

Bessé et Stellant dévoilent les principales conclusions de leur étude sur la sinistralité cyber des entreprises

13 octobre 2022 – **Bessé, courtier et conseils en assurances, publie, en partenariat avec le Groupe Stellant, une analyse approfondie des impacts d’une attaque cyber et de la capacité de gestion et de résilience des organisations françaises.**

A l’instar de sa participation au groupe de travail de la DG du Trésor qui vient de publier son rapport sur le développement de l’assurance du risque cyber, cette étude s’inscrit dans une démarche de réflexion et de sensibilisation que mène activement Bessé depuis 2016 pour contribuer à améliorer la posture des entreprises face au risque cyber. Alors que le taux de couverture des entreprises, tous segments confondus, reste faible et très contrasté, l’étude réalisée, examine un échantillon de 59 sinistres (entre 2019 et 2021) de sociétés ayant souscrit une police d’assurance cyber et dont les impacts financiers excèdent 100K€ pour les grands Groupes et 50K€ pour les petites et moyennes entreprises. L’étude confirme en premier lieu la **part majoritaire des attaques sur les PME à 44%**, particulièrement exposées avec les TPE, en raison d’un niveau de protection très faible.

Retour sur l’état de la menace cyber en quelques chiffres clés :

- **+ de 1000 affaires suivies** par l’ANSSI en 2021 vs 750 en 2020
- **36 % de taux de perte** totale de données suite à une attaque
- **79% des entreprises** avec des données sur le cloud ont subi au moins 1 violation depuis 2020
- La France est **le 3ème pays le plus attaqué par ransomware** après les USA et le Royaume-Uni

Autres conclusions significatives de l’étude :

> Nature, source et profondeur des attaques cyber :

- **Les attaques par ransomware constituent près de 90 %** de la sinistralité enregistrée. Le montant des rançons reste faible en comparaison du préjudice total subi et le nombre de dossiers concernés par un paiement de rançon est très limité.
- **Les campagnes de Phishing** (e-mail ou SMS incitant le destinataire à utiliser un lien corrompu) sont la **première source des attaques** du système d’information d’une entreprise pour **30% des dossiers**. L’attaquant pourra alors récupérer des mots de passe et des noms d’utilisateurs ou introduire un code malveillant utilisé par la suite.
- Les cyberattaques conduisent l’entreprise à devoir reconstruire totalement ou partiellement son système d’information dans **94 % des cas**.

> Impacts organisationnels :

- Toute attaque cyber entraine **des perturbations** plus ou moins fortes de l’activité **pendant plusieurs semaines voire plusieurs mois** : perte de la messagerie et de la téléphonie, indisponibilités des applicatifs dédiés aux fonctions supports, forte pression sur les équipes IT, ...
- Beaucoup d’entreprises sous estiment ou n’ont pas conscience des arrêts ou retards de fonctionnement qui peuvent être générés. En revanche, elles surestiment leur capacité à retrouver rapidement un niveau normal d’activités. **Ce retour à la normale** représente en moyenne **89 jours** pour **les Grandes Entreprises**, **20** pour **les ETI**, **29** pour **les PME** et **26 jours** pour **les TPE**.

> Impacts financiers :

- Les **pertes d'exploitation peuvent représenter plus de 80 % des coûts d'un sinistre majeur** touchant une ETI ou un grand Groupe. Suivent les frais de reconstitution des systèmes d'exploitation et les frais de gestion de crise.
- **174 M€ de pertes** ont été déclarées **au titre des sinistres** de l'échantillon analysé → **129 M€ ont été pris en charge à la date de notre étude** au titre des montants et natures de garanties prévus aux contrats d'assurance souscrits.

Quelques enseignements majeurs de l'étude :

- > Le volet assistance est un des points forts des polices Cyber car il apporte un véritable soutien aux entreprises victimes de cyberattaques. L'expérience acquise par les assureurs apporte aussi de la valeur.
- > La qualité de l'instruction du sinistre est clé : le calcul de l'indemnisation de l'ensemble des pertes d'exploitation subies par l'entreprise peut s'avérer très complexe.
- > La cyber résilience dépend tout autant de l'évaluation technique des risques que de l'interprétation des paramètres opérationnels et financiers régissant le fonctionnement de l'entreprise.
- > La valorisation financière des risques favorise le développement d'une compréhension commune des menaces cyber au sein de l'organisation.

La dernière partie de l'étude sinistralité Cyber est dédiée aux regards de

- > **Guy Philippe GOLDSTEIN**, enseignant à l'École de Guerre Économique, sur l'impact économique d'une attaque cyber
- > **Laurent PORTA**, associé chez Vae Solis Communications, sur la cyber-résilience
- > **Fabienne LOPEZ**, colonel de gendarmerie et cheffe du Centre de lutte contre les criminalités numériques (C3N), sur son observation au quotidien des affaires qui lui sont rapportées.

« Avec cette étude, nous avons choisi de nous placer au centre de la crise cyber en observant la gestion du sinistre. Notre objectif est d'apporter aux dirigeants et à leurs équipes un éclairage favorisant leur compréhension des frais et pertes auxquels sont exposés les entreprises et quelle pourrait être leur prise en charge au titre des contrats d'assurance cyber qu'ils peuvent décider de souscrire. » **Pierre BESSÉ, Président-directeur général de Bessé**

« Il nous a paru important de faire progresser la nécessaire sensibilisation des différents acteurs au risque cyber car nous constatons encore trop souvent que ce risque n'est pas intégré à son juste niveau de survenance par les différents acteurs économiques. » **Christophe ARREBOLLE, Président du Groupe Stellant.**

- **Accéder à l'intégralité de l'étude :** [ici](#)

Précédentes études cyber réalisées par Bessé :

[Le secteur maritime et portuaire face au risque cyber](#) (2022)
Baromètre DATA BREACH : [3ème Édition](#) (2022), [2ème Édition](#) (2021), [1ère Édition](#) (2020)
[Crise cyber : Quel impact sur la valorisation des entreprises non cotées ?](#) (2020)
[Les dirigeants d'ETI face à la menace cyber - Point de situation](#) (2019)
[Les dirigeants d'ETI face à la menace cyber](#) (2018)

A propos de Bessé

Les hommes et les femmes de Bessé sont des experts du conseil et du courtage en assurance pour les grandes entreprises et les ETI. Au quotidien, ce sont 470 collaborateurs qui s'appuient sur leur expertise et leur capacité d'innovation pour accompagner les clients du Groupe en France et dans le monde dans la protection de leurs activités et de leurs salariés. En 60 ans, avec les mêmes valeurs et la même indépendance, Bessé a développé sa stratégie d'hyperspécialisation pour s'imposer au fil du temps comme un acteur global et l'un des leaders français sur son marché. Régulièrement distinguées pour la qualité de leurs services et de leur présence sur le terrain, les équipes de Bessé construisent une relation de confiance durable avec leurs clients. L'entreprise, qui fait partie des « *500 champions des territoires* », a été primée, pour la deuxième édition consécutive, Courtier #1 du Baromètre de satisfaction 2020 des Risk Managers (Golden & Partners et OMC Luxembourg). Bessé a réalisé en 2021 un chiffre d'affaires de 124 M€.

[Site Internet](#) - [Linkedin](#) - [Media Center](#) - [TV Bessé](#)

A propos de Stelliant

Leader en France des services à l'assurance, le groupe Stelliant accompagne, depuis plus de 30 ans, la gestion des risques et des sinistres que rencontrent les particuliers, les professionnels et les entreprises. Nous intervenons sur l'ensemble de la chaîne de valeur assurantielle : Conseil et Prévention (gestion des risques, prévention, aide à la souscription), Expertise, Délégation (expérience client, vente, gestion déléguée), Solutions Après Sinistre (mesures conservatoires, investigations, réparation et gestion de crise). Nos 3000 collaborateurs œuvrent au quotidien pour trouver ensemble les solutions adaptées qui répondent à chaque besoin, à chaque spécificité. Nous sommes présents en France, au travers de 140 implantations et à l'international avec notre partenaire Crawford.

Depuis 2017, Inquest, cabinet de conseil en gestion des risques, et filiale du Groupe, intervient sur l'ensemble de la chaîne du risque, au service d'entreprises de toutes tailles, et dans tous les domaines d'activité

Pour en savoir plus : www.stelliant.com – www.inquest-risk.com

Contacts Presse :

CICOMMUNICATION

Béatrice SAVOURET I Catherine ISNARD

Tél : +33 1 47 23 90 48

besse@cicommunication.com