



Assurance et Banque

Cyber Study

Observatoire de la sinistralité cyber

Édition 2026



Edito

Le risque cyber est plus que jamais une menace existentielle pour toutes les entreprises, quels que soient leur secteur et leur taille. Avec cette deuxième édition de la Cyber Study, nous poursuivons un engagement qui nous tient particulièrement à cœur : mettre à profit notre vision d’assureur d’une entreprise sur trois en France pour partager, au-delà des seuls chiffres de sinistres, les grandes tendances qui se dessinent.

Notre sinistralité reste maîtrisée, et c’est une bonne nouvelle. Mais derrière cette apparente stabilité, l’étude montre des évolutions profondes : la connexion frauduleuse progresse particulièrement, illustrant le poids croissant de l’identité et des accès dans les attaques, tandis que quelques failles simples expliquent encore l’essentiel des sinistres.

Cette nouvelle édition apporte également des éclairages inédits, notamment sur la survenance des attaques dans le temps. Ces analyses permettent de mieux comprendre comment la menace se synchronise avec la vie réelle des entreprises, et d’orienter plus finement les actions de prévention et de vigilance.

Dans un contexte où l’Intelligence Artificielle accélère la vitesse et la sophistication des menaces, nous avons la conviction que la meilleure protection repose sur trois piliers : la connaissance fine du risque, le partage d’expérience, et un accompagnement de proximité. C’est tout le sens de notre engagement en tant qu’assureur au service de nos clients, pour les aider à prioriser leurs actions et à transformer la cybersécurité en levier durable de performance et de confiance.

Bonne lecture.

Echantillon de l’étude :

- Étude portant sur l’ensemble des sinistres clos en 2025 sur le portefeuille d’assurés cyber d’AXA France, quelle que soit l’année de survenance.
- La sinistralité observée reflète en partie la composition de notre portefeuille, marqué notamment par une proportion significative de TPE PME.
- Compte tenu du nombre encore limité de sinistres et du faible recul temporel, nos résultats doivent être interprétés comme des tendances, et non comme des conclusions définitives.



Corinne Calendini

Directrice Générale d’AXA Vie Individuelle et IARD & Partenariats

Sommaire

6-7



Une sinistralité en évolution,
pour une menace qui ne fait pas
de distinction

18-21



Les failles exploitées chez
les entreprises visées

8-11



Les secteurs les plus visés :
quand la nature de l'activité
oriente la menace

22-25



L'impact des attaques cyber :
le cas des rançongiciels

Avis d'expert
de Christine Sinibardy

12-17



Temporalité des attaques et délais
de détection : une chronologie du
risque déterminante

26

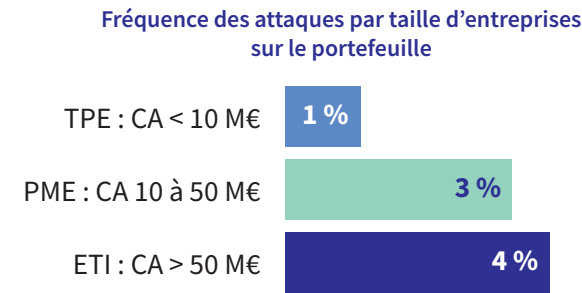


Conclusion
de Frédéric Coppin

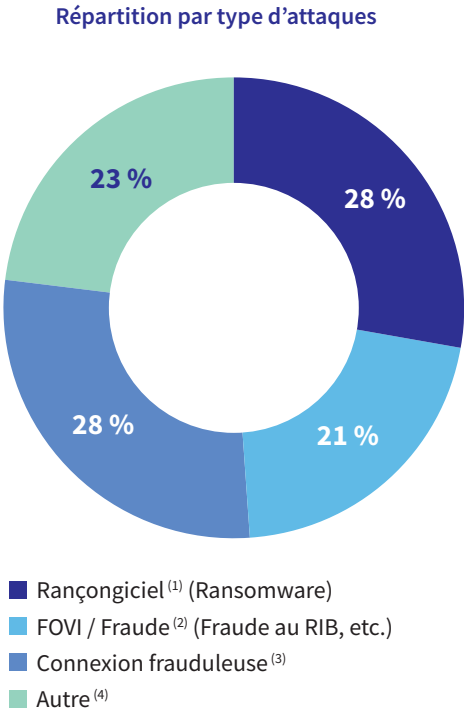
Une sinistralité en évolution, pour une menace qui ne fait pas de distinction

La fréquence des sinistres cyber reste contenue sur notre portefeuille de clients. En 2025, elle s'établit à 1 % pour les TPE (chiffre d'affaires inférieur à 10 M€), 3 % pour les PME (10 à 50 M€) et 4 % pour les ETI (au-delà de 50 M€).

Ces taux traduisent une réalité bien connue : plus l'entreprise est grande, plus sa surface d'attaque est étendue, et plus elle est, de fait, exposée. Mais la taille ne protège pas. Les TPE, bien que statistiquement moins touchées, ne sont pas épargnées. Et leur moindre maturité en matière de cybersécurité peut transformer un incident limité en crise existentielle.



(1) Rançongiciel : Attaques par ransomware avec chiffrement de données, exfiltration, ou blocage d'accès.
(2) FOVI / Fraude : Fraudes aux virements (RIB), fraudes au président, fraudes aux faux supports, etc.
(3) Connexion frauduleuse : Compromission de comptes (messagerie, réseau privé virtuel, etc.), phishing, etc.
(4) Autre : Incidents divers (ex. : Faux positifs, erreurs de configuration, attaques via hébergeurs).



Un paysage des attaques qui s'équilibre

Par rapport à l'année précédente, le trio de tête des menaces reste le même. On note cependant qu'un duo de tête s'affirme plus nettement, avec les rançongiciels et les connexions frauduleuses ex-aequo à 28 % des sinistres, suivi de plus loin par les fraudes, à près de 21 %.

Ce rééquilibrage est un signal important : la montée des connexions frauduleuses révèle un nouveau mode opératoire des attaquants. Elle s'explique à la fois par la multiplication des fuites de données, qui alimentent en identifiants et points d'entrée, et par l'usage de l'IA, qui permet de massifier et d'industrialiser les tentatives. La connexion frauduleuse doit être comprise comme un vecteur de compromission : un accès non autorisé ouvrant la voie à de l'information ou à des systèmes, sans déboucher nécessairement, ni immédiatement, sur une attaque aboutie.



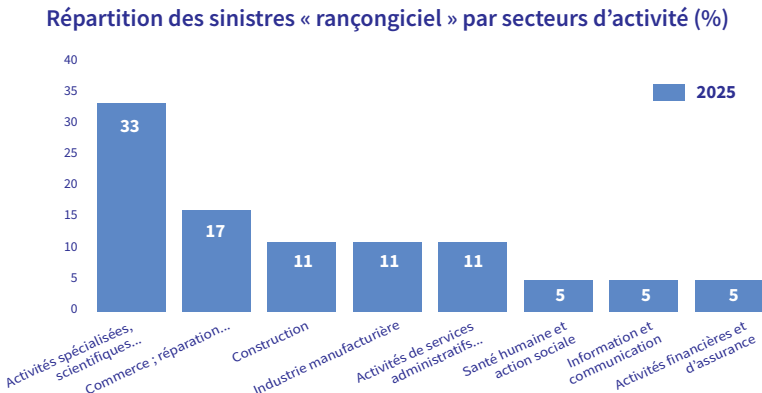
Les secteurs les plus visés : quand la nature de l'activité oriente la menace

Des profils de risque sectoriels bien distincts

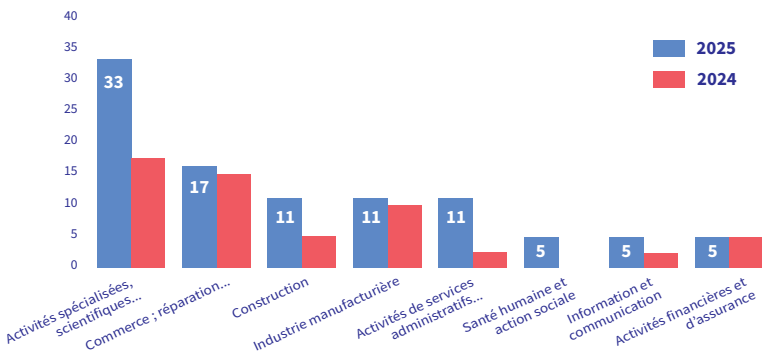
Comme l'an passé, on constate que le type d'attaque subi n'est pas aléatoire : il reflète la structure même de l'activité de l'entreprise affectée, ce qui doit orienter les investissements en cybersécurité, ainsi qu'en prévention.

Pour les rançongiciels, les secteurs les plus touchés sont les activités spécialisées, scientifiques et techniques (1/3 des sinistres rançongiciel). Ce sont des secteurs où la dépendance aux systèmes informatiques est forte, et où une paralysie, même brève, entraîne des pertes d'exploitation immédiates, ce qui en fait des cibles particulièrement rentables pour les attaquants.

Répartition des rançongiciels par secteurs d'activité les plus ciblés



Comparaison des répartitions des sinistres 2024 et 2025 « rançongiciels » par secteurs d'activité (%)



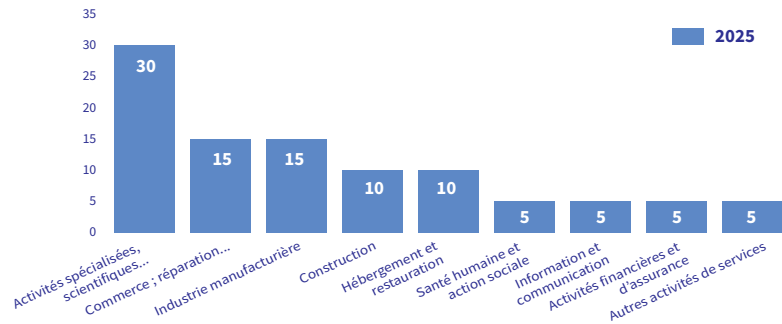


Répartition des connexions frauduleuses par secteurs d'activité les plus ciblés

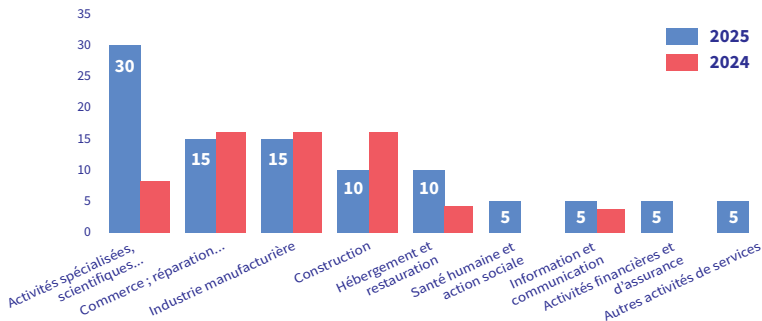
Pour les connexions frauduleuses, le classement est également dominé par les activités spécialisées, scientifiques et techniques (30 % des sinistres, avec une proportion multipliée par un peu moins de x 4 par rapport à l'an dernier), suivi par le commerce et la réparation auto/moto (15 %) et l'industrie manufacturière (15 %).

Ce type d'attaque, qui passe souvent par le phishing ou la compromission de compte, cible logiquement en priorité les secteurs où les collaborateurs sont nombreux à accéder à des ressources en ligne, messageries, outils métiers, ou VPN.

Répartition des sinistres « Connexion frauduleuse » par secteurs d'activité (%)



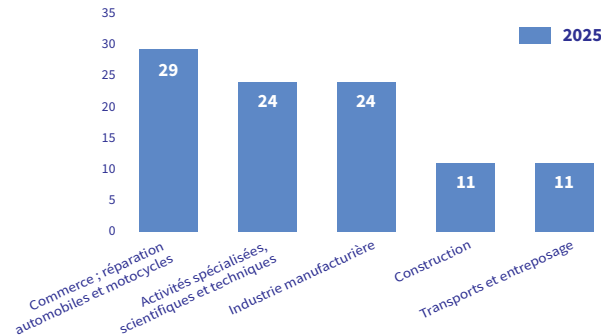
Comparaison des répartitions des sinistres 2024 et 2025 « Connexion frauduleuse » par secteurs d'activité (%)



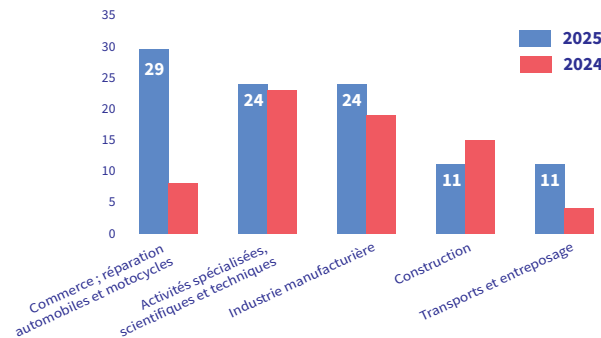
Répartition des fraudes par secteurs d'activité les plus ciblés

Pour les fraudes, le commerce, les concessionnaires et réparateurs auto/moto arrivent nettement en tête (près d'un sinistre sur trois), avec un profil très dynamique par rapport à l'an passé (multiplié par plus de 3,5), suivi des activités spécialisées, scientifiques et techniques et de l'industrie manufacturière (près d'un quart des sinistres chacun). Ces secteurs ont des modèles d'activité très transactionnels, avec des flux financiers réguliers et des échanges fréquents avec des tiers, autant de points d'entrée pour une usurpation d'identité ou une substitution de RIB.

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



Comparaison des répartitions des sinistres 2024 et 2025 « FOVI / Fraudes » par secteurs d'activité (%)



Les attaques s'adaptent au profil des entreprises : si dans le secteur de la construction, les trois types d'attaques sont également représentés, dans le secteur du commerce au sens large, près d'un sinistre sur deux relève de la fraude. Deux secteurs, deux profils de risque qui diffèrent, et donc deux stratégies de protection qui ne peuvent pas être identiques.

Temporalité des attaques et délais de détection : une chronologie du risque déterminante

Les cyberattaques ne frappent pas au hasard. L'analyse fine de la temporalité des sinistres montre au contraire des « fenêtres » de vulnérabilité très marquées, autant dans la semaine que dans la journée ou dans l'année. À cela s'ajoute un autre facteur déterminant : la rapidité de détection, très variable selon la taille de l'entreprise et le type d'attaque.

Quand surviennent les attaques ?

Dans la semaine, deux jours se détachent nettement : lundi et mardi concentrent à eux deux 42 % des sinistres, majoritairement des attaques planifiées (rançongiciels, phishing, fraudes). Le week-end (samedi-dimanche) ne représente que 12 % des sinistres, essentiellement des attaques automatisées ou opportunistes.

Le début de semaine apparaît clairement comme la période la plus critique, au croisement de deux dynamiques : le volume d'échanges (mails, validations, paiements) repart à la hausse, et la fatigue ou la pression du redémarrage peut entamer la vigilance.

Sur la journée, la tendance est tout aussi nette : 67 % des attaques surviennent entre 8 h et 18 h, en lien direct avec des interactions humaines (phishing, fraudes, connexions frauduleuses). Les attaquants ciblent les plages horaires où les collaborateurs sont actifs, disponibles... et susceptibles de cliquer, répondre, valider.

33 % des attaques se produisent entre 18 h et 8 h, plutôt associées à des actions automatisées (rançongiciels, exploitation de vulnérabilités connues – CVE).

Sur l'année, on observe également des saisons du risque : avril, mai et septembre sont les mois les plus actifs, avec respectivement 11 %, 12 % et 11 % des sinistres, souvent liés à des campagnes de rançongiciels et de phishing à grande échelle. Août et décembre affichent une nette baisse d'activité (5 % chacun), sans doute liée aux périodes de congés et à la moindre activité économique.

Cette cyclicité permet d'anticiper : les campagnes de sensibilisation, les tests de phishing ou le renforcement de la vigilance opérationnelle gagneront à être renforcés en amont de ces pics (fin mars, fin avril, fin août) plutôt que de manière uniforme sur l'année.

Temporalité des sinistres

Lundi et mardi concentrent

42 % des sinistres, souvent liés à des attaques planifiées (rançongiciels, phishing).

Week-end (samedi-dimanche) :

12 % des sinistres, souvent des attaques automatisées ou opportunistes.

67 % des attaques surviennent **en journée** (8 h-18 h), souvent liées à des interactions humaines (phishing, fraudes).

33 % des attaques surviennent **la nuit** (18 h-8 h), souvent automatisées (rançongiciels, exploitation de CVE).

Mois à risque

Avril, mai et septembre

sont les **mois les plus actifs** (11 %, 12 % et 11 % des sinistres), souvent liés à des campagnes de rançongiciels.

août et décembre

enregistrent une **baisse d'activité** (5 % chacun), probablement due aux périodes de congés.

Combien de temps pour détecter un incident ?

Un autre aspect clé concerne les délais de détection, avec un constat en deux temps : d'un côté, un nombre significatif d'attaques sont détectées très vite ; de l'autre, une proportion non négligeable reste sous le radar pendant plusieurs semaines.

Globalement, si près d'un sinistre sur 3 est détecté en moins de 24 heures, et près de 60 % en moins d'une semaine, 12 % ne sont détectés qu'au-delà de 30 jours, un délai bien trop long pour limiter les dommages.

La taille de l'entreprise joue un rôle important :

- Pour les structures de moins de 10 M€ de CA, la médiane de détection est de 2 jours, mais la moyenne monte à plus de 12 jours, avec un écart-type élevé. Certaines attaques sont vues presque immédiatement, tandis que d'autres restent invisibles pendant plusieurs semaines.
- Entre 10 et 50 M€, la médiane passe à 3-5 jours, la moyenne à 15-18 jours, avec des écarts encore plus marqués.
- Entre 51 et 100 M€, la médiane grimpe à 10 jours et la moyenne à 22 jours : la détection devient plus lente, malgré des moyens théoriquement plus importants.
- Au-delà de 200 M€, la médiane redescend à 4 jours et la moyenne à 14 jours, signe que les grandes structures les plus matures ont investi dans des capacités de supervision et de détection plus robustes, même si certains sinistres présentent des délais extrêmes.



Tous les sinistres ne sont pas détectés au même rythme

Les délais varient fortement selon le type d'attaque :

Rançongiciel

Médiane de 3 jours, moyenne de 15 jours.
L'impact est souvent brutal, mais la compromission initiale peut remonter à plusieurs semaines. Cela s'explique notamment par le fait que certains rançongiciels ne sont pas utilisés pour paralyser les activités mais dans le cadre d'un chantage à la non-divulgateion des informations récoltées, sans incidence directe sur le fonctionnement de l'entreprise.

Fraude (FOVI)

Médiane de 1 jour, moyenne de 6 jours.
Les flux financiers anormaux sont généralement repérés plus vite, mais parfois après plusieurs opérations.

Connexion frauduleuse

Médiane de 1 jour, moyenne de 7 jours.
Dès qu'un compte est utilisé de manière suspecte, les effets (mails envoyés, opérations inhabituelles) finissent par alerter, mais souvent après plusieurs actions déjà réalisées.

Fuite / vol de données, usurpation d'identité, erreur humaine, e-réputation ⁽⁵⁾

Médiane à 0 jour pour la plupart, et des moyennes réduites, inférieures à 1 jour, signe que ces incidents sont souvent visibles immédiatement (suppression de données, contenus publics, anomalies flagrantes).

Détournement de ligne téléphonique

Médiane de 5 jours, ce qui traduit le temps nécessaire pour identifier une facturation anormale ou un usage inhabituel.

Par taille d'entreprise et type d'attaque, les mêmes tendances se retrouvent :

CA < 10 M€

Détection rapide des fraudes et connexions frauduleuses (médiane = 1 jour), plus lente pour les rançongiciels (médiane = 2 jours, moyenne = 8 jours).

CA 10-50 M€

Délais variables et parfois très longs pour les rançongiciels (médiane = 5 jours, moyenne ≈ 20 jours), reflet d'attaques plus sophistiquées où l'intrusion initiale reste longtemps silencieuse.

CA > 50 M€

Détection rapide pour les connexions frauduleuses (médiane = 2 jours), mais certains sinistres « atypiques » présentent des délais extrêmes, preuve que même les organisations très outillées ne sont pas à l'abri d'angles morts. C'est en particulier le cas cette année sur des fraudes inusuelles de détournement de lignes téléphoniques de l'entreprise, une tendance atypique à suivre.

(5) E-réputation : Diffamation, faux avis, menaces en ligne.



Ce que cela implique pour les entreprises

De ces données, deux messages opérationnels se dégagent :

- **Une détection rapide permet de limiter les impacts d’une cyberattaque** : investir dans la supervision, les alertes, les procédures d’astreinte et la capacité à réagir vite permet de transformer une intrusion en incident maîtrisé, plutôt qu’en crise prolongée.
- **Les outils ne suffisent pas sans l’humain** : si plus de la moitié des attaques surviennent quand les collaborateurs sont connectés, c’est bien que la première ligne de défense reste le réflexe de l’utilisateur — celui qui hésite, qui signale, qui alerte.

Dans un contexte où l’IA accélère et automatise les attaques, la capacité à voir tôt, comprendre vite et agir immédiatement devient un enjeu aussi stratégique que la mise en place des barrières de prévention elles-mêmes.

Analyse des tendances

CA < 10 M€

Détection rapide

pour les **fraudes** (médiane = 1 jour) et **connexions frauduleuses** (médiane = 1 jour).

Délais plus longs

pour les **rançongiciels** (médiane = 2 jours, moyenne = 8 jours).

CA 10-50 M€

Délais variables

pour les rançongiciels (médiane = 5 jours, moyenne = 20 jours), reflétant des attaques plus sophistiquées.

CA > 50 M€

Détection rapide

pour les **connexions frauduleuses** (médiane = 2 jours), mais **délais extrêmes** pour certains sinistres.

Les failles exploitées chez les entreprises visées

L'analyse des sinistres clos en 2025 met en lumière un constat simple et dérangeant à la fois : une poignée de failles récurrentes expliquent l'essentiel des attaques, toutes tailles d'entreprises confondues. La défaillance humaine, les vulnérabilités de VPN et l'identification sans multiples facteurs expliquent la majorité des sinistres, ce qui signifie qu'un socle de mesures restreint mais bien ciblé peut réduire fortement l'exposition, quelle que soit la taille de l'entreprise.

Rançongiciels : la faille VPN comme voie royale

Pour les entreprises de moins de 10 M€ de chiffre d'affaires, le facteur humain (défaillance humaine) est très présent, mais la compromission d'accès VPN vient immédiatement derrière, souvent via des identifiants volés ou des vulnérabilités non corrigées.

Entre 10 et 50 M€ de chiffre d'affaires, le trio de tête se renverse au profit des failles techniques. La surface d'attaque s'élargit : plus de services exposés, plus de correctifs à appliquer, plus de comptes à gérer. Les attaquants en profitent pour s'installer discrètement au cœur du système d'information.

Au-delà de 50 M€, les failles deviennent franchement infrastructurelles. Plus l'entreprise grandit, plus l'enjeu se déplace vers la maîtrise de l'infrastructure : hyperviseurs, VPN, firewalls, prestataires techniques.

Connexions frauduleuses : le facteur humain prépondérant

Les « connexions frauduleuses » regroupent la compromission de comptes (messagerie, VPN, portails), les campagnes de phishing réussies et les intrusions par identifiants volés. Lorsqu'on regarde les failles exploitées, un schéma très homogène apparaît.

Pour les entreprises jusqu'à 100 M€ de chiffre d'affaires, la défaillance humaine, suivie par les défauts de robustesse des mots de passe, est la première porte d'entrée.

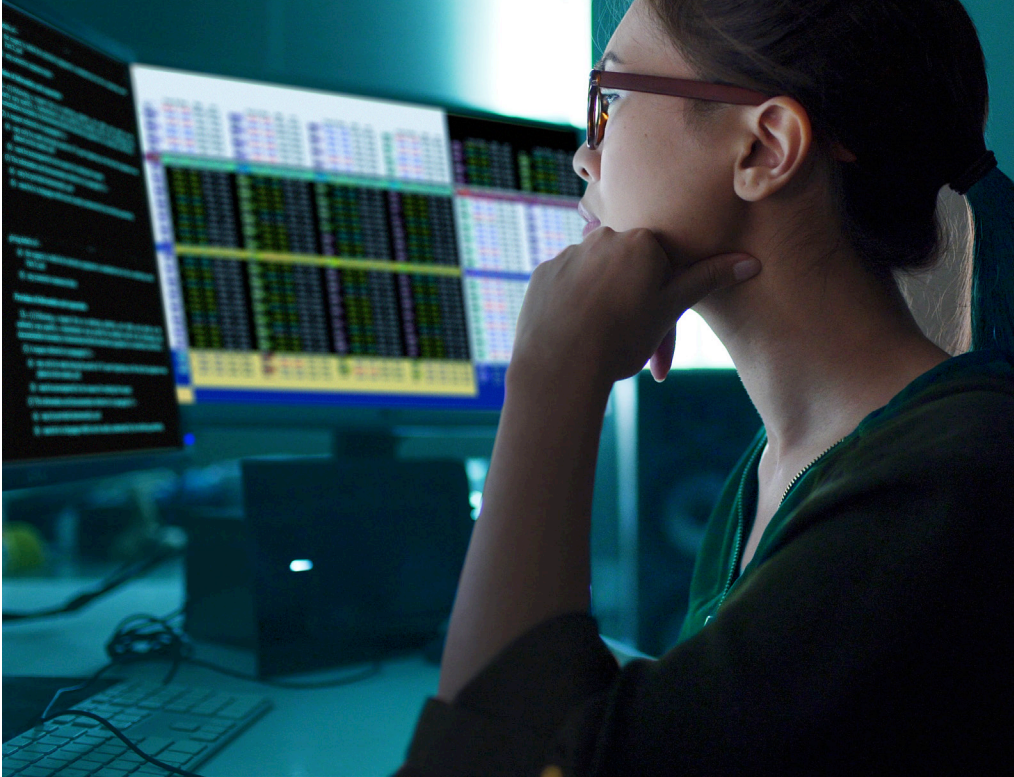
Ce n'est qu'au-delà de 100 M€, pour les plus grosses structures, que les défauts d'infrastructure techniques prennent le pas sur le facteur humain et les défauts basiques des processus d'identification.

Fraudes (FOVI) : l'usurpation d'identité comme arme principale pour les plus gros acteurs

Dans les entreprises de moins de 50 M€, les vulnérabilités humaines ou les défauts d'insuffisance des mots de passe sont la principale faiblesse exploitée par les attaquants.

Pour les plus grosses structures, c'est l'usurpation d'identité qui s'impose logiquement, ce qui fait écho aux nombreux cas de fraude aux dirigeants recensés ces derniers temps, alors que leur système d'identification et de mots de passe est souvent plus structuré et complexe.

La cybersécurité ne se joue pas uniquement sur les outils, mais aussi sur les procédures internes : double validation, rappel par un canal indépendant, segmentation des pouvoirs de signature, culture du doute face aux demandes urgentes.



Vol de données : les effets cumulatifs redoutables des attaques

Les sinistres de vol ou fuite de données confirment le même schéma selon la taille de l'entreprise. On note la prépondérance des vulnérabilités humaines pour les structures jusqu'à 100 M€ de chiffre d'affaires, tandis qu'au-delà, la dépendance aux prestataires devient centrale, avec les attaques via ESN et hébergeur.

Un fait mérite notre attention pour les entreprises jusqu'à 100 M€ de chiffre d'affaires : la réutilisation de failles déjà connues ou d'incidents antérieurs.

Des données déjà exposées, une faille non corrigée, peuvent être réutilisées dans le temps, parfois longtemps après l'incident initial. Le risque n'est donc pas seulement ponctuel, il est cumulatif : ce qui n'est pas corrigé ou renforcé lors d'un premier incident augmente la probabilité et la gravité des suivants.

Trois failles simples (défaillance humaine, VPN, MFA) expliquent la majorité des sinistres, ce qui signifie qu'un socle de mesures restreint mais bien ciblé peut réduire fortement l'exposition, quelle que soit la taille de l'entreprise.
Les failles de sécurité VPN regroupent principalement le vol de comptes VPN et l'exploitation de vulnérabilités référencées (de type CVE).

Ce qu'il faut retenir

Synthèse des tendances

CA < 10 M€

Ransomware :

Faillle humaine et failles VPN dominant.

Connexions frauduleuses :

Faillle humaine et mots de passe faibles sont les vecteurs principaux.

Fraudes :

Faillle humaine, usurpation d'identité et fuites de données sont les failles les plus exploitées.

Vol de données :

Faillle humaine et fuites de données antérieures sont les risques majeurs.

CA 10-50 M€

Ransomware :

Faillles VPN et défauts de patch management sont critiques.

Connexions frauduleuses :

Faillle humaine et défauts de robustesse des mots de passe restent dominants.

Fraudes :

Faillle humaine et usurpation d'identité sont les failles les plus fréquentes.

Vol de données :

Faillle humaine et attaques via hébergeurs/ESN sont les principaux vecteurs.

CA > 50 M€

Ransomware :

Faillles infrastructurelles (machines virtuelles, faille VPN, pare-feu) et défauts de patch management.

Connexions frauduleuses/

Fraudes :

Faillle humaine et usurpation d'identité ciblent les processus métiers (virements, RIB).

Vol de données :

Attaques via hébergeurs/ESN et failles applicatives sont les risques majeurs.

En synthèse, pour les très petites entreprises, la priorité est claire : renforcer la première ligne humaine (sensibilisation, formation aux failles humaines), sécuriser les mots de passe et activer systématiquement le MFA dès que cela est possible, même sur des environnements modestes.

Pour les PME, il ne suffit plus seulement de sensibiliser même si cela reste déterminant : il faut automatiser la gestion des correctifs (patch management), corriger les failles VPN, encadrer les accès des prestataires et mettre en place des processus de contrôle robustes autour des virements.

Pour les ETI, la cybersécurité devient un enjeu d'architecture et de gouvernance : gestion fine des privilèges, durcissement des environnements critiques, contractualisation et audit des prestataires, supervision pilotée (EDR, SOC), intégration de la sécurité dans les projets applicatifs.

Face à une menace qui s'automatise et se professionnalise, la réponse la plus efficace reste souvent la plus simple : fermer les portes que l'on sait les plus vulnérables. Faillle humaine, faille VPN, absence de MFA : c'est là que se joue, très concrètement, la différence entre une attaque évitée, un incident maîtrisé... ou un sinistre majeur.

La capacité de détection et de réponse rapide à l'incident est cruciale.

L'impact des attaques cyber : le cas des rançongiciels

Durée d'arrêt, mode dégradé : des réalités très variables

Quantifier précisément l'impact d'une cyberattaque reste un exercice difficile. Les coûts directs, perte d'exploitation, récupération des données, remise en état du système d'information, frais de gestion de crise, notifications CNIL, éventuelles sanctions réglementaires, sont déjà complexes à cerner. Les coûts indirects, atteinte à la réputation, perte de confiance des partenaires et clients, impact psychologique sur les équipes, le sont encore davantage.

Pour cette édition, nous avons concentré notre analyse sur les attaques par rançongiciel, qui offrent la base d'étude la plus significative, en nous attachant particulièrement à la durée d'interruption d'activité, un indicateur concret de l'ampleur des dommages.

Pour les TPE (chiffre d'affaires < 10 M€) : Ce segment présente une particularité : une proportion significative de TPE parvient à limiter fortement l'arrêt d'activité. **50 % des sinistres ne provoquent aucun jour d'arrêt formel**, et **75 % restent à 5 jours ou moins**. Cela tient souvent à des organisations plus simples à remettre en route, mais aussi — lorsqu'elles sont préparées — à des sauvegardes basiques mais efficaces. À l'inverse, les TPE insuffisamment préparées restent les plus vulnérables au risque de non-reprise.

Pour les PME (10 à 50 M€ de CA) : ce sont celles pour lesquelles l'impact se révèle le plus « explosif » : les arrêts moyens y sont nettement plus longs, et l'écart-type très élevé montre que certains cas basculent dans plusieurs semaines de paralysie. On retrouve ici le « double paradoxe » déjà identifié l'an passé : ce sont les entreprises qui ont une activité suffisamment structurée pour être des cibles rentables, mais qui n'ont pas toujours les moyens (ni la culture) pour investir dans une cybersécurité à la hauteur de leur exposition.

Les ETI (au-delà d'environ 50 M€ de CA) : présentent un profil à deux visages :

- Certaines, bien équipées (sauvegardes robustes, plans de continuité, supervision), parviennent à contenir l'arrêt autour de quelques jours ;
- D'autres, lorsqu'elles sont touchées sur des systèmes centraux ou via des prestataires clés, peuvent subir des arrêts de plusieurs semaines, avec un écart-type supérieur à 40 jours.

Dans tous les cas, plus la taille augmente, plus chaque jour d'arrêt pèse lourd : sur la chaîne de production, sur la logistique, sur les engagements contractuels, sur l'image vis-à-vis des clients et partenaires.



CA < 10 M€

50 % sans arrêt d'activité

75 % ont un arrêt d'activité < 5 jours

CA compris entre 10 et 50 M€

80 % sans arrêt d'activité

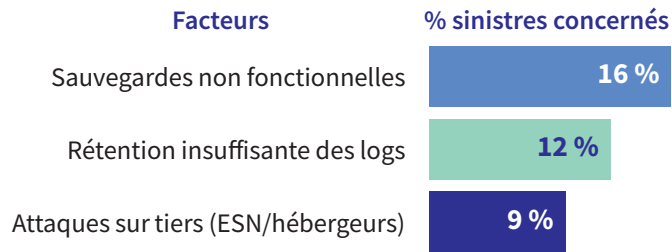
90 % ont un arrêt d'activité < 5 jours

La sauvegarde sécurisée :
la mesure qui change tout

En continuité avec les résultats observés l’an passé, dans 16 % des attaques recensées, quelle que soit la taille de l’entreprise, les sauvegardes étaient non fonctionnelles au moment de l’incident. Ce chiffre, en apparence modeste, entraîne des conséquences massives : l’absence de sauvegarde exploitable est l’un des principaux facteurs qui transforme un incident gérable en paralysie prolongée. La différence entre zéro jour d’arrêt et plusieurs semaines tient souvent à l’existence, ou non, d’une sauvegarde déconnectée, testée, et restaurable rapidement. C’est l’une des mesures au meilleur retour sur investissement de toute la chaîne de cybersécurité, le pendant aval de l’identification multifacteurs.

Parmi les autres facteurs aggravants identifiés : la rétention insuffisante des logs (12 % des sinistres), qui empêche une analyse post incident efficace, et les attaques transitant par des tiers, hébergeurs ou ESN, (9 %), qui soulignent l’importance de la sécurisation de toute la chaîne de valeur numérique.

Rançongiciel : Les facteurs d’aggravation de la durée d’arrêt total



Avis d’expert



Christine Sinibardy
Directrice Risques Techniques
et Cyber d’AXA France

“ Face à des menaces cyber toujours plus nombreuses, la prévention est devenue un levier essentiel de résilience. Grâce à des solutions comme KAMAE pour la sensibilisation des collaborateurs et Board Of Cyber pour l’identification proactive des vulnérabilités, nos clients réduisent significativement leur exposition au risque. Et lorsqu’un incident survient malgré tout, l’accompagnement dans la gestion de crise et l’indemnisation des pertes financières, leur permettent de reprendre leur activité dans les meilleures conditions.

Avec Global Cyber Secure, nous offrons ainsi une réponse globale face aux risques cyber. ”

Conclusion



Frédéric Coppin

Directeur Technique,
Performance Opérationnelle,
Marketing et Souscription Grands
Comptes

“

Cette deuxième Cyber Study confirme ce que nous observons au quotidien auprès de nos clients : la menace se déplace plus vite que les discours, mais elle exploite toujours les mêmes fragilités. Loin des scénarios spectaculaires, la plupart des sinistres naissent d’un trio très concret – phishing, VPN insuffisamment sécurisé, absence de MFA, et se transforment en crise à cause de sauvegardes défaillantes ou de plans de reprise insuffisamment testés.

Pour les entreprises, le véritable enjeu n’est plus de savoir « quand » elles seront ciblées, mais comment elles absorberont l’attaque le jour où elle surviendra. Cela suppose de sortir des approches génériques pour tenir compte de la réalité de chaque organisation : TPE, PME ou ETI n’ont ni les mêmes expositions, ni les mêmes marges de manœuvre, et les profils de risque diffèrent fortement d’un secteur à l’autre.

À la lumière des enseignements de cette édition, notre message est clair : concentrez vos efforts là où ils produisent le plus d’effet – sécurisation des accès, sauvegardes, détection rapide, procédures de décision pour la fraude – et faites-en un sujet de gouvernance, pas seulement d’outillage. De notre côté, nous continuerons à enrichir cette connaissance, à la partager et à la traduire en solutions concrètes de prévention et de protection, pour que chaque entreprise puisse passer d’une posture de vulnérabilité subie à une véritable culture de résilience cyber.

”

Remerciements

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

- Johann Andriandafimanana
- Corinne Calendini
- Alban Claude
- Frédéric Coppin
- Myriam Desgroux
- Jean-Pierre Marbaix
- Benoît Mauvais
- Thierry Piton
- Charlotte Prieur
- Christine Sinibardy
- Aude de Vorges

Scannez pour découvrir
notre Livre Blanc
sur la cybersécurité



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



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



AXA France IARD - S.A. au capital de 214 799 030 € - RCS Nanterre 722 057 460 • **AXA Assurances IARD Mutuelle** - Société d'Assurance Mutuelle à cotisations fixes contre l'incendie, les accidents et risques divers - Siren 775 699 309. Sièges sociaux : 313 Terrasses de l'Arche - 92727 Nanterre Cedex • **Juridica** - S.A. d'assurances de protection juridique au capital de 14 627 854 € - RCS Versailles 572 079 150 - Siège social : 1 place de Victorien Sardou - 78166 Marly le Roi Cedex • **AXA Assistance France Assurances** - S.A au capital de 24 099 560,20 € - 451 392 724 RCS Nanterre. Siège social : 6 rue André Gide - 92320 Châtillon • **Entreprises régies par le Code des assurances.**

Le contenu de ce document est fourni à titre informatif et n'a pas de valeur contractuelle.



Réf. 2008063-0826 - CAR/JOCA - Crédit photo : Getty Images, Adobe Stock, Shutterstock