



Communiqué de Presse

Les cyberattaques coûtent de plus en plus cher aux PME et ETI européennes et anglaises, malgré un recul du nombre de sinistres.

Paris, 20 août 2026 - L'analyse récente de la sinistralité observée chez Chubb révèle que, si la fréquence des incidents cyber se stabilise en Europe et au Royaume-Uni, le coût financier des attaques subies par les PME et ETI continue d'augmenter fortement.

Les données issues du [Rapport Chubb sur les sinistres cyber 2026](#) montrent qu'en 2025, la fréquence des déclarations de sinistres cyber des PME et ETI a atteint son niveau le plus bas depuis cinq ans. Dans le même temps, la valeur moyenne des sinistres a été multipliée par trois entre 2020 et 2025.

Si l'intelligence artificielle aide les entreprises à mieux identifier et détecter leurs vulnérabilités cyber, elle alimente également des usages malveillants de plus en plus sophistiqués, susceptibles d'accélérer et d'amplifier l'exposition au risque.

Jimaan Sané, Directeur du Développement Cyber chez Chubb, souligne que pour les PME et les ETI, la chaîne d'approvisionnement constitue l'un des principaux points de vulnérabilité, compte tenu de leur forte dépendance vis-à-vis de fournisseurs tiers.

« Les PME et ETI s'exposent aujourd'hui aux mêmes risques cyber que les grands groupes, mais sans bénéficier de la même résilience opérationnelle », déclare Jimaan Sané. « Au-delà de l'identification et de la prévention de leurs propres défaillances, elles doivent faire face aux répercussions financières et opérationnelles lorsque des systèmes, fournisseurs et partenaires interconnectés sont compromis. »

« Quand un prestataire technologique est victime d'une attaque par ransomware, les répercussions restent rarement limitées à son activité. Les commerces, fabricants ou industriels, et prestataires de services qui dépendent de ses systèmes en subissent immédiatement les effets : ventes interrompues, stocks inaccessibles, opérations suspendues. L'attaque est externe, mais la perte d'exploitation, elle, est bien réelle et pèse directement sur leur compte de résultat. Cette exposition grandissante rappelle combien la couverture en perte d'exploitation indirecte est indispensable dans toute stratégie cyber globale », ajoute Jimaan Sané.

Outre des menaces pilotées par l'IA de plus en plus sophistiquées et une dépendance accrue aux chaînes d'approvisionnement, les fraudes par ingénierie sociale, les incidents liés à la vie privée et les attaques par ransomware continuent de présenter des risques majeurs, selon Chris Collier, Vice-Président Indemnisation Cyber chez Chubb.

« Ces types d'incidents peuvent être dévastateurs, en particulier pour les PME et ETI qui ne disposent pas d'une couverture cyber adaptée et n'ont aucun moyen de se remettre de pertes irrécouvrables ou d'en assumer le coût », précise Chris Collier.

Selon le [Department for Science, Innovation and Technology](#), seules 24 % des entreprises de taille moyenne du Royaume-Uni sont couvertes par une police cyber spécifique.

Le ransomware, en particulier, reste une menace redoutable pour les PME et ETI. Même lorsqu'une attaque est partiellement bloquée, l'exfiltration de données sensibles suffit à déclencher une cascade d'obligations réglementaires et d'opérations de remédiation particulièrement lourdes à gérer.

« Chubb dispose d'une expertise reconnue dans le traitement des sinistres ransomware. Nous mobilisons pour nos clients des équipes spécialisées, juristes, experts en forensique informatique, communicants, pour les aider à gérer la crise efficacement, limiter les interruptions d'activité et reprendre le cours normal de leurs opérations », affirme Chris Collier.

Sur le plan défensif, les entreprises et les organisations peuvent déployer des outils de gestion des risques axés sur l'IA pour faire face à ces menaces et en réduire l'impact, tout en renforçant la sensibilisation, en faisant du cyber une priorité du comité de direction, et non plus un simple projet informatique.

Des outils en ligne tels que le [Chubb Cyber Index](#) offrent un accès en temps réel à des informations et ressources permettant d'évaluer et de gérer les risques cyber auxquels votre entreprise peut être exposée. Chubb propose également à ses assurés un large éventail d'outils et de solutions, couvrant tous les domaines, notamment la protection cyber des petites entreprises, la réponse à incidents, la gestion des vulnérabilités, de la sécurité, des outils de détection et de réponses, la gestion des risques liés à la vie privée, ainsi que la sensibilisation et la sécurisation des utilisateurs. En savoir plus [ici](#).

Le Rapport Chubb sur les sinistres cyber 2026 est disponible [ici](#).

À propos de l'expertise Cyber de Chubb

Leader en assurance cyber, Chubb conjugue une expertise de pointe en souscription à des services spécialisés de prévention et de gestion de crise. Nos solutions sur mesure s'adaptent aux enjeux spécifiques de chaque client pour lui garantir les outils et l'accompagnement indispensables en cas de cyberattaque.

A propos de Chubb

Chubb est un leader mondial de l'assurance. Présent dans 54 pays et territoires, Chubb propose des assurances de dommages et de responsabilité, des assurances santé et prévoyance, de la réassurance et des assurances vie à une clientèle diversifiée. L'entreprise se distingue par l'étendue de son offre de produits et de ses prestations de services, l'ampleur de son réseau de distribution, son exceptionnelle solidité financière et ses opérations locales à l'échelle mondiale. La société mère, Chubb Limited, est cotée à la Bourse de New York (NYSE : CB) et fait partie de l'indice S&P 500. Chubb emploie environ 45 000 personnes dans le monde. Pour plus d'informations, visitez : www.chubb.com.

Contact presse

Kathryn Coventry, Head of Communications EMEA, Chubb
kathryn.coventry@chubb.com