Assurance et Banque

# Cyber Study

## Observatoire de la sinistralité cyber

# Edito

Le risque cyber s'impose aujourd'hui comme une préoccupation majeure pour les entreprises, tous secteurs et toutes tailles confondues. Il figure ainsi au 3e rang des risques émergents mondiaux identifiés par le Future Risks Report d'AXA de 2025(1), tous publics, avec un classement dans le trio de tête continu depuis 8 ans.

Une inquiétude qui vient refléter la réalité d'un risque systémique en plein essor : le panorama de la cybermenace 2024 publié par l'ANSSI, révèle ainsi une augmentation de 15 % des cyberattaques en France sur un an seulement.

Derrière ces chiffres il y a des conséquences dommageables multiples : la perte de données, de ressources financières, la paralysie des infrastructures, l'atteinte de la réputation de l'entreprise, ou encore les impacts sociaux et psychosociaux sur le collectif.

Dans ce contexte, AXA France ne cesse de renforcer son accompagnement en cybersécurité pour les clients, à la fois en prévention, en gestion de crise, et en renforçant la résilience des entreprises victimes d'attaques.

Assureur d'une entreprise sur trois en France, nous sommes dotés d'une vision panoramique de la menace cyber en France, en évolution permanente. Ce sont les résultats de « ce tableau des risques » que nous avons pensé utile de partager au plus grand nombre, afin de mieux sensibiliser les entreprises, de nourrir le débat public et de contribuer à l'essor d'une véritable culture de la prévention cyber dans notre pays.

Il s'agit bien sûr d'une première photographie de la sinistralité cyber - avec les limites méthodologiques que cela impose. Elle est établie à partir d'un échantillon spécifique : l'ensemble des dossiers sinistres cyber clos en 2024 pour AXA France, quelle que soit leur année de survenance.

Le suivi sur le long terme des tendances dégagées permettra d'en préciser la portée et d'en affiner encore l'analyse.

Je vous souhaite une très bonne lecture !

**Mathieu Godart**
Directeur Général d'AXA IARD et Partenariats

« AXA France souhaite être un pilier de la résilience cyber pour les entreprises »

(1) Panorama global de la perception des risques à venir par un double panel – grand public et experts. Au total, plus de 23 000 répondants à travers le monde.

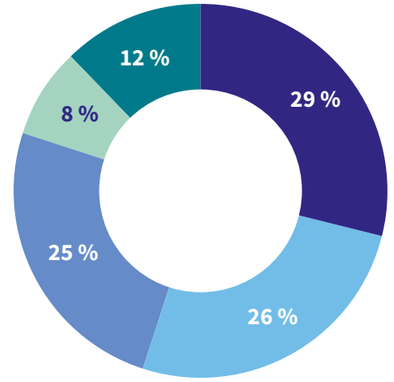
# Sommaire

# Une **sinistralité contenue chez AXA France**, pour une menace qui touche toutes les entreprises, quelle que soit leur taille

Malgré une intensification nette des attaques cyber en France, la fréquence des sinistres reste contenue au sein du portefeuille client d'AXA France (1,6 % en 2024 contre 1,4 % en 2021), par rapport aux tendances nationales, avec une augmentation limitée à 14 % sur 4 ans, cela s'explique probablement par la montée en puissance de la prévention. Un résultat qui appelle néanmoins à la vigilance continue face à une menace en constante mutation.

La principale menace recensée est l'usage de rançongiciels, avec près d'un sinistre sur trois, suivis de près par les piratages et les intrusions ainsi que la fraude. Avec des degrés d'ingéniosité divers, ces procédés relèvent tous in fine de la motivation pécuniaire.

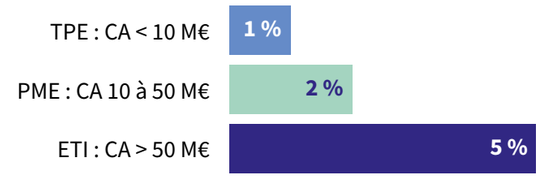
**Typologie de sinistres (%)**




Même si cette cybercriminalité touche particulièrement les ETI (Entreprises de Taille Intermédiaire), probablement avec des perspectives de gains conséquents, aucun type d'entreprise n'est épargné, y compris les TPE (Très Petites Entreprises), logiquement moins bien préparées et protégées que les plus grosses structures.

**Toutes les entreprises sont touchées par les cyber attaques. On peut noter que les TPE (CA < 10 M€), bien que deux fois moins victimes que les PME (Petites et Moyennes Entreprises), ne sont pas épargnées.**

**Fréquence des sinistres par taille d'entreprises en %**

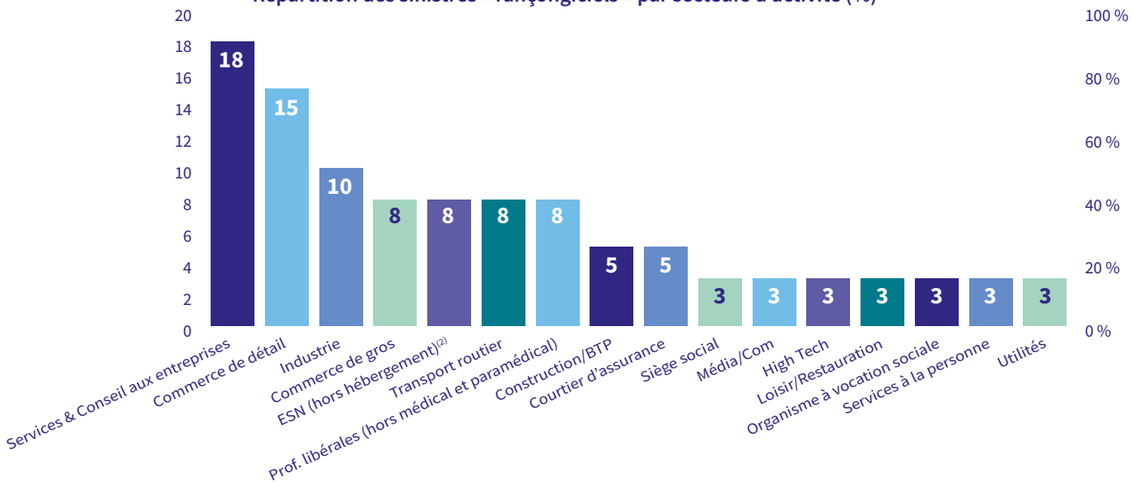


# Les **secteurs les plus visés** par type d'attaque : le reflet des spécificités de leurs activités

## Si l'on s'intéresse aux secteurs visés pour les principaux types d'attaques, on constate que :

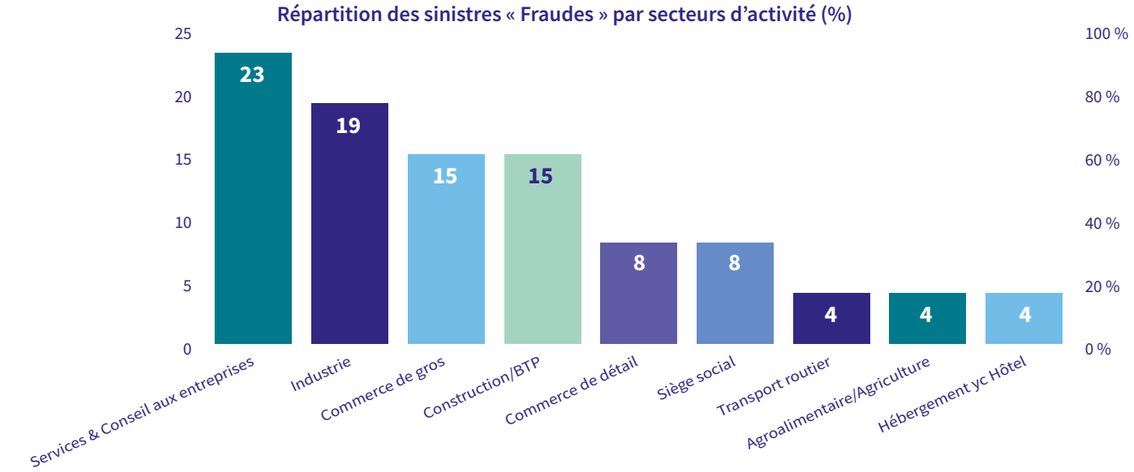
- Les secteurs du service et conseil aux entreprises, de l'industrie et du détail sont les premiers touchés par les **rançongiciels**. Les petits commerçants, malgré leur moindre exposition numérique, ne sont pas épargnés par cette cybercriminalité, qui est le plus souvent opportuniste.

**Répartition des sinistres « rançongiciels » par secteurs d'activité (%)**




- Les secteurs du service et conseil aux entreprises, de l'industrie et du commerce de gros sont les plus concernés par **les fraudes**, ce qui correspond à leur modèle d'activité transactionnel.

**Répartition des sinistres « Fraudes » par secteurs d'activité (%)**




- Pour ce qui est **des piratages et des intrusions**, ce sont les secteurs du commerce de gros, de détail, l'industrie, mais également le secteur de la construction, qui sont les plus impactés. On peut y voir la conséquence de la valeur de leurs données, dans des contextes concurrentiels forts.

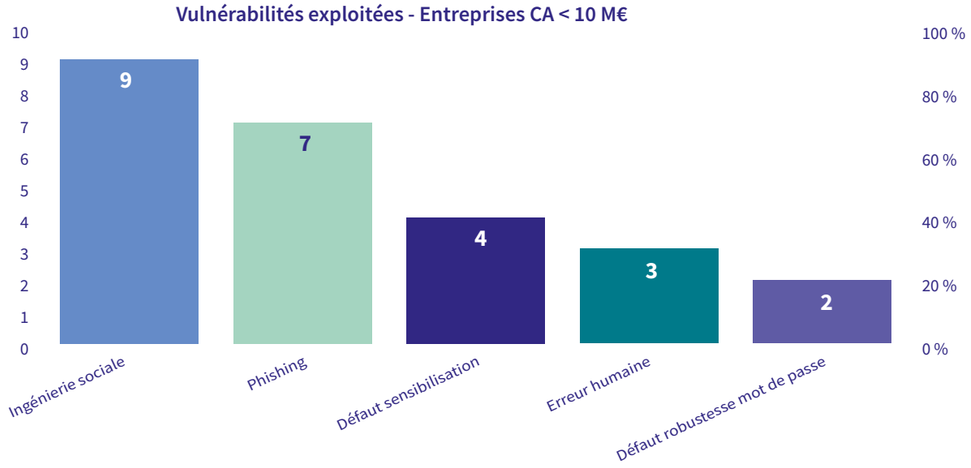
(2) Entreprise de Services du Numérique.

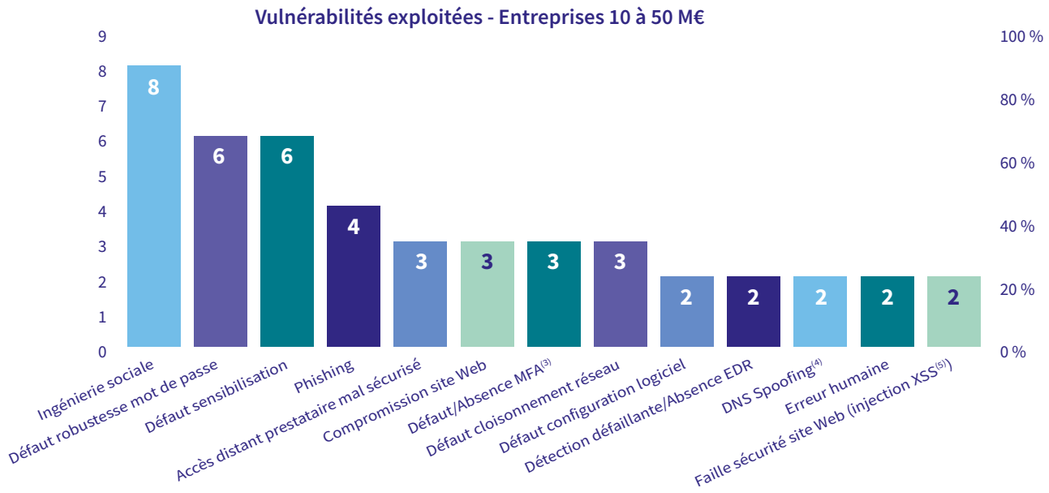
# Les principales **vulnérabilités exploitées par taille d'entreprise** : un potentiel fort de prévention

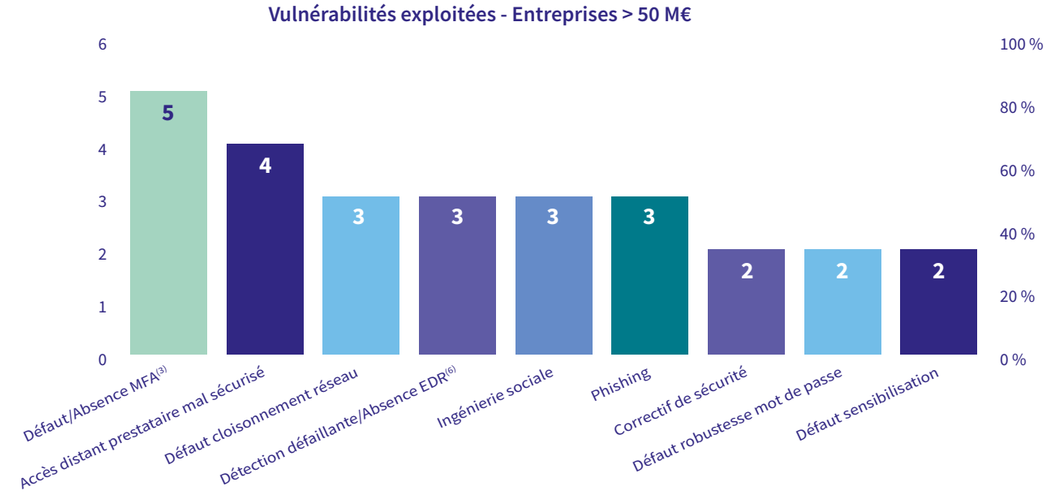
Quelle que soit la taille de l'entreprise, on constate que les vulnérabilités humaines sont un facteur de risque déterminant, dû au défaut de formation des employés au phishing.

Les vulnérabilités humaines sont le premier facteur exploité pour les attaques des TPE. Pour les PME, elles s'accompagnent des faiblesses des processus d'authentification (faible robustesse des mots de passe, absence d'authentification multifacteurs). Et elles viennent juste après les faiblesses organisationnelles et techniques pour les ETI, ce qui s'explique par une surface d'attaque plus importante pour cette catégorie d'entreprises.

Le facteur humain étant prépondérant, **la formation des salariés constitue donc un formidable levier de prévention**, qui en outre présente l'avantage d'être déployable à des coûts limités.




(3) MFA - Authentification multifacteur.
Cette méthode de sécurité requiert au moins deux « preuves » différentes pour accéder à un compte, service ou système en ligne. Ces facteurs, propres 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.).

(4) Le DNS Spoofing (ou falsification DNS) est une technique d'attaque qui consiste à manipuler ou à falsifier les réponses d'un serveur DNS afin d'orienter un utilisateur vers un site malveillant ou non souhaité.

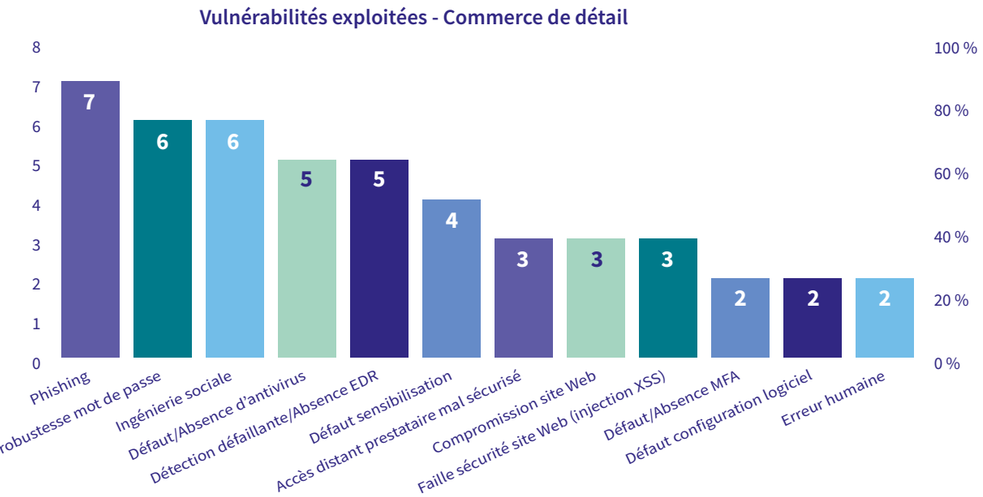
(5) L'injection XSS (Cross-Site Scripting) est une vulnérabilité de sécurité des applications web qui permet à un attaquant d'injecter du code malveillant, généralement du script JavaScript, dans une page web consultée par d'autres utilisateurs.

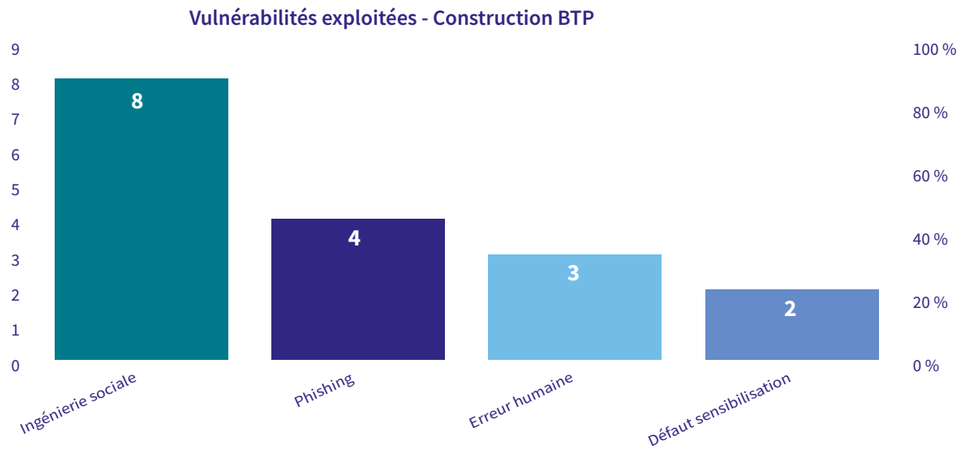
(6) EDR (Réponse aux incidents sur terminaux). L'EDR est une solution de sécurité des équipements terminaux reliés au système d'information. Par son action d'analyse comportementale, il permet la détection des menaces évolutives ou encore inconnues, ainsi que la réaction en cas d'incident (isolation 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.

# Les principales **vulnérabilités exploitées par type d'entreprise**, témoignage d'une culture du risque à plusieurs vitesses

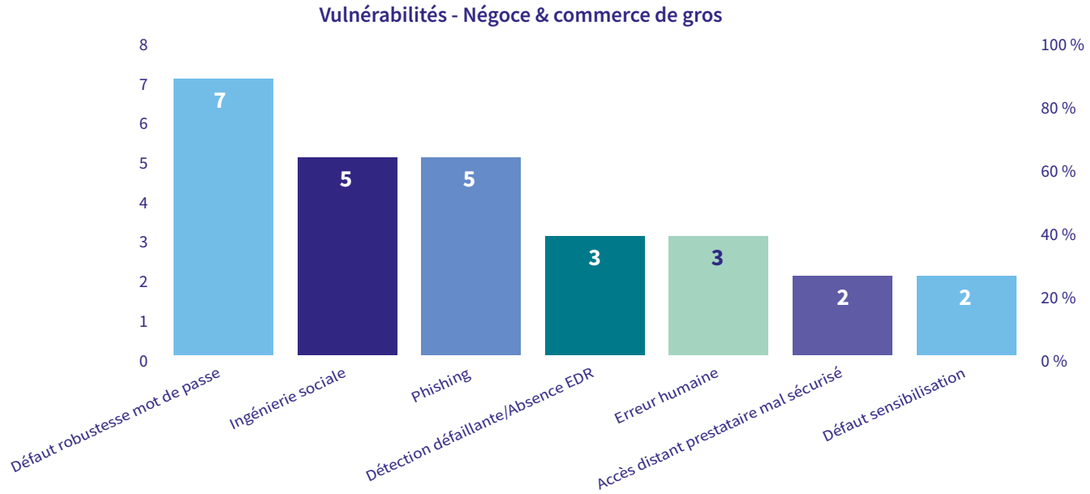
**En entrant dans le détail, par secteur, des principales vulnérabilités, on distingue :**

- **Un premier groupe**, celui des entreprises où les vulnérabilités humaines prédominent très largement, comme le secteur du commerce de détail, ou celui de la construction. Cela reflète la situation d'entreprises dont l'activité est peu tournée vers le numérique, et où la prise en compte de la menace cyber est très peu développée.



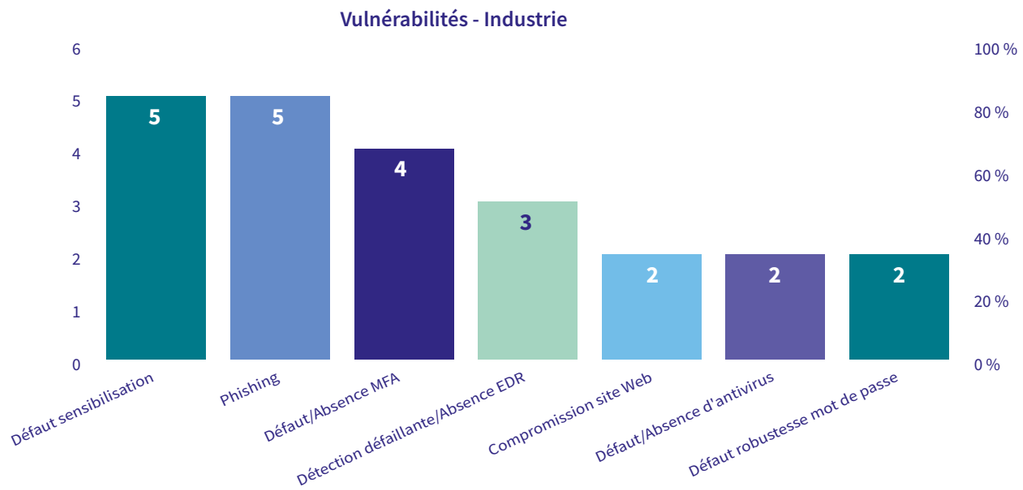

- **Un deuxième groupe** où les enjeux d'authentification sont le premier facteur de vulnérabilité. On y retrouve les secteurs du commerce de gros et du transport, dont le modèle suppose des structures IT[7] plus ouvertes, où des acteurs étrangers à l'entreprise, notamment des prestataires, sont susceptibles d'interagir.

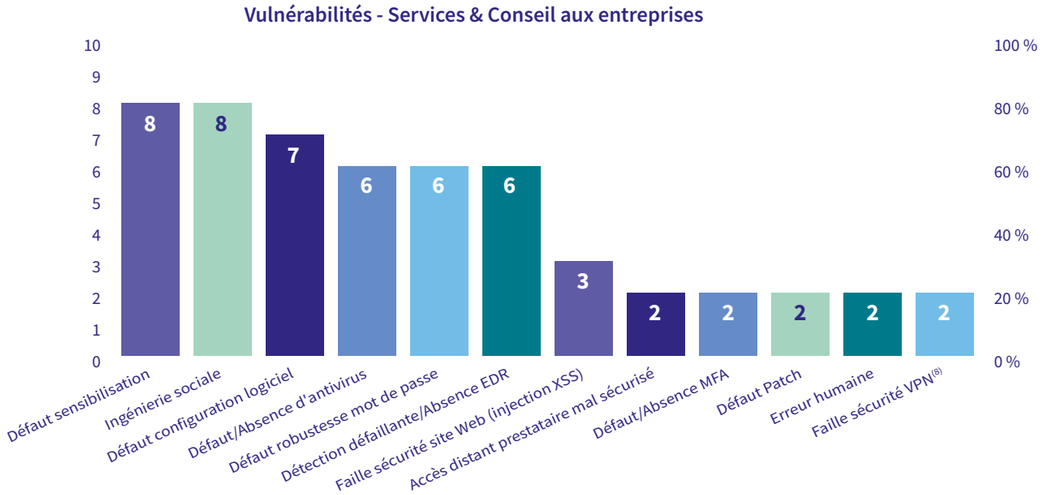




(7) L'infrastructure de technologie de l'information – « IT » (ou infrastructure informatique) désigne l'ensemble des composants matériels, logiciels et réseau dont dépendent les entreprises pour gérer et exploiter efficacement leurs environnements informatiques.

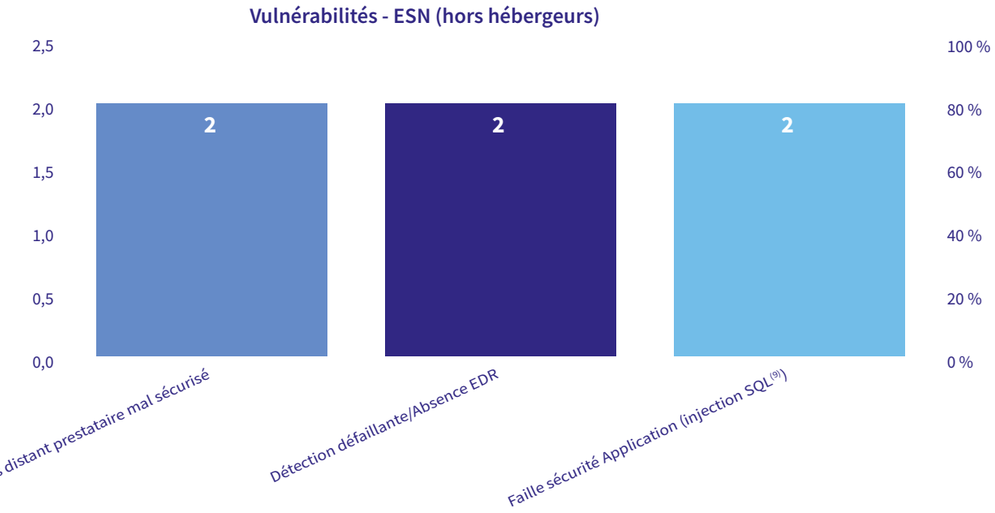
- **Un troisième groupe**, au profil de vulnérabilité plus mixte, avec les secteurs de l'industrie et des services et conseils aux entreprises. Cela correspond à des secteurs plus exposés car à l'infrastructure IT plus conséquente, et où le facteur humain reste déterminant. On note en particulier que l'absence d'une solution de protection des équipements terminaux informatiques de type EDR, est un facteur important ayant favorisé la réussite de cyber attaques.




(8) 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.

- Enfin, pour les entreprises de l'économie des services du numérique, ce sont logiquement les vulnérabilités techniques qui sont en tête, à l'image d'un secteur où les employés sont naturellement bien au fait des enjeux de sécurité cyber. En particulier, l'exploitation de faiblesses des dispositifs permettant l'accès distant aux systèmes d'information de leurs propres clients est à souligner.




(9) Une vulnérabilité qui permet à un attaquant d'insérer ou d'injecter du code SQL malveillant dans une requête envoyée à une base de données via une application web. Cette vulnérabilité peut entraîner la divulgation, la modification ou la suppression de données sensibles, voire un accès non autorisé à l'ensemble du système.

# **L'impact des attaques cyber :** étude des suites des attaques par rançongiciels

**Les attaques cyber ont un impact massif sur les entreprises touchées, mais il est encore difficile d'en proposer un chiffrage complet, à la fois par manque de recul, par la difficulté à embrasser l'ensemble de leurs répercussions, et par les extrêmes variations constatées d'un cas à l'autre.**

### On distingue ainsi :

- **Les coûts directs :**
  - atteinte à l'activité,
  - vol/pertes de données,
  - coûts inhérents à la gestion de l'évènement : investigations numériques, récupération et restauration des données, remise en état du système d'information, frais de communication de crise,
  - frais exposés dans le cadre d'enquêtes de la CNIL (Commission Nationale de l'Informatique et des Libertés) et frais de notification individuelle aux personnes concernées par une violation de leurs données à caractère personnel,
  - engagement de responsabilités,
  - éventuelles amendes ou sanctions liées à une non conformité réglementaire,
  - coûts de renforcement du niveau de sécurisation du système d'information.

- **Les coûts indirects :**
  - atteinte à l'image, perte de clientèle, perte de talents en interne, perte de confiance de l'écosystème de l'entreprise : banques, fournisseurs, sous traitants, partenaires…,
  - coûts de restauration de l'image de marque,
  - atteinte psychologique des acteurs ayant géré la crise sur le temps long.

Dans une première approche, nous avons étudié l'impact des attaques par rançongiciels sur nos clients, qui offrait une base d'étude suffisamment significative. Nous avons porté une attention particulière à la durée complète de perturbation du fonctionnement normal de l'entreprise, qui nous paraît être un indicateur éclairant de l'ampleur des dommages causés.

Il en ressort que 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 quant à lui **de 16 jours en moyenne**, avec de forts écarts – 1 à 111 jours. Il varie en particulier selon le degré de maturité en termes de cybersécurité de la structure.

Dans le cas d'attaques de type rançongiciel, la part de la perte d'exploitation représente **environ 70 % du montant total du sinistre**.

Dans **17 % des attaques recensées**, les sauvegardes ont été compromises, ce qui a eu pour conséquence d'augmenter significativement le délai de retour à la normale.

# Avis d'expert

## Le double paradoxe de la prévention cyber des PME

**Christine Sinibardy**
Directrice Risques Techniques
et Cyber d'AXA France

Cette étude met en avant un double paradoxe : les TPE/PME sont de plus en plus exposées aux attaques cyber (+ 53 % d'attaques en 2024 suivant une étude d'Orange Cyber Défense), alors qu'elles investissent encore peu dans leur cybersécurité, faute de moyens, mais également parce qu'elles ne se sentent pas encore suffisamment concernées par ce risque.

Les TPE et les PME présentent des vulnérabilités humaines et techniques, notamment dans les processus d'authentification. Des actions simples et peu coûteuses comme la formation des employés au phishing ou la mise en place de mesures de base d'hygiène informatique (telles qu'une politique de mots de passe robuste, l'existence de sauvegardes exploitables en cas d'incident) permettent d'améliorer significativement la sécurité et la résilience de ces entreprises face à une attaque cyber.

Il est important d'agir sur les leviers permettant de réduire la probabilité de survenance d'une attaque, mais également sur ce qui permet, le jour où l'attaque survient, d'en réduire les conséquences.

L'existence de sauvegardes fiables et de plan de reprise d'activité seront clés pour permettre une reprise rapide de l'activité, au moins en mode dégradé. Une entreprise non préparée risque de ne pas se relever d'une attaque cyber.

Chez AXA, nous nous engageons à accompagner nos clients en leur fournissant des outils et des conseils adaptés pour renforcer leur résilience cyber. La connaissance approfondie du risque et une veille constante sont indispensables pour anticiper et contrer les menaces futures.

# Conclusion

**Cette première étude de la sinistralité cyber sur l'ensemble de nos entreprises clientes est riche d'enseignements sur l'état de la menace en France aujourd'hui.**

**Trois aspects semblent particulièrement significatifs :**

- Tout d'abord, la cybercriminalité se distingue par son adaptabilité. Elle vient jouer sur les faiblesses propres à chaque modèle d'activité, et à chaque structure IT.
- Ensuite, ses conséquences obéissent à la loi de la peine exponentielle : si les manquements à la cybersécurité facilitent les attaques, ils viennent également en démultiplier les effets, comme l'illustre le prolongement drastique de la durée de paralysie de l'entreprise si l'on ne dispose pas de sauvegarde sécurisée.
- Enfin, on peut limiter cette menace avec des mesures simples de prévention qui sont accessibles, surtout au regard des dommages potentiels. Il s'agit de sensibilisation et de formation des salariés ainsi que de mise en place de mesures de sécurité élémentaires.

Face à une menace en évolution constante, qui peut toucher n'importe quelle entreprise, quelle que soit sa taille ou la nature de ses activités, il est impératif d'agir sans attendre pour mieux garantir son intégrité et sa pérennité.

Aux côtés des chefs d'entreprises et des responsables des systèmes d'information, nous nous engageons à nourrir l'éventail et l'efficacité des mesures de protection mises à leur disposition. Pour cela, la connaissance du risque, son étude, est essentielle. C'est pourquoi nous vous donnons d'ores-et-déjà rendez-vous pour la prochaine édition de cette Cyber Study, afin de suivre au plus près les tendances à l'œuvre, et de caractériser encore plus précisément les vulnérabilités critiques à circonscrire.

**Frédéric Coppin**
Directeur technique et marketing Entreprises



## Remerciements

**Ont contribué à la réalisation de cette publication :**

Alban Claude
Frédéric Coppin
Myriam Desgroux
Mathieu Godart
Jean-Pierre Marbaix
Benoît Mauvais
Thierry Piton
Charlotte Prieur
Christine Sinibardy
Christophe Tiabeu
Aude de Vorges

**Scannez pour découvrir notre Livre Blanc sur la cybersécurité**

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



Réf. 2008063-1025 - CARÎOCA - Crédit photo : Getty Images, Adobe Stock, Shutterstock