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

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

+30 % C'est l'augmentation des attaques cyber dans le monde entre 2023 et 2024(1).

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

34 % L'Asie Pacifique est la première zone touchée par les cyberattaques en 2024(2),

24 % suivie par l'Amérique du Nord,

24 % et l'Europe

10 % puis le Moyen-Orient,

8 % et enfin l'Amérique Latine.

(1) Check Point Software Technologies. (2) IBM, X-Force 2025 Threat Intelligence Index.

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.

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 sont de plus en plus visées, avec une hausse des attaques de

+53 % en 2024(4).

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

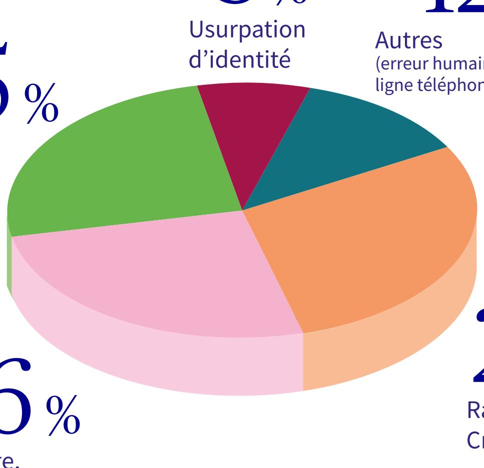
78 % des entreprises se disent insuffisamment préparées ou l'ignorent(3).

(3) Cybermalveillance.gouv.fr, Etude de notoriété auprès de TPE et PME, Opinionway, 2024 Baromètre de la cybersécurité des entreprises, 2025.(4) Orange Cyberdefense, security Navigator 2025.

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.



Typologie de sinistres (%)(5)

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

7 grandes familles **de menaces cyber**

1 Hameçonnage *(phishing)*

Fréquence : **Très élevée**

3.4 Mds d'e-mails de phishing sont envoyés chaque jour dans le monde en 2025(6).

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.

2 Rançongiciels *(ransomware)*

Fréquence : **élevée**

59 % des entreprises dans le monde ont subi une attaque par ransomware(7) 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.

3 Ingénierie sociale *(social engineering)*

Fréquence : **élevée**

98 % des cyberattaques utilisent des techniques d'ingénierie sociale en 2023(8).

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.

4 Attaques par rebond

Fréquence : **élevée**

30 % des compromissions impliquent un tiers en 2024, deux fois plus qu'en 2023(9).

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.

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(10).

MODE OPÉRATOIRE

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

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.

7 Attaques ciblées

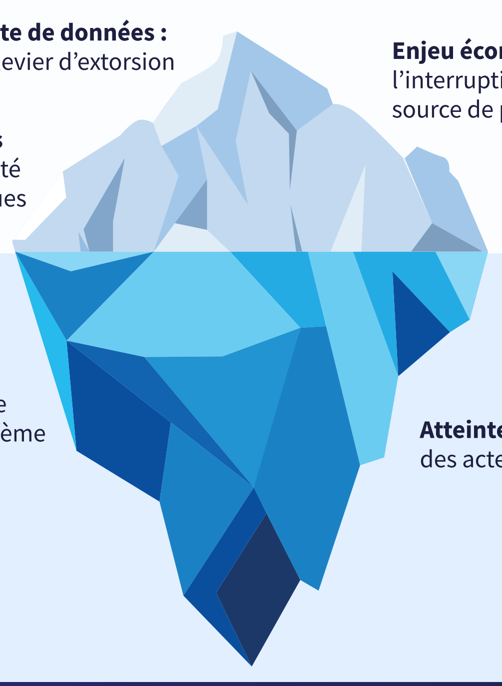
Fréquence : **faible**

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.

(6) DeepStrike, Phishing statistics 2025.
(7) Sophos, The State of Ransomware 2025 (entreprises comptant 100 à 5000 employés).
(8) Firewall Times, 2023.
(9) Verizon, Data Breach Investigations Report, 2025.
(10) Cloudflare, Rapport sur les DDoS, 2024.

Impacts des attaques cyber **sur les entreprises**



Perte de données : un levier d'extorsion

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

Risques juridiques et de non-conformité associés aux attaques

Atteinte à l'image de l'entreprise : Perte de confiance de l'écosystème de l'entreprise

Atteinte psychologique des acteurs impliqués

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.

Réf : 2008520 01 2026