Prévention, Assurance et Assistance en cas de sinistre.

Une **réponse face aux risques cyber** qui ne sont pas couverts par les produits classiques avec des garanties et des services innovants.

L'expertise AXA et celles de nos partenaires en matière de prévention et de gestion des risques cyber.

Une **couverture personnalisée des pertes financières**, avec la possibilité d'ajouter une option de garantie Responsabilité Civile.

Comment Global Cyber Secure se distingue-t-elle des autres solutions sur le marché ?

Notre solution présente plusieurs atouts qui renforcent la position de leader d'AXA France sur le marché de l'assurance cyber.

Un premier point clé réside dans la veille permanente sur l'évolution des cybermenaces, permettant d'adapter nos solutions en temps réel et de garantir une protection optimale à nos clients.

En matière de prévention, notre offre inclut deux solutions cybersécurité de référence sur le marché qui permettent à nos assurés de réduire leur exposition aux risques cyber. La première, un scan de vulnérabilités externes, leur permet de prendre connaissance et de corriger leurs vulnérabilités techniques exposées sur internet. La seconde, une plateforme de sensibilisation, leur permet de mettre en place une véritable culture de la cybersécurité au sein de leur entreprise. Ces services sont essentiels pour réduire la surface d'attaque et prévenir les intrusions opportunistes.

Grâce à une équipe d'ingénierie cyber interne, AXA France développe des solutions innovantes et en phase avec l'évolution de la menace. Nous disposons de notre propre équipe de souscription spécialisée, capable d'évaluer les besoins spécifiques des clients et leur proposer des solutions adaptées, assurant une couverture optimale.

En termes d'assistance, AXA France se démarque avec une offre très complète. Une équipe sinistre dédiée coordonne les prestataires techniques, la communication de crise et l'accompagnement juridique et réglementaire (y compris les notifications et le dépôt de plainte). Cette équipe accompagne l'entreprise à chaque étape du processus, garantissant une gestion efficace des sinistres. AXA est par ailleurs le seul assureur à proposer un soutien psychologique, soulignant son engagement envers le bien-être de ses clients et de leurs employés.

THIERRY PITON,
Référent National Souscription Risques Cyber, AXA France

Un accompagnement complet à 360°, reposant sur 3 piliers[1]

AXA France a choisi une approche résolument proactive, plaçant la prévention et l'assistance au cœur de la démarche, afin de prévenir les cyberattaques et de réduire leurs impacts. Les prestations suivantes sont proposées en inclusion des contrats – ils peuvent être complétés par d'autres services à la carte (voir pages 72 et 73).

1 Prévention

- **Scan hebdomadaire** des vulnérabilités externes : Board of Cyber – Security Rating.
- **Sensibilisation** à la cybersécurité : plateforme Kamaé.

2 Assistance

En cas d'incident :
- Une **plateforme disponible** 24/7 avec intervention dans l'heure.
- Accompagnement **technique et juridique**.
- Conseils en **communication de crise et soutien psychologique**.

3 Garanties

Couverture financière pour[1] :
- Les **pertes directes** : atteinte aux données, vol de données personnelles, détournement de fonds.
- Les **pertes indirectes** : pertes d'exploitation, atteinte à la réputation.

L'AVIS DE L'EXPERT

L'ingénierie prévention cyber d'AXA France aide ses clients à évaluer leur exposition au risque et à renforcer leur niveau de protection. Avec une approche adaptée aux réalités de chaque entreprise, elle définit les actions de prévention les plus pertinentes.
Cette démarche de conseil permet de maintenir des mesures de prévention efficaces face à des menaces en constante évolution.

JEAN-PIERRE MARBAIX,
Ingénierie Prévention Cyber,
AXA France

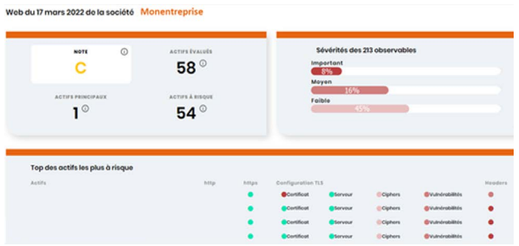
(1) Selon clauses et conditions du contrat

AXA, un acteur au cœur de l'écosystème cyber

Zoom sur deux services essentiels de prévention inclus dans l'offre

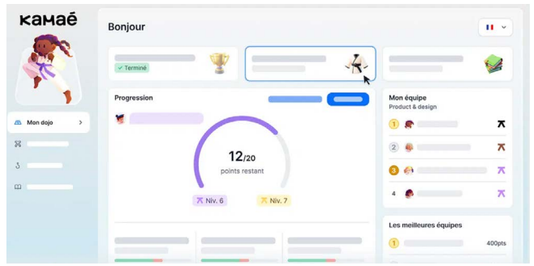
board of cyber

- **Notation** de votre maturité cyber à travers 7 axes d'analyse (surface d'attaque, messagerie, contrôles de sécurité, vulnérabilités potentielles…).
- **Pilotage** en continu de **l'évolution** de vos vulnérabilités au travers d'un tableau de bord.
- **Recommandations d'améliorations** via un rapport détaillé.
- **Benchmark sectoriel** pour vous comparer avec vos pairs.



KAMAÉ

- **Plateforme de sensibilisation** en cybersécurité et RGPD contenant micro-learnings et challenges ludiques.
- **Deux tests de phishing par an** et un kit de prévention avec des fiches réflexes.
- Visualisation de l'acquisition des connaissances via des **tableaux de bord personnalisés.**



Des outils et services additionnels sont proposés à des tarifs préférentiels aux entreprises assurées chez AXA. Des solutions combinant valeur ajoutée, simplicité d'utilisation et accompagnement humain

Renforcer la résilience grâce à des audits et accompagnements sur-mesure[1].

1

Audits et diagnostics

Nous avons la capacité d'accompagner tout type d'entreprise, quels que soient sa taille, son activité, sa localisation géographique et ses besoins.

- Analyses des risques, basées sur la méthode préconisée par l'ANSSI et conseils de cybersécurité.
- Audits techniques (tests d'intrusion, audits d'architecture, de code…).
- Audits de Gouvernance – Risques – Conformité.
- Audits et diagnostics de cyber-résilience : audit diagnostic du plan de continuité d'activité **(PCA)**, diagnostic de la résilience du **Système d'information.**

2

Accompagnement

- Accompagnement dans la mise en place de plans de continuité d'activité **(PCA)**, de reprise des activités du SI **(PRA SI)**, de continuité informatique **(PCI)**, de continuité d'activité cyber (**PCA Cyber**, modes dégradés métiers).
- Conception et mise en œuvre d'une structure de **gestion de crise cyber** et exercices d'entraînement..

Partenaires : Almond, spécialisé dans les services de cybersécurité, qui dispose de la qualification PASSI délivrée par l'ANSSI ; Adenium BRG, spécialisé dans la gestion de crise et des dispositifs de continuité d'activité, en conformité avec la norme ISO 22301.

XAVIER HARTOUT,
Président d'Adenium BRG

L'AVIS DE L'EXPERT

Adaptés aux spécificités de chaque entreprise, les audits et diagnostics menés par Adenium évaluent les dispositifs de continuité et de reprise d'activité, avec des préconisations concrètes. Ils s'accompagnent de la mise en œuvre opérationnelle et d'exercices de gestion de crise, simulant des attaques pour tester la réactivité des équipes et identifier les failles. La différence entre une crise bien gérée et un échec tient souvent à la capacité à mobiliser l'intelligence collective.

(1) Il s'agit de services en option. Sur devis, tarif négocié pour les assurés AXA IARD Entreprises.

Deux nouveaux services pour renforcer la protection de l'entreprise[1].

1

Détection précoce : EDR managé

(Endpoint Detection Response)

- Surveille, détecte et réagit face aux menaces ciblant les postes de travail, les serveurs et les appareils mobiles.
- Assure l'identification de comportements malveillants, le blocage des menaces et concourt à la remédiation des équipements compromis.

2

Sauvegarde immuable

- Sauvegarde sécurisée des données (jusqu'à 50 Go par utilisateur) : chiffrement des sauvegardes, interdiction des modifications et accès authentifié.
- La sauvegarde est inaltérable et indestructible pendant toute sa durée prévue de conservation.

Partenaire : Docaposte, référent de la confiance numérique en France et expert dans le traitement de données sensibles.

L'AVIS DE L'EXPERTE

Pouvoir ajouter des services à la carte constitue un véritable atout pour les clients, qui peuvent sélectionner les solutions adaptées à leurs besoins, tout en bénéficiant de conditions tarifaires avantageuses. Cela rend ces services accessibles, même aux structures de plus petite taille.

CHRISTINE SINIBARDY,
Directrice Risques Techniques et Cyber, AXA France

Retrouvez tous nos services de prévention en flashant ce QR code.

(1) Il s'agit de services en option. Sur devis, tarif négocié pour les assurés AXA IARD Entreprises.

Un accompagnement continu, grâce aux réseaux de distribution et aux équipes d'experts en cybersécurité d'AXA France

Nos réseaux de distribution, composés de nos Agents généraux et de nos courtiers, sont solidement implantés sur l'ensemble du territoire, au plus près des enjeux des entreprises. Avec les experts cyber d'AXA France, ils accompagnent leurs clients à chaque étape clé.

En amont de la souscription

1 Conseil en amont de la souscription

Le niveau de sécurité de l'entreprise est étudié dès l'étape de souscription d'une assurance cyber, en fonction de sa taille et de son secteur d'activité. Cela permet de formuler des recommandations adaptées pour renforcer sa maturité cyber au regard de son exposition au risque et de ses enjeux.

L'AVIS DE L'EXPERT

Lorsqu'une faille est identifiée, nous mobilisons les équipes prévention ainsi qu'une société d'experts afin de mettre en œuvre un accompagnement personnalisé :

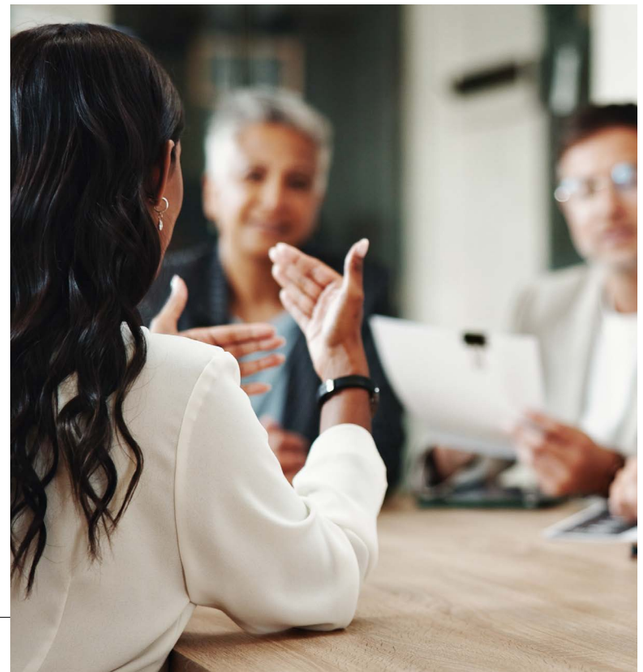
- Sensibilisation des équipes dirigeantes ;
- Coordination avec les prestataires informatiques ;
- Formulation de recommandations concrètes pour renforcer la sécurité de l'entreprise et de ses partenaires technologiques.

GUILLAUME BERCIER,
Agent général, AXA France

En continu

2 Suivi personnalisé

Bilan périodique permettant d'évaluer les besoins en matière de cybersécurité et d'apporter des recommandations en termes de prévention.
Prise en compte des évolutions réglementaires et de leur impact.
À l'occasion du renouvellement ou à la demande du client, propositions d'ajustement de la couverture, si nécessaire.



En cas d'incident

3 Réponse coordonnée

L'équipe dédiée de « régleurs sinistres » d'AXA France est mobilisée pour coordonner les intervenants techniques, veiller à la conformité administrative (notification, dépôt de plainte, etc.) et accompagner l'entreprise tout au long de la vie du contrat.

En cas de crise, il ne faut pas rester seul face à l'urgence.
L'assurance cyber d'AXA France permet aux entreprises de s'appuyer sur des équipes de spécialistes pour gérer les crises liées aux incidents cyber.
L'activation d'experts via une hotline H24/7 dédiée, qui permet d'enclencher dans les minutes suivant l'appel les premières mesures de réponse en cas d'incident.
Une cellule spécialisée est mobilisée dès les premières heures : gestionnaires de sinistres expérimentés, experts de réponse à incident qualifiés par l'ANSSI, juristes spécialisés, experts en communication de crise, psychologues…
L'objectif est clair : contenir rapidement l'incident, protéger la réputation de l'entreprise et limiter les impacts opérationnels.
Pour cela AXA France s'appuie sur des partenaires spécialisées en gestion de crise afin d'aider ses clients à revenir au plus vite à un fonctionnement normal, dans des conditions sûres et efficaces.

L'AVIS DE L'EXPERTE

Parce qu'un sinistre Cyber ne laisse pas de place à l'improvisation, nous nous engageons à apporter une réponse rapide, efficace et professionnelle. L'équipe CYBER d'AXA France, disponible en 24H/24 et 7J/7, coordonne rapidement les interventions d'urgence pour soutenir nos entreprises sur le plan technique, humain et financier. Un accompagnement sur-mesure et une écoute attentive orientée vers une reprise des activités du client.

CHARLOTTE PRIEUR,
Chargée de règlements déléguée, AXA France

L'AVIS DE L'EXPERT

En cas d'attaque, AXA fait preuve d'une réactivité et d'une fiabilité exemplaires. Grâce à son équipe sinistre expérimentée, les entreprises bénéficient d'un accompagnement immédiat et efficace.
Ce sont de vrais spécialistes qui prennent le relais pour contenir l'incident et remettre l'activité en route.

PHILIPPE HERMETZ,
Agent général,AXA France

AXA XL : CyberRiskConnect, une offre sur-mesure pour accompagner les entreprises de plus 5 000 salariés

AXA XL accompagne les entreprises de taille moyenne et les grandes entreprises dans plus de 200 pays. Avec CyberRiskConnect, elle déploie une offre d'assurance et de services différenciante sur le marché pour aider les organisations opérant à l'échelle nationale ou internationale à contrer une menace cyber de plus en plus intense.

Une expertise unique sur le risque Cyber

AXA XL regroupe un ensemble d'experts cyber, de la souscription à la gestion des incidents, pour gérer le risque cyber sur l'ensemble de ses dimensions.

Expérience

Expérience collective construite depuis 10 ans, sur des milliers de cas à travers le monde.

Ancrage global / local

Couverture mondiale et gestion locale afin de répondre aux risques spécifiques à chaque région.

Disponibilité

Plateforme disponible 24/7 avec intervention en moyenne en moins de 2 heures après un signalement.

Innovation

Offre adaptée en permanence aux nouvelles formes de menaces et aux évolutions technologiques (ex : Intelligence Artificielle Générative).

CyberRiskConnect, l'offre cyber multidimensionnelle d'AXA XL

AXA XL a conçu un produit d'assurance évolutif afin de contrer un risque cyber en constante mutation et d'offrir une protection complète à ses clients. Il allie des garanties d'assurance et d'assistance et des services de cybersécurité tout au long du cycle de vie du contrat.

AXA XL Cyber Risk Consulting, une division spécialisée dans la gestion proactive des risques cyber

Les experts en cybersécurité d'AXA XL s'engagent à fournir un soutien et une protection inégalés à leurs clients en leur proposant des prestations de conseil personnalisé en gestion des risques, des formations pratiques et une sélection des meilleures solutions du marché. L'accompagnement continu permet d'anticiper les risques et de renforcer la résilience des organisations et de leurs systèmes informatiques.

L'AVIS DE L'EXPERTE

Nous proposons des services de conseil personnalisé en cybersécurité pour répondre aux besoins spécifiques de nos clients, avec des experts répartis en Amérique, en Europe et en Asie-Pacifique.

Cette présence mondiale nous permet de combiner une approche globale avec une compréhension fine des spécificités locales. Nous aidons nos clients à prévenir ou limiter l'impact des risques cyber en évaluant la protection de leurs actifs sensibles, comme les systèmes industriels, financiers ou logistiques.

En interne, nous travaillons étroitement avec les souscripteurs pour évaluer les risques et proposer des polices d'assurance adaptées, à des tarifs justes et compétitifs.

RÉBIAH BARDOT-GIRARD,
Chief Risk Consulting Officer, Cyber, AXA XL, a division of AXA

Focus sur les services proposés pour renforcer la cybersécurité des assurés

AXA XL propose un ensemble complet de services de cybersécurité, conçus pour renforcer la protection des entreprises et optimiser la gestion de leurs risques. Ces services, inclus dans l'offre ou disponibles en option à des conditions préférentielles pour les assurés AXA XL, sont délivrés par les équipes spécialisées d'AXA XL ou en partenariat avec les meilleurs experts du marché. Ils s'articulent autour de quatre piliers :

Prévenir - Évaluer le niveau de maturité de l'entreprise, identifier les risques et définir une stratégie de cybersécurité.

En amont de la souscription

Discussion avec des experts sur les besoins spécifiques de l'entreprise, à l'ouverture du contrat.

Évaluation du niveau de maturité cyber	Gestion des risques & Conformité *(Technologies de l'information & Technologies opérationnelles)*	Conseil stratégique en cybersécurité	Protection des données
Évaluer le niveau de sécurité d'une entreprise et le comparer à celui de ses pairs, à travers une analyse externe et des outils de notation clairs et accessibles. **Accès à la plateforme de cybersécurité ;** **Accès privilégié à des solutions complètes pour la gestion des risques fournisseurs et de leurs performances.**	Effectuer des analyses de sécurité détaillées et des audits de conformité s'appuyant sur les normes et standards reconnus (NIST Cybersecurity Framework (CSF), ISO 27001, DORA, GDPR, SOC 2, CEI 62443, NIS2,…). **Analyse de risque Cyber (Simple ou Avancé) ;** **Gestion des risques Tiers ;** **Conformité réglementaire & Standards ;** **Gestion des risques et analyse de conformité OT (technologies opérationnelles)**	Définir avec l'équipe Cyber Risk Consulting un objectif et élaborer un plan d'action opérationnel permettant de l'atteindre. **Stratégie et Feuille de Route Cyber ;** **RSSI (Responsable de la sécurité des systèmes d'information) / RS (Responsable de la sécurité) / DPO (Délégué à la protection des données) virtuel** **Analyse et compréhension des risques.**	Permettre aux entreprises de protéger leurs données contre les violations et d'assurer leur conformité avec les réglementations en constante évolution. **Évaluation de la confidentialité des données et transfert de données Gouvernementales ;** **Gestion des risques liés aux tiers ;** **IA responsable.**

Préparer - Identifier les vulnérabilités, anticiper les attaques et se préparer en conséquence.

Sensibilisation & formation	Défenses cyber	Surveillance des menaces et des fuites de données
Permettre aux employés de mieux comprendre les risques et les vulnérabilités, tout en adoptant les bonnes pratiques grâce à des formations et à des simulations de *phishing*. **Packs de formation à la Cybersécurité pour les collaborateurs ;** **Formation de sensibilisation à la sécurité et simulations d'attaques par phishing pour limiter le risque d'erreurs humaines face aux menaces cyber ;** **Formation & Sensibilisation Cyber OT (technologies opérationnelles)**	Tester et renforcer les défenses de l'entreprise de manière proactive en détectant les vulnérabilités puis en déployant les correctifs et les mesures de réduction des risques. **Scans périmétriques & rapports : analyse de la surface d'attaque pour identifier les vulnérabilités ;** **Tests d'intrusion & audits de configurations des systèmes ;** **Tests d'intrusion pour les OT (technologies opérationnelles)** **Red Team & Purple Team : équipes spécialisées pour tester la résistance de l'entreprise aux attaques ;** **Tests de Social Engineering & Phishing.**	Surveiller en continu les menaces potentielles et les fuites de données pour protéger efficacement les informations sensibles. **Rapports de veille sur les menaces : analyses semestrielles des menaces cyber (Threat intelligence) ;** **Webinaires périodiques sur les menaces cyber émergentes et conseils pratiques ;** **Synthèse des menaces majeures destinées aux dirigeants (Executive Threat briefings) ;** **Surveillance du dark web en temps réel pour alerter les entreprises en cas de fuite de données, de rançongiciel, et notifications en cas de compromission de fournisseurs.**

Protéger - Prioriser les efforts de protection et construire des défenses solides autour des actifs critiques.

Surveillance, détection et neutralisation des attaques	Gestion des identités et des accès	Identification & remédiation des vulnérabilités
Surveiller et protéger les systèmes pour détecter, prévenir et répondre aux menaces cyber en temps réel.	Protéger les systèmes contre les accès non autorisés et les menaces liées à l'identité grâce à un ensemble complet de services. **Protection des comptes de service ;** **Protection de l'Active Directory ;** **Gestion des accès privilégiés : PAM (Privileged Access Management) ;** **Détection et réponse aux menaces sur les incidents : ITDR (Incident Threat Detection and Response).**	Analyser la surface d'attaque grâce à des scans externes et évaluer la sécurité des actifs via un scan interne du réseau. Identifier les faiblesses de sécurité des systèmes industriels et mettre en place des mesures pour traiter efficacement les vulnérabilités potentielles. **Gestion d'inventaire et cartographie de réseaux OT (technologies opérationnelles) ;** **Audit sur site des technologies opérationnelles (OT) ;** **Déploiement de sondes sur le réseau industriel.**

Perdurer - Répondre, rétablir et sortir plus fort d'un incident.

Diagnostic de cyber-résilience	Réponse aux incidents	Entraînement à la gestion de crise	Reprise d'activité rapide
Évaluer la capacité d'une entreprise à faire face à une attaque en analysant sa maturité en termes de cybersécurité, sa stratégie de sauvegarde et ses capacités de récupération. **Évaluation de la Cyber-résilience selon les standards du NIST ;** **Services d'évaluation de la résilience des sauvegardes, de l'Active Directory (AD) et des configurations des pare-feu.**	Renforcer la capacité d'une organisation à réagir et à gérer efficacement une attaque, en optimisant son processus de réponse aux incidents. **Préparation de la Réponse aux Incidents Cyber ;** **Implémentation et revue du Plan de Réponse aux incidents cyber.**	Définir un programme de formation complet pour préparer l'entreprise à gérer efficacement les incidents et à mesurer leur impact sur l'activité. **Exercice théorique de gestion de crise ;** **Exercice de simulation de gestion de crise ;** **Exercice de Calcul des Pertes matérielles.**	Accélérer la restauration des systèmes en collaborant avec des spécialistes reconnus, experts des solutions de sauvegarde. **Réduire au minimum le temps d'interruption des opérations et accélérer la restauration des systèmes en collaborant avec des spécialistes reconnus des solutions de sauvegarde.**

SOMMAIRE

Focus sur les garanties et l'assistance en cas d'incident

Malgré les efforts réalisés an amont pour se protéger, aucune entreprise n'est à l'abri d'une attaque. L'offre CyberRiskConnect propose ainsi aux clients des garanties et des prestations d'assistance adaptées aux organisations.

Les garanties CyberRiskConnect incluent la couverture des pertes directes subies par les entreprises, mais également la responsabilité civile, en cas de préjudices causés à des tiers.

Garanties en dommages directs :

- Perte d'exploitation et frais supplémentaires ;
- Perte ou destruction d'actifs électroniques ;
- Prise en charge de la réponse à incident ;
- Frais de défense en cas de procédure réglementaire, d'amendes et sanctions (dans les limites de ce qui est assurable selon la législation) ;
- Restauration des données ;
- Extorsion cyber.

Garanties en responsabilité civile :

- Responsabilité en cas de violation de données, atteinte à la sécurité ou à la vie privée ;
- Responsabilité liée aux communications et contenus diffusés en ligne (internet, médias).

D'autres garanties, disponibles en option, peuvent être ajoutées au contrat.

L'assistance CyberRiskConnect est disponible 24/7 pour assurer une gestion immédiate et efficace des incidents.

Mobilisation immédiate d'une équipe sinistre cyber dédiée

En cas d'attaque cyber, AXA XL mobilise une équipe dédiée de gestionnaires sinistres pour accompagner ses clients dès les premières heures. Ceux-ci accèdent instantanément à un panel d'experts qualifiés – juridiques, techniques, communication de crise – pour contenir l'incident, limiter les impacts opérationnels et protéger la réputation de l'entreprise.

Cas d'une résolution décisive en 72h

En 2023, l'équipe sinistres d'AXA XL aux Etats-Unis a permis à un hôpital victime de ransomware de restaurer ses systèmes en seulement 72 heures, évitant des interruptions de soins critiques.

L'AVIS DE L'EXPERT

En cas d'incident, beaucoup d'organisations cherchent d'abord à « gérer seules ». C'est seulement quand elles sont dépassées, et que la situation leur échappe, qu'elles contactent leur assureur — parfois après avoir détruit des éléments clés pour identifier la cause de l'attaque. Notre conseil : en cas d'incident, appelez immédiatement votre assureur.

MATHIEU COUSIN,
Cyber Risk Consulting & Threat Intelligence Strategist, AXA XL, a division of AXA

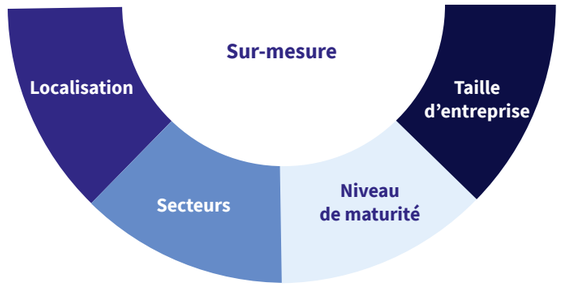
En 2025, AXA XL a été doublement récompensée aux États-Unis pour l'excellence de ses équipes cyber.

L'équipe de gestion des sinistres cyber a reçu le prix de la Cyber Claims Team of the Year lors des Zywave Cyber Risk Awards.

Les équipes de souscription et de gestion des sinistres ont également été élues Cyber Insurance Carrier of the Year aux Cyber Insurance Awards USA organisés par Intelligent Insurer.

Un accompagnement adapté au profil de l'entreprise

L'accompagnement d'AXA XL sur le risque cyber est conçu pour s'adapter à chaque entreprise, quels que soient son secteur d'activité, sa taille, sa localisation ou son niveau de maturité.



CyberRiskConnect est particulièrement adaptée aux environnements complexes et fortement exposés :

Une approche sectorielle spécifique

Les polices d'assurance sont adaptées à chaque secteur, en fonction de ses spécificités métier et réglementaires.

Par exemple, une couverture peut être prévue pour les interruptions d'activité causées par des fournisseurs tiers, lorsqu'un assuré est exposé à des risques liés à sa chaîne d'approvisionnement.

Zoom sur la nouvelle offre dédiée à la cybersécurité industrielle

Elle répond aux problématiques spécifiques des OT (technologies opérationnelles) en proposant des garanties et services adaptés, tels qu'un audit sur site industriel conforme aux normes du secteur ou des tests d'intrusion ciblant les OT.

Les entreprises moins matures en termes de protection cyber peuvent accéder à des ressources pédagogiques, sous forme de guides pratiques et de webinaires, pour mieux comprendre leurs vulnérabilités. Des services d'évaluation et de test de la cybersécurité – tels que des exercices de gestion de crise cyber – sont également proposés.

JONATHAN DRIKES,
Responsable Souscription Cyber, AXA XL France

L'AVIS DE L'EXPERT

Pour les activités sensibles, comme les OSE (Opérateurs de Service Essentiels) ou le secteur de la défense, AXA XL est en mesure de s'adapter aux besoins spécifiques de l'entreprise. Nous veillons à ce que nos clients soient prêts à agir rapidement et efficacement en cas d'attaque, en élaborant un plan de réponse aux incidents adapté à leurs besoins. En accord avec nos clients, des protocoles personnalisés de gestion de sinistre peuvent être mis en place pour s'aligner sur leur organisation et leurs exigences spécifiques.

Vers le « sur-mesure » pour les structures de grande taille

Au-delà de nombreux services inclus - gestion de crise, formation et sensibilisation des employés au risque cyber, réunions d'onboarding et de suivi - les grandes entreprises peuvent accéder à des services complémentaires, conçus sur-mesure.

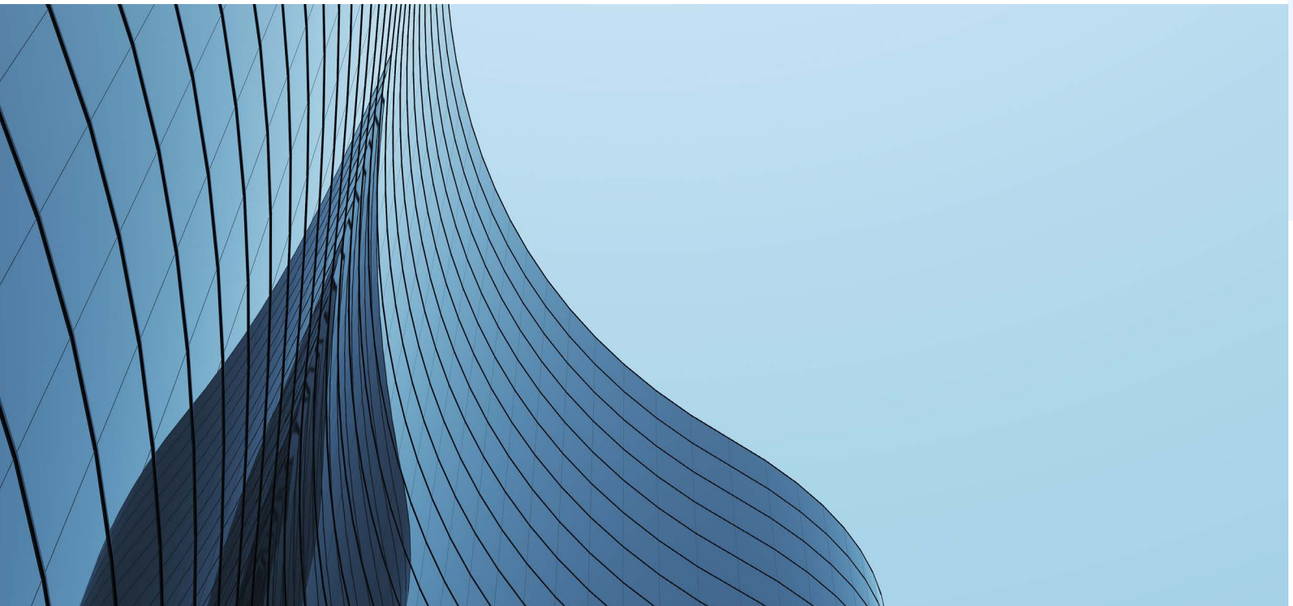
AXA XL peut également adapter le montant de la capacité et de la franchise aux enjeux des entreprises.

Grâce à son implantation internationale, AXA XL peut couvrir des entreprises présentes dans différentes régions du monde. Les multinationales peuvent ventiler la couverture dans les régions où elles sont présentes, afin d'adapter cette couverture aux niveaux de risques locaux.
Par exemple : sur un montant de couverture de 30M€, l'entreprise peut décider d'une couverture de 15M€ aux Etats-Unis, 10M€ en France et 5M€ en Suisse.

L'AVIS DE L'EXPERTE

De nombreux assureurs rencontrent des difficultés à proposer des polices d'assurance dans plusieurs pays. AXA XL est idéalement positionnée pour adresser cet enjeu grâce à son vaste réseau international, qui accompagne des clients dans plus de 208 pays et territoires.
Nous sommes en mesure d'offrir des programmes d'assurance cyber multinationaux, combinant des couvertures globales et locales.
Notre capacité à proposer des garanties adaptées aux spécificités locales permet aux entreprises de bénéficier de solutions sur mesure, alignées avec leurs besoins opérationnels, tout en s'appuyant sur la solidité et l'expertise d'un assureur mondial.
Cela permet à nos clients de gérer efficacement la complexité des risques cyber à travers différents marchés.

VANESSA LEEMANS,
Head of Cyber, UK & Lloyd's, AXA XL, a division of AXA



AXA, un acteur au cœur de l'écosystème cyber

Vers de nouvelles formes de gestion du risque cyber

Internaliser une partie du risque cyber à travers le « captive fronting »

Qu'est-ce que c'est le captive *fronting* ?

Une captive est une société d'assurance créée par une entreprise pour couvrir ses propres risques. Dans le cadre des risques cyber, elle permet d'internaliser une partie du risque, mieux le maîtriser et adapter les couvertures à ses besoins spécifiques. C'est une solution pertinente pour les grandes entreprises matures dans leur gestion des risques.

Comme une captive ne peut pas toujours émettre de contrats en direct, notamment à l'international, AXA XL intervient en tant qu'assureur « fronting ». Nous émettons la police, gérons la conformité et les sinistres, tout en transférant une partie du risque cyber à la captive. Ce modèle allie sécurité juridique, souplesse et maîtrise des coûts.

Quels sont les avantages pour une entreprise qui choisit ce modèle ?

Les avantages sont multiples :

Réduction des coûts : en absorbant une partie du risque, l'entreprise réduit le coût de sa prime assurantielle.

Personnalisation des garanties : possibilité d'exclure les sinistres mineurs ou de cibler des risques spécifiques à un secteur.

Accès à notre expertise : à travers un réseau d'experts techniques et juridiques ainsi qu'un accompagnement dédié à la gestion des sinistres.

Toutes les entreprises peuvent-elles créer une captive ?

Pas nécessairement. C'est une solution destinée aux organisations matures, qui ont une vision claire de leur exposition au risque et les capacités financières pour assumer une part des sinistres. Nous les accompagnons dans cette réflexion et dans leur mise en œuvre, de manière progressive et sécurisée.

CARLOS RODRIGUEZ SANZ,
Cyber Regional Product Leader APAC & Europe, AXA XL, a division of AXA

La gestion du risque à l'ère de l'Intelligence Artificielle

Nouveauté : l'extension de garantie « Gen AI »

Pour accompagner les entreprises dans l'adoption sécurisée de l'intelligence artificielle générative, AXA XL a récemment intégré une extension de garantie dans le contrat CyberRiskConnect. Cette garantie « Gen AI » étend la couverture aux risques spécifiques que les organisations peuvent rencontrer lors du développement ou de l'intégration de leurs propres modèles d'IA générative.

L'Intelligence Artificielle au service de l'amélioration continue de la prévention cyber

L'AVIS DE L'EXPERTE

AXA XL développe un modèle d'intelligence artificielle pour croiser les informations issues des déclarations de sinistres avec les mesures de sécurité mises en place par les entreprises. L'objectif : évaluer l'efficacité des mesures sur la fréquence ou la gravité des incidents. Grâce à cette approche, nous pourrons aider nos clients à arbitrer entre différents investissements en cybersécurité.

MICHELLE CHIA,
Chief Underwriting Officer Cyber, Design & Select Professional, Americas, AXA XL, a division of AXA

Glossaire

ANSSI
Agence nationale de la sécurité des systèmes d'information : agence nationale française, autorité nationale en matière de cybersécurité en France. Elle a pour mission de protéger les systèmes d'information de l'État, des administrations, des opérateurs d'importance vitale et du secteur privé. L'ANSSI intervient également dans la prévention, la détection et la réponse aux incidents de cybersécurité.

Attaque ciblée
Action malveillante délibérément dirigée contre une organisation, une entreprise, un gouvernement ou une personne spécifique, avec des objectifs précis tels que l'espionnage, le vol de données sensibles, le sabotage ou l'extorsion. Contrairement aux attaques opportunistes, les attaques ciblées reposent souvent sur une phase de reconnaissance approfondie et l'usage de techniques personnalisées (phishing sur mesure, exploitation de vulnérabilités spécifiques, ingénierie sociale, malware sur mesure).

Attaque multivectorielle
Cyberattaque combinant plusieurs vecteurs ou méthodes d'intrusion simultanément ou successivement afin d'augmenter ses chances de succès et de contourner les défenses de sécurité. Une attaque multivectorielle peut par exemple mêler phishing, exploitation de vulnérabilités logicielles, déni de service distribué (DDoS) et propagation de malware, ciblant à la fois les systèmes, les réseaux et les utilisateurs.

Attaque par déni de service distribué (DDoS)
Cyberattaque qui consiste à submerger un service, un site web ou une application avec un trafic massif provenant de multiples sources, souvent via un réseau de machines compromises (botnet), dans le but de le rendre lent, instable ou indisponible.

Attaque par rebond
Méthode d'intrusion dans laquelle un cybercriminel ne s'attaque pas directement à sa cible finale, mais passe d'abord par un tiers moins protégé (fournisseur, prestataire, partenaire, filiale). Ce « rebond » lui permet ensuite d'accéder au système principal visé.

Authentification multifacteur / MFA
Cette méthode de sécurité requiert au moins deux « preuves » différentes pour accéder à un compte, service ou système en ligne. Ces facteurs, propres à chaque individu, relèvent des catégories suivantes :

- Facteur de connaissance : « ce que je sais » (par exemple un mot de passe, un code PIN, une réponse à une question secrète).
- Facteur de possession : « ce que je possède » (un élément secret non mémorisable, contenu dans un objet physique qui en protège l'extraction, tels qu'une carte à puce, un token, un téléphone, etc.).
- Facteur inhérent : « ce que je suis » (caractéristique personnelle biométrique (empreinte digitale, rétinienne, ADN) ou comportementale (voix, rythme de frappe au clavier, etc.).

Botnet
Réseau de dispositifs informatiques (ordinateurs, serveurs, objets connectés) compromis et contrôlés à distance par un acteur malveillant, souvent à l'insu de leurs propriétaires. Chaque appareil infecté devient un bot (ou zombie), pouvant être utilisé pour mener des actions coordonnées : attaques par déni de service distribué (DDoS), envoi massif de spams, vol de données, minage de cryptomonnaie ou diffusion de malwares.

CCPA (California Consumer Privacy Act)
La Loi CCPA accorde aux résidents de Californie des droits étendus sur leurs données personnelles (droit d'accès, de suppression, d'opposition à la vente des données), et impose aux entreprises des obligations de transparence et de sécurité.

Crime-as-a-service (CaaS)
Outils et services prêts à l'emploi mis à disposition sur le dark web par des cybercriminels, permettant à d'autres acteurs de mener des attaques sans avoir de compétences techniques avancées. Cela inclut par exemple des ransomwares, des botnets, des kits de phishing ou des services de fraude.

CryptoLocker
Nom donné à l'un des premiers ransomwares de grande ampleur, apparu en 2013. Ce logiciel malveillant infectait les ordinateurs via des pièces jointes piégées, chiffrait les fichiers de la victime et exigeait une rançon (souvent en cryptomonnaie) pour en restaurer l'accès.

Deepfake
Contenu audiovisuel (vidéo, image ou audio) généré ou manipulé à l'aide de techniques d'intelligence artificielle, dans le but de faire croire qu'une personne a dit ou fait quelque chose qu'elle n'a jamais réellement dit ou fait.

EDR (Réponse aux incidents sur terminaux)
L'EDR est une solution de sécurité des équipements terminaux reliés au système d'information. Par son action d'analyse comportementale, il permet la détection des menaces évolutives ou encore inconnues, ainsi que la réaction en cas d'incident (isolation d'un poste, blocage, arrêt d'un processus, etc.). Un EDR peut être managé, c'est-à-dire que la surveillance et l'analyse sont confiées à un prestataire externe.

ERP (Progiciel de gestion intégré)
Système logiciel centralisé qui intègre et automatise les principales fonctions opérationnelles d'une organisation, telles que la gestion financière, les ressources humaines, la chaîne logistique et la production.

Experts forensic
Experts techniques spécialisés dans l'analyse et l'investigation des incidents de cybersécurité, visant à comprendre l'origine, l'ampleur et la méthode d'attaque.

Faille zero-day
Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.(1) Le terme « zero-day » désigne une faille découverte par des attaquants avant même que le développeur en ait connaissance, ne lui laissant aucun délai pour publier un correctif. Ces failles sont particulièrement dangereuses car elles peuvent être exploitées avant la mise à disposition d'une mise à jour de sécurité ou d'une protection antivirus.

(1) ANSSI, CyberDico

GLBA (Gramm-Leach-Bliley Act)
La Loi Gramm-Leach-Bliley encadre la protection des informations personnelles des clients par les institutions financières aux États-Unis. Elle impose aux banques, assurances et autres établissements financiers de sécuriser les données privées, d'informer les clients sur le partage de leurs informations, et interdit l'obtention frauduleuse de ces données.

Hacktivists
Individus ayant pour objectif de véhiculer des messages et idéologies en ayant recours à différentes cyberattaques pour amplifier l'écho de leur action.(1)

Hameçonnage (phishing)
Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. Les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.(1)

HIPAA (Health Insurance Portability and Accountability Act)
La Loi HIPAA protège les informations médicales personnelles des patients aux États-Unis, en imposant des règles de confidentialité et de sécurité pour leur utilisation et leur transmission.

Ingénierie sociale
Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.(1)
Contrairement aux attaques purement techniques, l'ingénierie sociale cible la vulnérabilité humaine. Elle peut prendre diverses formes : appels téléphoniques frauduleux, usurpation d'identité, hameçonnage (phishing).

Logiciel malveillant (malware)
Programme dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, ...) et, souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Il s'implante au sein de programmes, se duplique à l'insu des utilisateurs, et peut nécessiter l'intervention explicite de ces derniers pour se propager (ouverture d'un courrier électronique, lancement d'un programme exécutable, etc.).(1)

Logiciel non patché
Logiciel dont les mises à jour de sécurité (correctifs ou « patchs ») disponibles n'ont pas été appliquées, laissant les vulnérabilités connues ouvertes aux attaques.

Patch management (gestion des correctifs)
Processus consistant à identifier, tester et déployer régulièrement les mises à jour et correctifs logiciels afin de corriger les vulnérabilités et maintenir les systèmes informatiques sécurisés. Une gestion efficace des correctifs réduit significativement les risques d'exploitation par des cyberattaquants et contribue à la continuité des activités de l'entreprise.

PCA (Plan de Continuité d'Activité)
Dispositif prévoyant des procédures pour maintenir les opérations essentielles d'une organisation en cas de perturbation majeure, assurant ainsi la résilience face aux crises.

(1) ANSSI, CyberDico

SOMMAIRE

PRA (Plan de Reprise d'Activité)
Ensemble des procédures et dispositifs de secours des moyens informatiques pour la reprise des capacités du système d'information lorsqu'une perturbation se produit. Le PRA est l'une des composantes du Plan de Continuité Informatique (PCI).

PRI (Plan de Réponse à un Incident)
Document ou dispositif structuré définissant les procédures et responsabilités à suivre lorsqu'un incident de cybersécurité survient.

Rançongiciel (ransomware)
Type de malware qui chiffre les fichiers ou verrouille l'accès à un système informatique, en exigeant le paiement d'une rançon pour en restaurer l'accès.

Rançongiciel-as-a-service (RaaS)
Outils prêts à l'emploi de type rançongiciel proposés sur le dark web par des développeurs. Ces outils permettent à des individus ne disposant pas de compétences techniques avancées de mener des attaques par rançongiciel, en louant ou en achetant l'accès aux logiciels.

Software as a Service (SaaS)
Modèle de distribution de logiciels dans lequel l'application est hébergée par un fournisseur et accessible via Internet, généralement par abonnement.

Shadow IT
Ensemble des outils, applications ou services numériques utilisés au sein d'une organisation sans validation ni contrôle de la direction informatique (par exemple un stockage cloud personnel ou une messagerie instantanée non autorisée).

Technologies quantiques
Ensemble de technologies reposant sur les principes de la physique quantique qui exploitent des phénomènes tels que la superposition et l'intrication pour traiter et transmettre l'information de manière fondamentalement différente. Ces technologies ont des applications majeures en calcul haute performance, communication sécurisée et cryptographie. En cybersécurité, ces technologies sont porteuses d'opportunités (notamment via la cryptographie quantique garantissant une communication ultra-sécurisée) mais aussi de menaces. Les ordinateurs quantiques, une fois suffisamment puissants, pourraient en effet casser les algorithmes cryptographiques classiques, rendant obsolètes de nombreux systèmes de protection actuels.

TIC
Technologies de l'Information et de la Communication.

VPN : Réseau privé virtuel
Outil qui permet de créer une connexion sécurisée et chiffrée entre un utilisateur et un réseau distant via Internet. Le VPN protège les échanges de données contre les interceptions et masque l'adresse IP réelle de l'utilisateur. Il est utilisé dans les entreprises pour sécuriser le télétravail et l'accès aux ressources internes.

Vulnérabilités
Failles ou faiblesses présentes dans un système informatique, un logiciel, un matériel ou un processus, susceptibles d'être exploitées par un acteur malveillant pour compromettre la confidentialité, l'intégrité ou la disponibilité des données ou des services.

Remerciements

Nous souhaitons adresser nos sincères remerciements à toutes les personnes qui ont contribué à la réalisation de ce livre blanc. Leur concours a permis d'apporter des éclairages concrets, des recommandations pratiques et une vision constructive de la prévention cyber.
À travers cet ouvrage notre ambition est de poursuivre une mission qui nous tient à coeur : éveiller les consciences face aux risques cyber et aider les entreprises à se prémunir efficacement.

Cécile Augeraud
Rébiah Bardot-Girard
Libby Benet
Guillaume Bercier
Michelle Chia
Frédéric Coppin
Frédéric de Courtois
Mathieu Cousin
Luc Declerck
Jonathan Drikes
Manuel Fontanier
Xavier Hartout
Philippe Hermetz
Coppélia Joly
Vanessa Leemans
Jean-Pierre Marbaix
Gwenaëlle Martinet
Benoît Mauvais
Jean-Luc Montané
Thierry Piton
Charlotte Prieur
Carlos Rodriguez Sanz
Christine Sinibardy
Stéphane Vauterin

Coordination
Myriam Desgroux

Directeur de la publication
Aude de Vorges

Rédaction
Equancy

Découvrez la version digitale

Vous souhaitez bénéficier d'un accompagnement adapté ?
Contactez votre interlocuteur AXA.

Réf. 2007566 0725 - Solutions Graphiques - Crédit photo : Adobe Stock, Gettyimages