ÉTUDE SINISTRALITÉ CYBER

OCTOBRE 2022

RISQUES CYBER ANALYSE DE LA SINISTRALITÉ : QUELS ENSEIGNEMENTS ?

BESSÉ

CONSEIL EN ASSURANCES

stelliant

sommaire

préface

de Pierre Bessé

Pierre Bessé
Président Directeur Général de BESSÉ

Je suis très heureux de cette nouvelle étude sur un sujet qui me tient à cœur : le risque cyber auquel tous les dirigeants sont désormais confrontés, quelles que soient la taille et l'activité de leurs entreprises.

Dès 2016, BESSÉ a adopté une posture de « lanceur d'alerte » pour contribuer, avec toutes les parties prenantes du Public et du Privé, à sensibiliser, mobiliser et organiser la lutte contre la menace que constitue ce risque émergent à caractère systémique.

À l'époque, il était difficile de faire prendre conscience au plus grand nombre qu'il s'agissait d'un phénomène qui allait devenir l'une des préoccupations majeures des chefs d'entreprises et de leurs Directions Générales, et, pour toutes leurs équipes, l'un des grands défis du management des risques.

Fort heureusement, cette phase de sensibilisation est désormais derrière nous ; les différentes crises que nous avons connues et continuons de connaître ont permis d'accélérer la prise de conscience et le développement des actions de gouvernance du risque.

En tant qu'acteur contribuant à la chaine de valeur de la cybersécurité, nos équipes ont ensuite poursuivi nos travaux en analysant l'impact d'une crise cyber sur la valorisation et la réputation de l'entreprise : c'était le fruit de notre étude de 2020 menée en collaboration avec Guy-Philippe Goldstein qui actualise ces recherches dans ce document.

Avec cette nouvelle étude menée en partenariat avec Christophe Arrebolle et ses équipes du Groupe STELLIANT, 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 exposées les entreprises et de leur éventuelle prise en charge au titre des contrats d'assurance cyber qu'ils peuvent décider de souscrire.

Cette analyse très opérationnelle est complétée d'un focus sur la valorisation du risque par Cédric Lenoire, expert BESSÉ, ainsi que des regards de Laurent Porta, spécialiste de la communication de crise pour Vae Solis et de Fabienne Lopez, Colonelle de Gendarmerie et cheffe du Centre de lutte contre les criminalités numériques (C3N).

Je vous en souhaite bonne lecture.

L'ÉTAT DE LA MENACE EN QUELQUES CHIFFRES CLÉS

4e

La France, en 4e place des pays à l'origine* de la menace informatique

** celle des serveurs à partir desquels sont lancées les attaques*

Source Etude Kaspersky – 07/2022

+ de 1 000

Le nombre d'affaires suivies par l'ANSSI est passé de 750 en 2020 à plus de 1000 en 2021

36 %

Pour chaque attaque, les entreprises n'ont pas pu récupérer 36 % de leurs données perdues

#chiffres clés

18 376 → 90 %

18 376 vulnérabilités *(CVE, Common Vulnerabilities and Exposures)* émis en 2021

90 % de tous les CVE découverts en 2021 étaient exploitables par des attaquants ayant des compétences techniques minimales

79 %

Des attaques dans le CLOUD en hausse. Depuis 2020, 79 % des entreprises ayant des données sur le cloud ont subi au moins une violation du cloud

55 %

55 % des CVE de 2021 ne nécessitent aucun privilège pour être exploités

89 %

89 % des entreprises ne parviennent pas à protéger leurs données

(Étude Veeam Data Protection Trends Report 2022)

3e

La France est à la 3e place des pays ayant le plus concentré d'attaques *ransomware,* derrière les États-Unis et le Royaume-Uni, mais devant le Canada et l'Allemagne

EN SYNTHÈSE, CE QU'IL FAUT RETENIR **ANALYSE DE LA SINISTRALITÉ**

#1	#2	#3	#4	#5
Les attaques par Ransomware constituent près de 90 % de la sinistralité enregistrée. Le montant des rançons est très faible en comparaison du préjudice total subi. Le nombre de dossiers concernés par un paiement de rançon est très limité.	Toute attaque cyber entraîne des perturbations plus ou moins fortes de l'activité pendant plusieurs semaines, voire plusieurs mois. Beaucoup d'entreprises sous-estiment ou n'ont pas conscience des arrêts ou retards de fonctionnement qui peuvent être générés. Elles surestiment souvent aussi leur capacité à retrouver rapidement un niveau normal d'activité.	• Une première phase de crise aiguë liée à l'arrêt total ou partiel des systèmes d'information. • Une phase de redémarrage progressif des applications essentielles et donc du niveau d'activité. • Une phase de retour à la normale des activités et l'achèvement complet de la reconstruction numérique.	La perturbation du niveau d'activité peut générer des pertes d'exploitation élevées qui représentent plus de 80 % des coûts d'un sinistre majeur/ touchant une ETI ou un grand groupe. Les frais de reconstitution des systèmes d'exploitation et les frais de gestion de crise constituent les deux autres postes majeurs des frais et pertes des dossiers étudiés.	Les polices d'assurances cyber répondent lorsque les risques et leurs impacts ont été correctement analysés et valorisés pour adapter les garanties en conséquence. La qualité de l'instruction du sinistre est clé, d'autant plus que le calcul de l'indemnisation de l'ensemble des pertes d'exploitation subies par l'entreprise peut s'avérer très complexe. Au niveau des coûts de reconstruction informatique, la prise en charge des frais engagés se heurte à la non prise en compte par l'assurance des améliorations qui seront apportées.

CHIFFRES À RETENIR

174 M€
de pertes déclarées

129 M€
pris en charge au titre des montants et des natures de garanties prévus aux contrats d'assurance souscrits.

Échantillon de 59 sinistres sur la période 2019-2021.

#points clés
sur le reste de l'étude

#6 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.

#7 La cyber résilience est l'affaire de tous. Elle doit être pilotée au plus haut niveau de l'entreprise qui saura allouer ressources et budgets adaptés.

Sur le plan de la communication, manifester une mobilisation en demi-teinte, déconnectée de l'ampleur de l'attaque, est improductive en termes d'image. Il faut savoir communiquer auprès de ses cibles de manière forte et assumée.

#8 Une analyse BESSÉ / G.P. Goldstein sur 48 incidents cyber sur des entreprises françaises non cotées entre 2017 et 2021 montre un résultat fort et fondamental : le risque de défaillance de l'entreprise augmente d'environ 50 % dans les 6 mois qui suivent l'annonce de l'incident.

Une analyse de corrélation avec les échos négatifs sur les réseaux sociaux semble indiquer que c'est bien la réputation de l'entreprise qui est en partie en jeu dans la dégradation économique significative suite à l'incident cyber.

#9 L'année 2021 a été marquée par une croissance continue des infractions numériques, avec près de 130 000 faits enregistrés contre 104 000 en 2020 pour la seule zone gendarmerie, soit une augmentation de 20 %. En quatre ans, la cybercriminalité a ainsi doublé. L'année 2022 s'inscrit dans la même continuité en termes de procédures judiciaires recensées. Il ne faut cependant pas oublier qu'un grand nombre d'infractions ne font pas l'objet d'un dépôt de plainte auprès des forces de l'ordre et que le nombre de faits commis est beaucoup plus important. Le nombre de plaintes est variable en fonction du type de contentieux. Si l'on prend l'exemple des attaques par rançongiciels, contentieux prioritaire pour le C3N en raison des préjudices subis et de la capacité de déstabilisation qu'il représente, il est courant que nous soyons informés de plusieurs attaques dans une même semaine. Les cybermenaces demeurent donc un risque majeur pour les années à venir. Les acteurs malveillants vont continuer à cibler des entreprises stratégiques, les administrations, mais également des entreprises de petites et moyennes tailles, ainsi que les particuliers.

Cf : #06 - Cédric Lenoire | #07 - Laurent Porta | #08 - Guy-Philippe Goldstein | #09 - Fabienne Lopez

PARTIE #01

Risques Cyber
Analyse de la sinistralité 2019 - 2021
Quels enseignements ?

#01

avant-propos

Comment se caractérise cette sinistralité ? Est-elle ou non globalement homogène ?

Comment se répartissent les différents postes de préjudices ?

Quels sont les délais de remédiations ?

Y a-t-il des facteurs qui influencent la gestion et le coût des sinistres cyber ?

Est-ce que les couvertures d'assurance cyber sont efficientes ?

Quels enseignements en tirer ?

Ces questions nous sont apparues rapidement essentielles pour les analyses de risques de chaque entreprise.

C'est dans ce contexte que BESSÉ et STELLIANT ont décidé de s'associer pour mener cette étude sur la sinistralité cyber. Son objectif n'est pas de présenter l'évolution de la sinistralité ni de rentrer en détail sur tel ou tel dossier, mais d'apprécier ce qui la caractérise en termes d'impacts. Le but est aussi de faire ressortir les facteurs qui en ont facilité ou complexifié la gestion.

Cette étude est donc une première. Elle combine l'expertise de BESSÉ sur le cyber et celle du Groupe STELLIANT et des analystes de sa filiale INQUEST appelés en réponse aux incidents.

contributeurs

Christophe Madec
Directeur de clientèle
BESSÉ

Alexis Nardone
Directeur Général
INQUEST - Groupe STELLIANT

Rajâa Aouina
Directrice des Spécialités
STELLIANT Expertise
Groupe STELLIANT

introduction

de Christophe Arrebolle

Christophe Arrebolle
Président du
Groupe STELLIANT

Les attaques cyber se sont très fortement amplifiées ces dernières années. Elles touchent l'ensemble des acteurs de notre vie quotidienne, quelle que soit leur taille ou leur secteur d'activité : administrations, services publics, entreprises petites ou très grosses, mais aussi des particuliers voire des états.

Elles sont très souvent associées à des démarches criminelles pour déstabiliser ou à des tentatives d'extorsion, dans un but purement lucratif.

Le développement des outils, mais aussi de la technicité, relativement facile d'accès au travers du darkweb, ont facilité le déploiement à grande échelle de groupes spécialisés et organisés.

En contrepartie, les entreprises ou organismes augmentent leur niveau de sécurité, déploient de nouvelles solutions techniques, améliorent la préparation des équipes permettant de réduire le risque, mais toutes ces actions nécessaires ne sont pas suffisantes pour garantir une absence d'attaque conduisant au blocage des activités.

C'est donc un risque majeur dont la multiplication des attaques constatées et les conséquences de ces dernières sont présentées dans cet ouvrage. Il nous paraît 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.

C'est dans ce contexte que le secteur de l'assurance a pleinement joué son rôle. Tout d'abord en privilégiant la prévention et en sensibilisant aux moyens à déployer pour garantir un niveau de sécurité conforme. Ensuite en apportant des garanties financières pour accompagner les entreprises concernées par ces attaques. La complexité technologique et les coûts associés, les impacts économiques d'arrêt d'activité qui peuvent être très conséquents, couplés à l'augmentation significative de la survenance, mettent en évidence toute la difficulté que représente la couverture de ce risque.

L'étude présentée dans cet ouvrage apporte un éclairage sur ces différents aspects du risque cyber et contribue à la sensibilisation sur ce risque structurel.

> Il nous paraît important de faire progresser la nécessaire sensibilisation des différents acteurs au risque cyber.

1.

Base de l'étude, présentation du périmètre de l'étude

Avant d'être étudiées et partagées par STELLIANT, les données propres à chaque dossier ont toutes été anonymisées.

Intervalle

2019 > 2021

Nombre de sinistres

59

dont 47 dossiers avec un état de pertes finalisé et

12

dossiers à un stade avancé d'instruction et de chiffrage

Seuil d'intervention

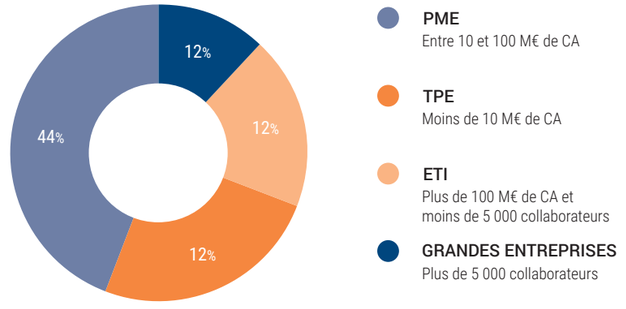
sinistres dont les impacts financiers excèdent 100 K€, à l'exception des petites et moyennes entreprises où le seuil retenu est de 50 K€

L'étude ne porte que sur des sociétés ayant souscrit une police d'assurance cyber.

Il est admis que le taux d'équipements des entreprises, tous segments confondus, reste globalement faible. Il est aussi très contrasté.

Les grandes entreprises (SBF 120), ont, a priori, toutes souscrit une couverture d'assurance cyber. Au niveau des ETI et selon l'étude LUCY publiée par l'AMRAE en 2021, seules 8 % d'entre elles auraient souscrit une assurance cyber. Ce pourcentage est sans aucun doute encore plus faible pour les PME / TPE.

Répartition par population des sinistres cyber étudiés



Sans grande surprise, la proportion des TPE / PME est la plus importante au regard du nombre de contrats en vigueur sur ce segment. Les entreprises de cette taille, bien que très peu assurées, sont particulièrement exposées, en raison d'un niveau de protection très faible.

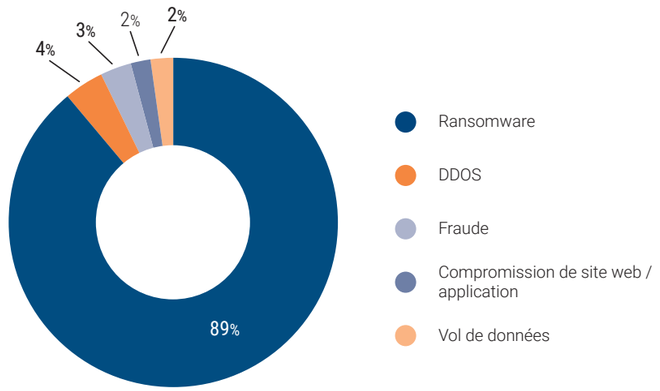
Le nombre de sinistres relevé sur le périmètre ETI / Grands comptes est de 18 dossiers, ce qui est plus que significatif sur la période étudiée (33 mois).

Ce graphique confirme surtout que toutes les entreprises, quelle que soit leur taille ou leur domaine d'activité, sont bien des cibles.

2.

Nature, source et profondeur des attaques cyber

2.1 Nature des attaques

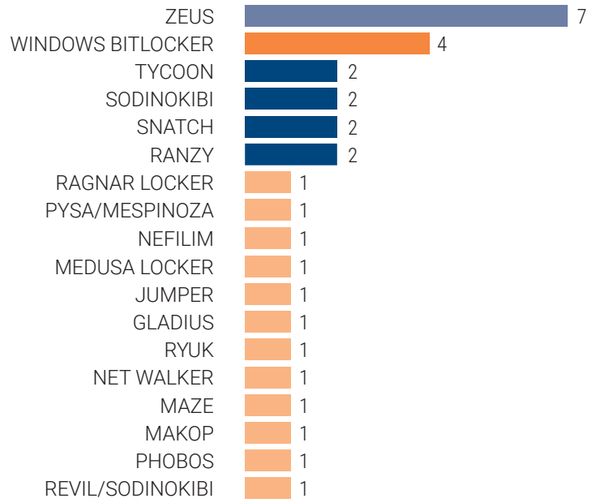


Sans surprise, les attaques par *ransomware* constituent 89 % des attaques sur l'échantillon étudié. Ces attaques par *ransomware* sont le plus souvent accompagnées de vol de données avec menace de divulgation pour contraindre l'entreprise à payer.

Le vol de données comme seule motivation se limite à un seul dossier, tout comme la compromission de site web.

TYPES DE *RANSOMWARES*

Répartition par type de *ransomwares*



Un total de vingt et un *malwares* est identifié sur 43 dossiers, dont 1 attribué à Revil / Sodinokibi et 1 à Phobos.

La famille des *ransomwares* ne cesse d'évoluer au fil des ans, ce qui souligne à quel point la menace est multiforme et évolutive.

Identifier la nature du *ransomware* s'avère utile car les attaquants ont des modes opératoires souvent spécifiques. Cette phase exploratoire va permettre de tracer la circulation des attaquants au sein du SI et de comprendre les mécanismes utilisés.

Ce travail est facilité par l'utilisation d'outils de recherche de compromission, appelés aussi ORC. Ces outils favorisent grandement l'analyse des investigations remontant toute trace explicite d'un indicateur de compromission (IOC - *indicator of compromise).*

Cet état des lieux s'avère essentiel pour délimiter le périmètre compromis et donc définir les mesures de remédiation à engager.

- **REVIL / SODINOKOBI**

Ce *ransomawre* est détecté pour la première fois en avril 2019. Le groupe à l'origine de son développement et de sa diffusion en mode Raas *(ransomware as a service)* a choisi de limiter fortement le nombre d'affiliés (groupe de cybercriminels) et de leur imposer un niveau d'activité élevé.

Selon l'ANSSI, la France est l'un des pays le plus touché par ce *ransomware,* derrière les USA et la Chine. GEFCO, PIERRE FABRE, OUEST FRANCE ou FAREVA en ont été les victimes. Le groupe a été démantelé en janvier 2022 après une opération menée en Russie.

- **RYUK**

Le ransomware Ryuk est apparu pour la première fois en 2018. Ryuk utilise le logiciel malveillant Trickbot pour s'installer, une fois l'accès aux serveurs d'un réseau obtenu. Il a la capacité de vaincre de nombreuses contre-mesures anti-*malware* qui peuvent être présentes et peut complètement désactiver un réseau informatique. Il peut même rechercher et désactiver les fichiers de sauvegarde, s'ils sont conservés sur des serveurs partagés. Une fois que Ryuk prend le contrôle d'un système, il crypte les données stockées, rendant impossible l'accès des utilisateurs, à moins qu'une rançon ne soit payée par la victime en bitcoins ce qui suppose aussi de pouvoir en disposer. Dans de nombreux cas, des jours ou des semaines peuvent s'écouler entre le moment où les pirates accèdent initialement à un système et celui où le cryptage massif se produit.

- **CONTI**

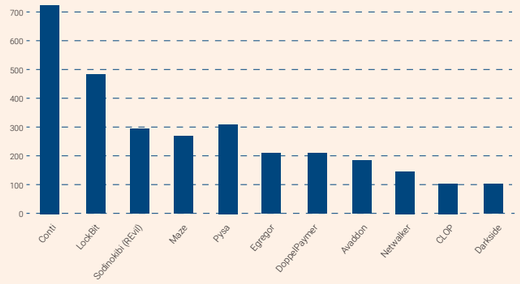
Conti est un *ransomware* observé depuis 2020. Toutes les versions de Microsoft Windows sont connues pour être affectées. Au-delà du très grand nombre d'attaques revendiquées par le groupe derrière ce *ransomware,* Conti présente un mode de rémunération original pour les affiliés. Celui-ci comprend le versement d'un salaire fixe assorti d'une partie variable sur les gains obtenus à la suite d'une attaque.

Pour ceux qui tiennent les rênes de la franchise, cette approche offre l'avantage d'attirer un nombre plus important d'affiliés et donc d'accroître le volume de gains.

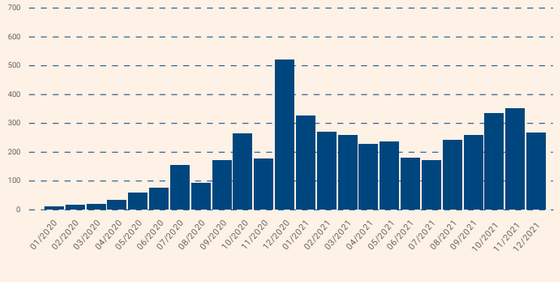
NATURE, SOURCE ET PROFONDEUR DES ATTAQUES CYBER

NOMBRE DE VICTIMES D'ATTAQUES *RANSOMWARE* IDENTIFIÉES DANS LE MONDE

Les attaques *ransomware* les plus prolifiques

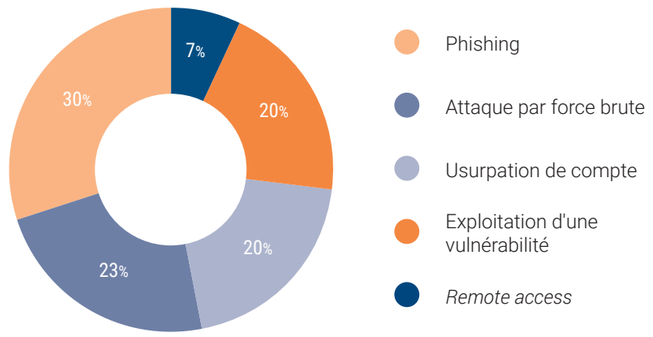


Données des victimes d'attaques *ransomware*



2.2 Source des attaques

Mécanisme des attaques



Le premier objectif des attaquants est de s'introduire dans le système d'information afin de le compromettre, c'est-à-dire de porter atteinte à la confidentialité, l'intégrité ou la disponibilité des données. Un des moyens pour y parvenir est de disposer d'un *login* / mot de passe. Cette combinaison ouvre l'accès au SI quelle que soit la qualité du blindage périphérique. Tous les moyens sont bons pour obtenir une clé d'entrée, ce qui explique notamment l'importance des campagnes de *phishing* et l'importance à donner aux fuites de données.

Une fois à l'intérieur du SI, les attaquants vont chercher à obtenir des privilèges (les fameux droits d'administrateur) afin de procéder à un état des lieux le plus complet possible, en accédant aux endroits normalement les plus protégés sans être détectés.

À défaut d'obtenir une clé d'entrée, l'exploitation de vulnérabilités critiques constitue un autre moyen de compromission. Elles sont la cause de 20 % des sinistres de notre échantillon, ce qui est loin d'être négligeable.

Les éditeurs de logiciels comme Microsoft et bien d'autres publient très régulièrement des bulletins de sécurité afin de corriger ces vulnérabilités. Ces vulnérabilités sont rapportées par les éditeurs eux-mêmes, mais aussi par des tiers. Certains publient même le moyen de les exploiter avant qu'elles ne soient corrigées par les éditeurs.

Ces stratégies de compromission soulignent combien les campagnes de sensibilisation des utilisateurs sont importantes. La prévention du risque cyber passe aussi par une stricte gestion des comptes à privilège et le compartimentage des réseaux. Il en est de même pour ce qui concerne la politique de *Patch management* (application des correctifs de sécurité).

Compte tenu des enjeux, les assureurs portent aujourd'hui une attention toute particulière sur ces sujets.

LA VULNÉRABILITÉ LOG4J

La vulnérabilité « LOG4J », annoncée sous la référence « CVE-2021-44228 », a été publiée le 9 décembre 2021. Qualifiée comme la plus importante vulnérabilité de ces 10 dernières années, en raison de sa criticité (possibilité d'exécuter un code malveillant à distance) et du nombre de programmes concernés, elle a perturbé les fêtes de fin d'année de nombreux DSI et RSSI.

Selon le site d'information Techspot, **plus de 840 000 cyberattaques ont été enregistrées en utilisant cette vulnérabilité dans les 72 heures suivant la découverte initiale.**

La raison d'une telle crainte ?

Cette faille a confronté les administrateurs système à une double difficulté. La première de corriger cette faille dans les meilleurs délais et la deuxième de chercher à identifier si un produit ou un système était bien affecté par cette vulnérabilité.

Le Ministère de la Défense Belge aurait été l'une des premières victimes de cette faille. Dans le mois qui a suivi la publication de cette vulnérabilité, le groupe de cybercriminel Conti a spécifiquement exploité cette faille pour diffuser un nouveau *ransomware* nommé Khonsari.

En 2022, les craintes d'exploitation de cette vulnérabilité sont toujours d'actualité.

PHISHING OU HAMEÇONNAGE

Le *phishing* constitue la première cause de compromission des SI.

Avec cette technique, l'attaquant adresse un e-mail ou SMS incitant le destinataire à utiliser le lien figurant dans cet envoi. L'attaquant pourra dans ce cas récupérer des mots de passe et des noms d'utilisateurs ou introduire un code malveillant utilisé par la suite.

ATTAQUES PAR FORCE BRUTE

L'attaquant emploie un programme permettant de générer des noms d'utilisateurs / mots de passe potentiels pour tenter d'accéder à une ressource (les attaques par dictionnaire constituent un type d'attaque en force brute). L'attaquant peut également tenter d'utiliser les mots de passe les plus couramment employés (de type « Password123 ») sur différents comptes.

USURPATION DE COMPTES

Des milliards d'informations sont dérobées chaque année lorsque des violations de données sont commises. Les mots de passe et noms d'utilisateurs divulgués sont un moyen pour les *hackers* d'avoir les clés pour prendre le contrôle d'un compte et compromettre ensuite les systèmes d'informations.

EXPLOITATION D'UNE VULNÉRABILITÉ

Des failles de sécurité affectant les navigateurs web ou les logiciels sont régulièrement révélés. Ces vulnérabilités, surtout lorsqu'elles ne sont pas corrigées, sont autant d'opportunités pour les *hackers*.

REMOTE ACCESS OU ACCÈS À DISTANCE

Avec la crise sanitaire et le déploiement du télétravail, la sécurisation souvent insuffisante des accès à distance a favorisé les attaques cyber. L'absence de VPN *(Virtual Private Network* ou réseau privé virtuel), un VPN mal sécurisé ou le non-déploiement de solutions d'authentification par multifacteur (MFA) favorise la réussite des attaques cyber.

L'ANNUAIRE *ACTIVE DIRECTORY*

L'annuaire *Active Directory,* centre névralgique de la sécurité des systèmes d'information Microsoft, est un élément critique permettant la gestion centralisée de comptes, de ressources et de permissions. L'obtention de privilèges élevés sur cet annuaire entraîne une prise de contrôle instantanée et complète de toutes les ressources ainsi administrées.

Suite aux multiples attaques sur les AD, les observations de l'ANSSI ont fait apparaître un manque de maturité critique et récurrent sur la sécurité des annuaires *Active Directory*. Un faible niveau de sécurité des annuaires met en danger les systèmes d'information dans leur globalité et fait porter un risque systémique sur les organisations.

Consécutivement à la recrudescence d'attaques, Microsoft, conscient du problème, a publié un document décrivant le « Tier-Model », seul modèle de design efficace pour concevoir des infrastructures *Active Directory* résistantes aux attaques de nouvelles générations.

2.3 Profondeur des attaques

Sur l'échantillon des sinistres analysés, les attaques cyber conduisent l'entreprise à devoir reconstruire totalement ou partiellement son système d'information dans 94 % des cas.

Le niveau maximum de compromission est constaté lorsque l'*Active Directory* est touché.

Après l'*Active Directory,* les sauvegardes représentent la deuxième cible stratégique des attaquants. En effet, la neutralisation des sauvegardes réduit la possibilité d'un redémarrage dans de bonnes conditions.

Les sauvegardes censées constituer une solution de secours en cas de sinistre s'avèrent souvent elles-mêmes compromises, insuffisantes ou défaillantes pour la récupération des données.

Très souvent, ces solutions de sauvegarde ont été pensées avant tout pour répondre à des scénarios de risques traditionnels, tels que l'incendie par exemple, et non pour faire face aux attaques cyber.

Face à ce constat, il est vivement recommandé, notamment par les assureurs, de disposer de sauvegardes hors lignes et d'une historisation suffisante.

3.

Impacts organisationnels

Les impacts d'un sinistre cyber sont multiples. Les activités seront plus ou moins fortement perturbées avec des répercussions à tous les niveaux.

Au niveau organisationnel et de manière non limitative :

- **perte de la messagerie (mail) et de la téléphonie (aujourd'hui sous IP),**

Les flux de communication internes / externes sont stoppés ou très perturbés :

- **indisponibilité des applicatifs dédiés aux fonctions supports, gestion RH, comptabilité, achats, ventes, gestion des stocks et de la chaîne logistique.**

Impossibilité de traiter les opérations en *front* et *back office :*

- **forte pression sur les équipes IT qui se retrouvent en première ligne pour remédier à l'indisponibilité totale ou partielle du SI.**

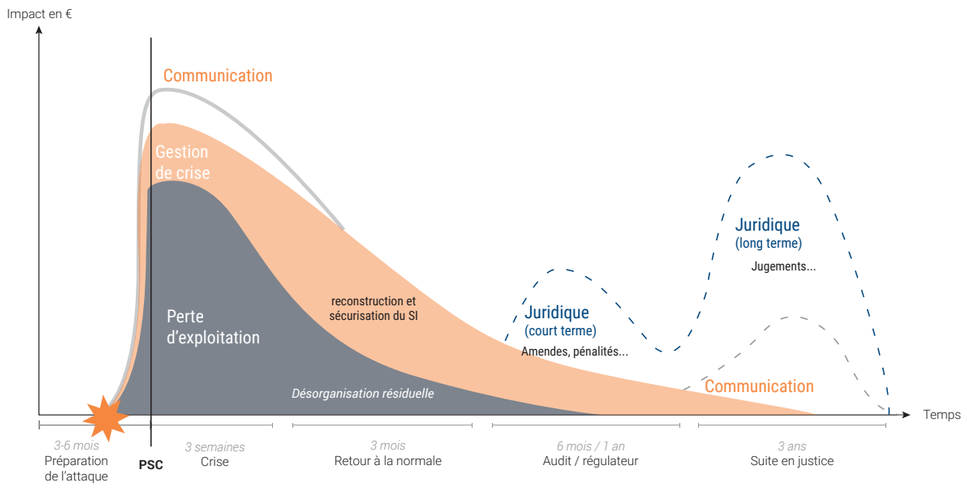
Difficulté à gérer à la fois l'incident au niveau technique et la pression interne du management ou des opérationnels.

3.1 Déclenchement de la gestion de crise

La découverte de l'attaque conduit à enclencher une situation de crise. La gestion de cette situation constitue la phase la plus critique d'une attaque cyber. La nature des mesures qui seront déployées, leur priorisation et la stratégie retenue vont influencer à la fois :

- l'organisation de la crise en interne,
- la gestion vis-à-vis de l'externe (clients, fournisseurs, actionnariats),
- les délais de remédiation,
- les coûts financiers.

Typologie et répartition des impacts d'une crise majeure avec destruction forte du SI



Cette première phase de sidération, puis de crise où l'entreprise est plus ou moins paralysée à différents niveaux, est non seulement une phase de stress mais également de déstabilisation.

Les interrogations quant à la date d'infection initiale et la profondeur de l'attaque sont étendues et les perspectives de redémarrage ne trouvent aucune réponse immédiate, surtout si l'entreprise ne s'y est pas préparée.

Cette préparation repose, sur des mesures organisationnelles telles que disposer d'un plan de gestion de crise testé, d'un plan de continuité d'activité éprouvé. Elle dépend aussi de mesures techniques comme la robustesse de la politique de sauvegarde ou l'organisation de l'architecture IT.

C'est dans cette phase particulière de crise qu'une déclaration de sinistre sera effectuée.

3.2 Le rôle de l'assistance et l'importance des mesures de Forensic en phase de crise.

Les polices d'assurance cyber prévoient toutes un volet Assistance. C'est un des points forts de ces contrats car il apporte un véritable soutien aux entreprises victimes de cyberattaques. Il est confié par les assureurs à des prestataires tel qu'INQUEST qui interviennent en réponse à un incident 7/7 jours et 24/24h.

Dans la phase de crise, cette assistance participe à la mise en œuvre rapide de bonnes pratiques et évite donc des décisions précipitées, potentiellement préjudiciables pour l'entreprise. L'intervention à distance sur le SI de l'entreprise va rapidement permettre de qualifier la nature de l'incident cyber et de soutenir les mesures à prendre pour limiter sa propagation. Un support en communication de crise ou pour toute déclaration CNIL sera également proposé.

Le prestataire fera également le lien avec l'assureur pour l'informer des options de remédiation dans les meilleures conditions.

La découverte d'une attaque ne signifie pas que celle-ci soit stoppée. Il est donc indispensable de mener des opérations d'investigations numériques afin de :

- s'assurer que l'attaquant n'a plus accès au système d'information avant de redémarrer et donc d'éviter la poursuite de l'attaque ou une seconde intrusion ;
- recueillir les éléments de preuve de l'attaque, utiles à l'assurance et à toute enquête judiciaire ;
- mesurer le niveau et l'étendue de la compromission du système d'information afin d'optimiser les actions de remédiation et le planning de déploiement ;
- arbitrer entre les délais nécessaires au *forensic* et la remise en état du SI au regard des impacts financiers.

Certaines entreprises, en particulier les TPE et PME, négligent cette phase d'investigation numérique car jugée trop onéreuse, complexe voire inutile. Cela va de pair avec la volonté de redémarrer au plus vite des activités.

La mise en œuvre de ces mesures participe à optimiser la gestion de tout sinistre cyber.

Toutefois, ces mesures de *forensic* ne donnent pas toujours de résultats probants, notamment lorsque l'historisation des journaux d'évènements est insuffisante ou pire, lorsque ces derniers sont supprimés par l'attaquant.

Les journaux d'évènements sont des fichiers textes où sont enregistrées de manière chronologique toutes les actions exécutées (ouverture et fermeture d'une application, d'une session, installation d'un programme, navigation sur Internet...).

Chaque action produit une ligne d'information dans un fichier de *log*. L'ensemble des évènements exécutés est stocké sur ces fichiers. Ils s'avèrent indispensables pour identifier et analyser la provenance d'un *bug* ou relever toute compromission d'un système d'information car toute attaque laisse des traces.

Sans ces journaux de *log,* aucune opération de *forensic* n'est possible. L'identification exhaustive des zones impactées ou non par l'attaque sera de fait limitée. La question de la reconstruction numérique se posera nécessairement pour les zones où un doute subsiste sur l'existence d'une compromission forte.

Les décisions prises à ce moment-là auront un impact sur les délais de remédiation et les coûts du sinistre.

3.3 Délais de retour à la normale

Le délai de retour à une situation normale est une composante clé de la sinistralité cyber.

Ce délai comprend à la fois :

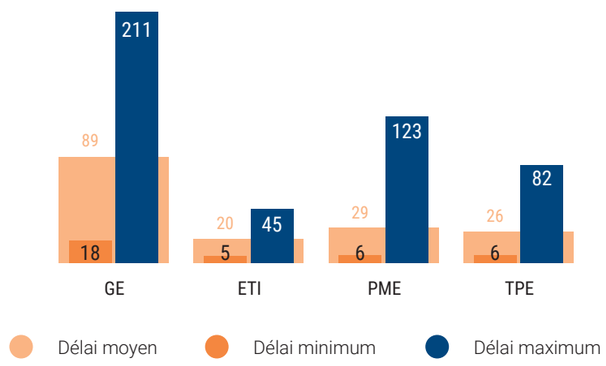
- le délai à partir duquel l'entreprise retrouve un niveau normal en termes d'activités, il sert de référence pour déterminer le montant des pertes d'exploitation indemnisables ;
- le délai nécessaire à la reconstruction du système d'information où se concentre l'ensemble des dépenses informatiques. Il peut être supérieur au délai retenu pour l'indemnisation des pertes d'exploitation, en particulier lorsque la remise en œuvre de certaines composantes du SI qui n'influencent pas le niveau d'activité intervient en fin de période de remédiation.

Le délai de retour à une situation normale est très variable car inhérent au profil de risque de chaque entreprise.

Ce délai est influencé par plusieurs facteurs :

- le nombre de filiales,
- l'organisation géographique et métier,
- les interdépendances,
- la complexité du SI.

Délai de retour à la normale (en jours)



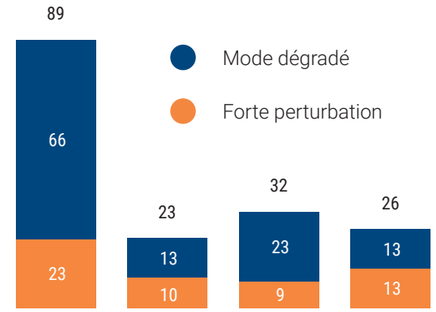
3.4 Délais de perturbation des activités

Le délai de perturbation des activités se répartit en deux périodes.

Une période de très forte perturbation des activités qui est concomitante avec la phase de crise. Durant cette phase, l'objectif est de tout mettre en œuvre pour retrouver rapidement un niveau d'activité satisfaisant.

Une période de reprise des activités en mode dégradé suivi d'un retour progressif à un niveau d'activité normal.

Délai de perturbation des activités / SI (en jours)



Le niveau de perturbation des activités dépend en particulier :

- du niveau de destruction du SI et du volume de données à restaurer,
- du niveau de dépendance des activités par rapport au SI.
- du nombre de postes et de serveurs potentiellement infectés. Les opérations de *forensic* seront d'autant plus longues à réaliser que le nombre de postes et de serveurs à vérifier est important.
- de la capacité de restauration du SI via les sauvegardes.

Quel que soit le niveau de maturité de la politique de cybersécurité ou le niveau de résilience de l'entreprise, le délai de résolution d'une attaque cyber se compte en semaines ou en mois.

Les délais de reprise d'activité, évalués à quelques heures suite à une indisponibilité du système d'Information sur des scénarios classiques de risque (pannes, incendie…) sont sans commune mesure avec les délais auxquels il faut s'attendre en cas d'attaque cyber. À minima, le délai pour conduire les seules opérations de *forensic* est de 3 à 5 jours.

La corrélation entre le niveau d'activité et le bon fonctionnement des systèmes informatiques est également variable selon les entreprises. Le niveau d'exposition varie en fonction de l'imbrication du SI sur les métiers.

Ces quelques constats soulignent par ailleurs que la modélisation du risque cyber est un sujet complexe.

4.

Impacts financiers

Nous avons pu conduire une analyse fine du coût de la sinistralité pour en faire ressortir les principales composantes.

Au niveau des impacts financiers, l'étude distingue les montants de frais et pertes rapportés par les entreprises sinistrées, du montant des frais et pertes indemnisé par l'assurance.

4.1 Montants des frais et pertes rapportés par les entreprises sinistrées

Ces informations proviennent des rapports d'expertise établis par STELLIANT.

	NOMBRE DE DOSSIERS	PERTES DÉCLARÉES (M€)
GE	7	109
ETI	11	32
PME	26	30
TPE	15	3
TOTAL	**59**	**174**

Sur la période 2019-2021 et sur un total de 59 sinistres, le montant global des préjudices financiers rapportés par les entreprises impactées s'élève à 173,5 M€.

Nous développerons plus en détail, ci-après, la répartition des postes de préjudices.

Moyenne des frais et pertes rapportés par segment

L'échelle des pertes par sinistre oscille entre 50 K€ et plus de 40 M€ au global, avec un fort écart type sur chaque segment.

	NOMBRE DE SINISTRES	MOYENNE DES PERTES REPORTÉES (M€)
GE	7	15
ETI	11	3
PME	26	1
TPE	15	0,2

Sans surprise, les impacts financiers d'un sinistre cyber sont proportionnels à la taille des entreprises.

Ces données soulignent également que les impacts sur les TPE-PME sont loin d'être négligeables. Compte tenu de la surface financière des TPE, une perte nette moyenne de 210 K€ est de nature à les fragiliser.

Le coût moyen d'un incident cyber, bien souvent repris comme indicateur dans différentes études, est par ailleurs un indicateur très relatif étant donné les écarts observés.

4.2 Montants des frais et pertes traités par l'assurance

Ces montants de frais et pertes incluent :

- l'ensemble des frais et pertes indemnisés sur les dossiers clos,
- les frais et pertes rapportés sur les dossiers toujours en gestion à la date de réalisation de cette étude. Ces frais et pertes sont donc susceptibles d'évoluer à la hausse ou à la baisse.

	NOMBRE DE DOSSIERS	TOTAL DOSSIERS TRAITÉS PAR L'ASSURANCE (M€)
DOSSIERS CLOS	47	65
DOSSIERS OUVERTS*	12	64
TOTAL	**59**	**129**

(*) La base des dossiers traités a été arrêtée en février 2022 pour analyse. À cette date 12 dossiers étaient toujours en gestion à un stade avancé sur le chiffrage.

La différence entre le total des frais et pertes rapportés (173,5 M€) et les frais et pertes traités par l'assurance (129,09 M€), soit près de 43 M€, trouve plusieurs explications :

- une limite de garantie assurée inférieure au montant du sinistre. Cela concerne quelques dossiers pour un montant global non garanti de plus de 35 millions au titre des pertes d'exploitation.
- Un écart entre la prise en charge des postes de préjudices qui relèvent du contrat d'assurance et la somme des dépenses engagées ainsi que des montants de pertes présentés. Trois postes de garanties sont identifiés :

1 -> **Les pertes d'exploitation** où le total des pertes d'exploitation rapportées nécessite d'être retraité.

2 -> Certaines **dépenses informatiques** lorsqu'elles conduisent à des améliorations du système d'information, notamment les dépenses engagées pour renforcer la sécurité.

À la suite d'une attaque cyber, la reconstruction du système d'information de l'entreprise ne se limite pas à une reconstruction à l'identique. Le sinistre ouvre en effet la possibilité d'engager des travaux de refonte, d'amélioration ou d'évolution qui étaient souvent programmés à terme.

L'assureur vérifiera donc avec attention l'ensemble des factures présentées pour ne retenir que les frais nécessaires à la reconstruction afin de ne pas avoir à supporter des investissements dont le financement est du seul ressort de l'entreprise.

Les choix qui seront faits pour la reconstruction du SI influenceront de fait les délais de reprises des activités et le niveau des pertes d'exploitation. Pour ce qui concerne les frais de reconstruction informatique engagés, il y aura donc un écart avec le niveau d'indemnisation retenu.

3 -> Les **frais internes** tels que les salaires, lorsque les équipes sont fortement mobilisées pour un redémarrage rapide des activités.

Cette problématique vise plus particulièrement les équipes SI lorsqu'elles sont employées à reconstruire le SI plutôt qu'à leurs tâches habituelles. La prise en charge de ces frais, prête à discussion et ces frais peuvent ne pas être couverts. Ce sujet est toutefois accessoire par rapport aux deux premiers.

4.3 Montant des frais et pertes indemnisés sur les sinistres clos

Sur l'ensemble des dossiers clos, soit 47 dossiers à la date de réalisation de l'étude, le montant des pertes indemnisées fait ressortir un décalage avec le montant des pertes rapportées par les entreprises pour les raisons indiquées précédemment.

EN M€	SINISTRES CLOS
PERTES RAPPORTÉES	110
PERTES INDEMNISÉES	65,29 (1)

(1) Dont 35 M€ non indemnisés du fait de limites de garanties insuffisantes et un écart de 8 M€ entre les pertes d'exploitation déclarées et le montant retenu à dire d'expert.

Ce montant de pertes indemnisées ne reflète en aucune manière la portée des résultats techniques du marché de l'assurance en cyber sur la période considérée. Les dossiers en cours d'instruction, les provisions passées par les assureurs, tout comme les sinistres sur lesquels STELLIANT n'intervient pas, n'étant pas pris en compte.

REMARQUE IMPORTANTE

Sur l'ensemble des sinistres étudiés, aucune réclamation de nature à actionner le volet « Responsabilité Civile » des polices Cyber n'a été instruite, bien que des fuites de données aient été constatées.

Il est vrai que l'environnement réglementaire et juridique, en France comme en Europe (RGPD), n'est pas comparable à celui des États-Unis où les fuites de données se traduisent le plus souvent par des sinistres particulièrement coûteux.

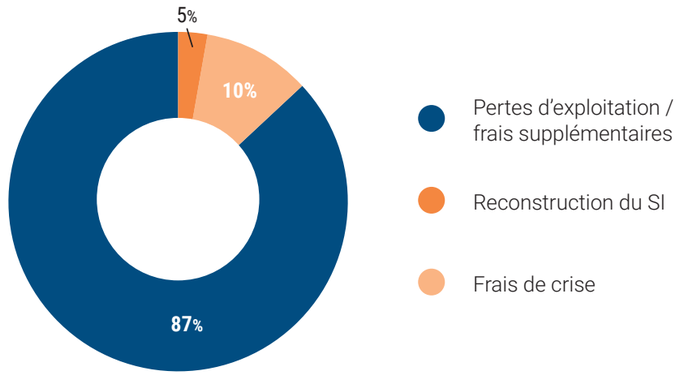
4.4 Répartition des frais et pertes

Les frais et pertes sont répartis sur trois grands postes.

- Les frais engagés pendant la **phase de crise** qui comprennent notamment :
  - les frais liés aux mesures d'investigation numérique *(Forensic),*
  - les frais de communication et autres frais spécifiques de gestion de crise,
  - les frais liés aux mesures à prendre en cas de fuite de données personnelles.
- Les frais engagés pendant **la phase de reconstruction du système d'information.** Ces frais comprennent :
  - les dépenses de reconstruction du SI par le biais de prestataires externes,
  - les frais de déchiffrement,
  - les frais de reconstitution des données.
- Les frais et pertes du fait de **la baisse du niveau d'activité :**
  - les pertes d'exploitation,
  - les frais supplémentaires d'exploitation.

4.4.1 Répartition des frais et pertes rapportés sur l'ensemble des dossiers

	FRAIS DE CRISE	RECONSTRUCTION DU SI	PERTES D'EXPLOITATION / FRAIS SUPPLEMEN-TAIRES
GE	1,21	10,96	96
ETI	0,63	2,04	29
PME	2,79	4,30	23
TPE	0,54	1,09	2
TOTAL	5,18	18,39	150



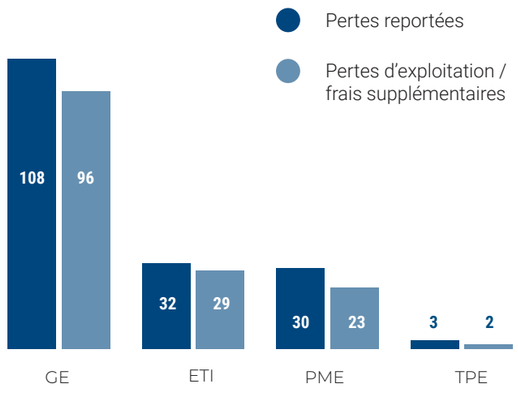
Il ressort nettement que le poids des pertes d'exploitation est prépondérant par rapport à l'ensemble des frais et pertes. Cela illustre à quel point l'activité des entreprises est dépendante de leur système d'information (SI).

4.4.2 Répartition des frais et pertes sur les dossiers clos

DOSSIERS CLOS (M€)	FRAIS DE CRISE	RECONSTRUCTION DU SI	PERTES D'EXPLOITATION / FRAIS SUPPLEMENTAIRES
PERTES RAPPORTÉES	3,70	7,76	98
PERTES INDEMNISÉES	3,12	5,21	57

4.4.3 Poids des pertes d'exploitation reportées par segment (tous sinistres)

	TOTAL DES PERTES REPORTÉES	PERTES D'EXPLOITATION / FRAIS SUPPLEMENTAIRES	PART AUTRES FRAIS ET PERTES
GE	108	96	89%
ETI	32	29	92%
PME	30	23	76%
TPE	3	2	49%
TOTAL	173	150	86%



Le montant des pertes d'exploitation est logiquement corrélé avec le volume d'activité de l'entreprise. Toutefois, les conséquences d'un sinistre cyber sont très variables d'une entreprise à une autre, à taille et activité comparables.

Plusieurs facteurs entrent en jeu pour apprécier les impacts financiers d'un sinistre cyber :

- le secteur économique,
- le modèle économique qui sous-tend la création de valeur,
- l'organisation du SI de l'entreprise,
- la qualité de la politique de cybersécurité de l'entreprise et son niveau de résilience,
- le niveau de compromission du SI lié à l'attaque.

Chaque organisation a donc son propre profil de risque, influencé par l'ensemble des facteurs présentés.

PERTES D'EXPLOITATION

La perte d'exploitation est une notion financière qui s'intéresse au préjudice économique des entreprises lié aux pertes subies ou aux gains manqués à la suite d'une activité réduite, voire un arrêt complet d'activité.

Il n'y a pas de définition légale de la perte d'exploitation — la comptabilité légale ne s'y intéresse pas directement — le droit français ne la définit pas spécifiquement.

ASPECT ASSURANTIEL DES PERTES D'EXPLOITATION

Dans le langage de l'assurance, elle résulte, sauf cas particulier tel le cyber, d'un préjudice matériel (incendie, inondation, bris de machine, etc.).

Un arrêt ou une diminution d'activité engendre une perte de chiffre d'affaires et donc une perte d'exploitation. C'est la marge sur les coûts variables non engagés, rapportée au chiffre d'affaires non réalisé, qui est indemnisable. L'indemnisation d'une perte d'exploitation par la marge sur les coûts variables vise donc à couvrir les charges fixes plus le bénéfice éventuel sur la période d'interruption de l'activité liée au sinistre.

Il appartient à la victime de chiffrer sa demande avec les différents justificatifs des postes composant le préjudice total.

4.4.4 Poids des frais et pertes (hors pertes d'exploitation) rapportés par segment (données en M€)

Sur les frais de gestion de crise

	TOTAL DES PERTES REPORTÉES	DONT FRAIS DE GESTION DE CRISE	PART DES FRAIS DE CRISE
GE	108	1	1%
ETI	32	0,6	2%
PME	30	3	9%
TPE	3	0,5	17%
TOTAL	173	5,1	3%

Sur les frais de reconstruction du SI

	TOTAL DES PERTES REPORTÉES	DONT FRAIS DE RECONSTRUCTION DU SI	PART DES FRAIS DE RECONSTRUCTION DU SI
GE	108	11	10%
ETI	32	22	6%
PME	30	4	14%
TPE	3	1	34%
TOTAL	173	18	11%

Les frais et pertes, hors pertes d'exploitation, représentent en moyenne près de 14 % des impacts financiers générés par une attaque cyber, ce qui est non négligeable.

Les frais de gestion de crise, tout comme les frais de reconstruction du SI, sont a priori plus conséquents sur les petites et moyennes structures proportionnellement au montant total des pertes.

5.

Quels enseignements ?

La survenance d'un sinistre cyber majeur est avant tout un traumatisme pour les entreprises qui en sont victimes. Ne plus être en mesure de communiquer, de produire, de facturer ou de stocker parce que l'informatique ne répond plus, relève du risque catastrophique.

LE POIDS IMPORTANT DES PERTES D'EXPLOITATION ET UN CHIFFRAGE SOUVENT COMPLEXE

Sans grande surprise, les pertes d'exploitation représentent plus de 80 % des impacts financiers. Elles sont particulièrement importantes rapportées à la période d'interruption des activités, qui est en moyenne inférieure à 3 mois.

Les caractéristiques de ce risque en termes d'impacts sont bien différentes des caractéristiques des sinistres plus classiques tels que l'Incendie ou tout évènement naturel par exemple.

Contrairement au risque d'incendie ou de catastrophe naturelle dont les effets directs sont très circonscrits, une attaque cyber est susceptible d'avoir des impacts bien plus étendus, au niveau géographique notamment. C'est le cas lorsque les fonctions supports portées par l'informatique sont hors service (logistique, facturation, communication…) et que les activités de tous les sites d'un groupe se retrouvent paralysées.

Lorsque plusieurs sites sont directement ou indirectement touchés par un sinistre cyber, le chiffrage et la consolidation des pertes d'exploitation comme des frais supplémentaires d'exploitation se révèlent être un exercice complexe. L'exercice suppose en effet de traiter la situation de chaque site, de chaque métier et d'intégrer une vision d'ensemble consolidée. Sur ces questions, l'interfaçage entre l'expert et l'entreprise suppose une coordination étroite et un accès aux interlocuteurs qualifiés.

La gestion des pertes d'exploitation sur le risque cyber présente donc des caractéristiques spécifiques pour l'assurance. Dans la pratique, il est parfois difficile pour les entreprises de documenter les états de pertes présentés.

Quelques exemples de situations complexes rencontrées :

- les sites d'un même groupe victimes d'une attaque cyber enregistrent des niveaux de perturbation différents et des dates de redémarrage variables suivant les sites ;
- l'interdépendance des activités entre plusieurs sites induit des difficultés à traiter la perte de marge de chaque site par rapport à la perte de marge consolidée ;
- la détermination des capacités de report et de rattrapage de l'activité peut difficilement être réalisée durant la période de perturbation ;
- des facteurs exogènes à l'attaque, telle que la crise COVID, viennent complexifier l'appréciation des pertes rapportées.

Le périmètre des pertes d'exploitation est parfois difficile à circonscrire. Sur un certain nombre de sinistres, la question des pertes d'exploitation se pose lorsque des sites n'ont pas été directement touchés mais ont vu leur SI débranché par sécurité afin d'éviter tout risque de propagation.

La même question se pose pour des filiales dont le SI n'est pas impacté par l'attaque, mais qui enregistrent des pertes du fait de leur dépendance à d'autres entités ou activités du groupe.

Ces différents cas de figure entrainent une analyse différenciée des pertes d'exploitation et un débat sur la notion de pertes d'exploitation directes et indirectes. En fonction de la rédaction des polices d'assurance, le traitement indemnitaire ne sera donc pas le même.

De manière générale, retenons que les décisions de l'entreprise dans la phase de crise et de reprise de ses activités ont un impact sur les pertes d'exploitation. À défaut de les avoir suffisamment partagées avec l'assureur et justifiées sur le plan technique, les conséquences de ces choix constituent une source de discussion sur la prise en charge des états de pertes présentés. Le lien avec l'expert mandaté par l'assureur en charge du volet pertes d'exploitation et le courtier est donc primordial.

DES OPÉRATIONS DE *FORENSIC* ESSENTIELLES

Elles participent à la compréhension de l'incident et à l'identification des points de faiblesse. Elles permettent surtout de mettre en place une stratégie de redémarrage et de remédiation optimum en limitant au maximum le risque de résurgence des attaquants.

Il est impératif de mener ces opérations avant toute reconnexion du système d'information. Selon la configuration du SI, ces opérations prennent a minima quelques jours, tout comme la phase de redémarrage.

Quelle que soit la qualité de la politique de cybersécurité d'une entreprise, toute compromission du SI peut rapidement avoir des impacts financiers importants.

LES IMPACTS D'UN SINISTRE CYBER S'APPRÉCIENT EN SEMAINES, VOIRE EN MOIS

C'est un des enseignements de cette étude. On ne se rétablit pas d'une attaque cyber significative en quelques heures ou en quelques jours. A minima, les opérations de *forensic* nécessitent entre 2 et 5 jours selon la configuration du SI.

Ensuite, l'affichage d'un retour à la normale des activités est, dans la plupart des cas, la résultante d'un fonctionnement en mode dégradé.

LE RÔLE IMPORTANT DU VOLET ASSISTANCE DES POLICES D'ASSURANCE CYBER

Dans la phase de crise, obtenir très rapidement un accompagnement via le volet Assistance des polices d'assurance Cyber apporte une aide indéniable car peu d'entreprises disposent d'un plan de gestion de crise testé et surtout adapté face à ce type de risque.

L'intervention d'experts qualifiés sur ces problématiques, mandatés par l'assureur ,participe à installer un dialogue efficace, voire apaisé, dans cette phase importante.

Des questions simples mais essentielles vont rapidement se poser, en particulier sur la planification des actions à conduire. Dans quel ordre redémarrer ? Que faut-il prioriser ?

Le partage des retours d'expériences acquis par les assureurs facilite une gestion d'ensemble et la prise de décision.

La coordination et l'échange régulier d'informations entre l'entreprise, son courtier, l'assureur et son expert, favorise fortement la bonne instruction du sinistre.

CÉDRIC LENOIRE

PARTIE #02

La valorisation des risques, un outil de pilotage face à la menace cyber

#02

Regard

de Cédric Lenoire

Cédric Lenoire
Analyste financier pertes d'exploitation, BESSÉ

De nombreuses études réalisées par les professionnels de l'assurance, de la gestion des risques, et de la cybersécurité nous permettent aujourd'hui de mieux appréhender les risques cyber. Nous savons par exemple que la professionnalisation et la spécialisation des acteurs malveillants entraine une évolution constante de la menace.

L'écosystème cybercriminel étant désormais bien plus riche en ressources, les attaquants sont en mesure de préparer plus minutieusement leurs opérations, d'exploiter plus efficacement les vulnérabilités présentes sur les systèmes des potentielles victimes, ou encore d'élargir les surfaces d'attaques grâce aux nouveaux usages numériques comme le Cloud ou la multiplication des divulgations de données.

Nous savons aussi que les conséquences d'une menace cyber peuvent être identiques à celles associées aux risques d'entreprise plus traditionnels : l'outil opérationnel d'une société peut être mis à l'arrêt par une attaque cyber au même titre qu'un incendie entraînant la destruction d'une usine ou une rupture de chaîne d'approvisionnement provoquant une pénurie de matières premières. Les pertes financières générées (frais de remédiation et de gestion de crise, pénalités, pertes d'exploitation, etc.) peuvent alors fragiliser la structure touchée jusqu'à en compromettre sa survie.

Enfin, nous constatons que le transfert du risque cyber vers l'assurance devient de plus en plus restreint. Augmentation des primes et des franchises, limitation des conditions et garanties, durcissement par les assureurs des exigences relatives à la maturité des programmes de cybersécurité, l'assurance cyber est devenue plus difficilement accessible pour de nombreuses entreprises faisant face à des contraintes budgétaires imposées par une conjoncture économique actuelle défavorable.

> 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.

Face à ces constats, les dirigeants d'entreprise ayant pris conscience des enjeux associés à la cybermenace se lancent dans une démarche de structuration et de coordination des mécanismes de traitement du risque. La cyber résilience visant à garantir une stabilité opérationnelle, commerciale et financière en toutes circonstances devient alors un élément incontournable de gouvernance. Cependant, un problème récurrent auquel les organisations sont confrontées implique la priorisation des ressources dédiées lorsqu'il n'y a pas de vision commune au sein des équipes dirigeantes. Élaboration d'un programme de cybersécurité visant à identifier les activités malveillantes, sensibilisation des employés et autres parties prenantes à la menace, mise en place d'une gestion de crise visant à anticiper les conséquences néfastes d'une attaque, développement de plans de continuité des activités assurant un mode de fonctionnement dégradé et de reprise d'exploitation facilitant la remise en état des opérations perturbées : les dirigeants cherchant à établir une feuille de route pertinente doivent faire face à la nécessité d'arbitrer les ressources financières, humaines ou technologiques dans un environnement de plus en plus incertain. Le développement d'un outil de pilotage et d'aide à la décision est alors essentiel pour assurer le déploiement d'une cyber résilience visant à protéger la pérennité financière et commerciale de l'organisation en situation de crise.

> La valorisation financière des risques favorise le développement d'une compréhension commune des menaces cyber au sein de l'organisation.

À ce titre, la valorisation financière des risques visant à évaluer l'impact des scénarios les plus probables est devenue indispensable puisque le déploiement de 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 contribue au développement d'un business plan de la cyber résilience en phase avec les enjeux financiers associés aux principales menaces identifiées et détermine l'orientation et le niveau des investissements à consentir pour préserver la pérennité de l'entreprise. Concrètement, elle se réalise à partir de l'identification des métiers et activités clés dépendant des systèmes informatiques pouvant être compromis en cas d'attaque, ainsi que l'analyse des enjeux stratégiques, financiers et commerciaux de l'entreprise. En se lançant dans cette démarche, les dirigeants se donnent les moyens de mesurer avec exactitude les différents scénarios de risques qu'ils estiment pertinents et ainsi de prioriser les efforts de résilience sur les activités les plus vulnérables à la menace cyber et dont l'entreprise ne peut absolument pas se passer.

PARTIE #03

Regards croisés

#03

Regard

de Guy-Philippe Goldstein

Guy-Philippe Goldstein

Guy-Philippe Goldstein est enseignant à l'École de Guerre Économique, contributeur au journal académique de l'Institute for National Security Studies à Tel-Aviv sur les questions de cyber-puissance et cyberdéfense, et advisor pour PwC ainsi que pour ExponCapital, un fonds de Venture Capital. Il est également l'auteur de romans d'anticipation sur les questions cyber ainsi que d'un essai, « Cyberdéfense et Cyberpuissance au XXI[e] siècle » (Balland, 2020).

> Les dirigeants français d'entreprise placent même ce risque à un niveau supérieur que celui de leurs homologues mondiaux.

Une accélération de la menace

Les cyber-risques continuent de constituer une des menaces les plus importantes pour l'entreprise, amplifiée par la crise COVID-19, avec une accélération de la menace en 2021 comparée à 2020, déjà année de hausse considérable. Sur la totalité de l'année, selon les sources, le nombre d'attaques de rançongiciels a augmenté entre +48 %[(1)] et +93 %[(2)] toujours comparé à 2020, avec des augmentations de +120 % aux États-Unis et +230 % en Grande-Bretagne[(3)]. Les dirigeants français d'entreprise placent même ce risque à un niveau supérieur à celui de leurs homologues mondiaux : 55 % en France[(4)], et en progression de 36 %, contre 49 % au niveau mondial[(5)] selon le PwC Global Survey.

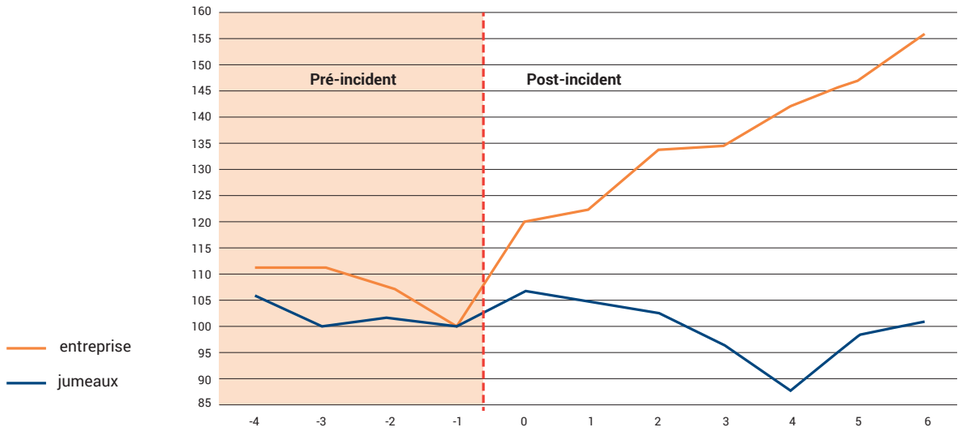
La prise de conscience est donc désormais là, mais il reste donc une question clé : jusqu'où investir ? Si le coût total de l'impact n'est pas clair pour l'entreprise, les mesures de réduction du risque seront trop limitées. Les entreprises risquent donc d'échouer dans leur objectif d'amortissement du choc.

L'impact économique total des incidents cyber

Complétant et approfondissant une première étude de BESSÉ publiée fin 2020 sur les entreprises non-cotées[(6)], une nouvelle étude de BESSÉ Assurance, réalisée avec l'aide de G.P. Goldstein Consulting, montre que pour les ETI et les PME françaises non cotées, sur un panel de 48 incidents entre 2017 et 2021, le risque de défaillance augmente en moyenne de 50 % dans les 6 mois qui suivent l'annonce d'un incident cyber[(7)].

Évolution du risque de défaillance – Entreprises victimes & jumeaux statistiques

(N=48 / 2017-2021/ Entreprises françaises uniquement / Base 100 = « Mois -1 » avant le mois de l'incident)



> Le facteur moteur de la dégradation économique semble être une crise de réputation et de confiance dans l'entreprise.

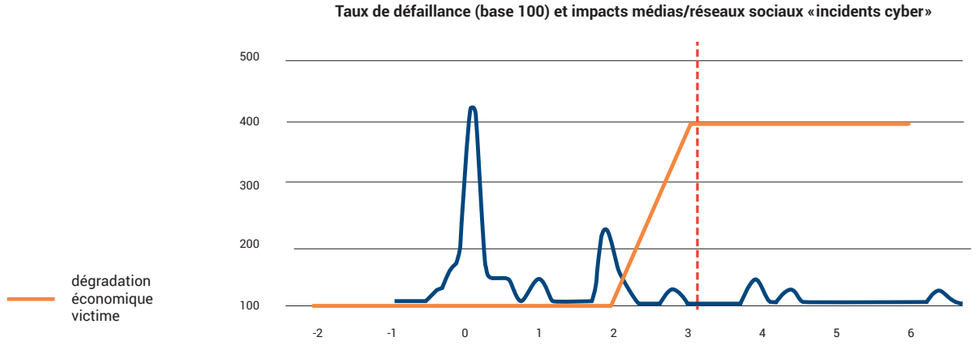
Une crise de réputation et de confiance

La dégradation continue notée plus haut semble indépendante de la remédiation technique, souvent acquise dans ses aspects les plus saillants au bout de quelques semaines. Le facteur moteur de la dégradation économique semble être une crise de réputation et de confiance dans l'entreprise.

Une analyse préliminaire de corrélation entre activités et réaction en ligne autour de l'incident cyber d'une part, et évolution de la probabilité de défaillance de l'autre, présente une corrélation modérée (r=45 %), non due au hasard, soulignant bien l'existence de phénomènes réputationnels [8]. À nouveau, l'impact est différé dans le temps, comme vu sur l'exemple illustratif, sur la base d'un cas anonymisé.

Illustratif - Evolution du risque de défaillance et des impacts médias/réseaux sociaux

Exemple anonymisé / Base 100 = « Mois -1 » avant le mois de l'incident



Cependant, les impacts économiques réels surviennent dans les 2-3 mois et peuvent être entretenus par des effets rebond de l'actualité. L'analyse de certains cas montre le danger réputationnel à ne se montrer ni transparent ni responsable dans la communication vis-à-vis des clients, partenaires et collaborateurs. C'est particulièrement vrai avec l'essor récent d'attaques de « double extorsion », où certains groupes cybercriminels finissent par divulguer eux-mêmes au public l'existence de l'attaque afin de faire pression sur la victime.

Données récoltées : Altarès/ Dun& Bradstreet (données de dégradation économique) et Talkwalker (analyses d'impact de réaction en ligne).

(1) *https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/*
(2) *https://www.computerweekly.com/news/252504676/Ransomware-attacks-increase-dramatically-during-2021*
(3) *https://www.sonicwall.com/news/sonicwall-the-year-of-ransomware-continues-with-unprecedented-late-summer-surge/*
(4) *https://www.pwc.fr/fr/publications/dirigeants-et-administrateurs/global-ceo-survey/25eme-annual-global-ceo-survey.html*
(5) *https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html*
(6) *https://www.besse.fr/en/crise-cyber-quel-impact-sur-la-valorisation-des-entreprises-non-cotees*
(7) *Analyse réalisée sur la base de données Altarès - Dun & Bradstreet, sur 48 incidents entre 2017 et 2021, incluant les données de score « taux de défaillance » (compris entre 1 et 20, 1 = risque maximal, 20 = risque minimal), incluant les scores « taux de défaillance » moyen pour les secteurs industriels liés à chaque incident ; ainsi qu'un panel de 3-5 jumeaux statistiques pour chaque entreprise victime (entreprise du même secteur et de la même taille)*
(8) *Analyse préliminaire réalisée sur la base de données Talkwalker, sur n=21 incidents, en particulier concernant le rapport entre nombre d'engagement (re-publication, commentaires, « like ») total sur le nombre total d'articles parus suite à l'incident cyber – note "Incident Cyber – transformation Engagement/Résultats" avec p-value=0.1%<1%*

Regard

de Laurent Porta

Laurent Porta

Titulaire d'une maîtrise de Droit International Public, Laurent Porta a débuté sa carrière comme chargé de mission au Ministère de la Justice, puis consultant chez D'Arcy corporate et Leo Corporate. Il a rejoint Vae Solis Communications en tant que Directeur Associé. Spécialiste de la communication de crise et de la prévention des risques, il est intervenu en gestion de crises pour des organisations et grandes entreprises, sur des thématiques sociales, sanitaires et judiciaires. Il accompagne également des dirigeants en communication d'engagement et prises de parole.

*Aujourd'hui, l'actualité cyber peut facilement se résumer par trois notions : **volumétrie, détection et évaluation de la résistance.** L'objectif visé pour les entreprises étant d'atteindre un niveau élevé de cyber résilience.*

L'anticipation et la préparation sont donc les maîtres-mots qui doivent être au cœur de la stratégie de résistance que ces dernières se doivent d'opposer aux attaques cyber.

Ce n'est plus la peine de perdre du temps à s'interroger si « je vais être touché » mais plutôt « Qu'est-ce que je dois protéger ? » et « Comment je me prépare ? ». Si la place de l'IT est indéniable dans cette phase, elle doit, pour être complète, s'accompagner d'une forte préparation de la communication.

Selon l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) les attaques cyber ont été multipliées par 4 en 2020. Le constat réalisé fait état de hackers qui innovent et propagent des menaces informatiques de plus en plus sophistiquées.

En 2021, le rapport NTT Global Threat Intelligence indique une augmentation de 300 % des attaques par ciblage opportuniste. Cela signifie, s'il fallait encore le préciser, que toutes les entreprises (indépendants, TPE/PME, ETI, grandes entreprises, etc.) peuvent être touchées.

La France se place en huitième position des pays les plus impactés par les attaques cyber, le FBI ayant recensé en 2020 1 640 victimes de délits informatiques. Nous restons cependant loin derrière les États-Unis, mais aussi le Royaume-Uni qui figure en deuxième place avec 216 633 proies. La France se place par ailleurs devant l'Allemagne qui dénombre 1 578 victimes.

La forte digitalisation des entreprises et de leur écosystème, notamment lors de la pandémie de COVID-19, amène à une vigilance de plus en plus accrue des systèmes d'information et des données. Le débat aujourd'hui étant de savoir quel sera l'impact de l'attaque qu'elles subiront sur leur fonctionnement ?

Quelle réaction faut-il avoir ?

La cybercriminalité est protéiforme, elle ne décroit pas, elle ne disparait pas… elle peut seulement se combattre de façon plus complète et donc plus efficace. Il s'agit dans un premier temps d'intégrer au sein de l'entreprise que la cyber résilience est l'affaire de tous. Elle doit être pilotée par la Direction Générale qui lui allouera les budgets et ressources adaptés.

La crise cyber est donc bien du ressort de l'IT, du juridique, de la finance, mais également de la communication et aussi de tout salarié peu ou mal informé des principes de précaution les plus élémentaires à respecter lorsqu'il est connecté aux réseaux de son entreprise ; constituant alors un point d'entrée privilégié pour les hackers.

La réduction des impacts de survenance des évènements de sécurité sera essentiellement réalisée grâce à des mesures se situant en amont. On parle en effet de mesures préventives car nous sommes là dans le domaine de la gestion du risque.

Les entreprises doivent donc toutes travailler à développer leur cyber résilience en identifiant les données et les applications vitales sans lesquelles elles ne peuvent plus fonctionner.

Une fois ce travail réalisé, il faut alors veiller à protéger ces données et réfléchir aux moyens de revenir rapidement à une situation acceptable pour l'entreprise victime d'une attaque. Ce plan de continuité (PCA), s'il prévoit les mesures techniques, doit, pour être complet et efficace, inclure un volet communication conséquent.

La cyber résilience s'appuie sur 2 jambes : les moyens techniques et la communication

Préparer la crise cyber sur le plan de la communication implique de réfléchir à la réputation de l'entreprise et à ses obligations réglementaires.

La communication doit être préparée à l'aune de la visibilité que pourrait avoir demain une attaque cyber auprès des collaborateurs, des clients, des prospects, des partenaires.

La visibilité d'une attaque peut être multiple. Parfois, elle n'est visible que de l'entreprise et de ses salariés ; bien souvent, ce sont les clients ou les partenaires qui découvrent par hasard le défaut de fonctionnement, conséquence de l'attaque.

Pour ces derniers, la communication fait partie des obligations règlementaires des entreprises. La raison est simple : la protection des données détenues par une entreprise est de son entière responsabilité. Il lui revient donc de prendre les mesures adéquates pour en assurer l'intégrité. L'enjeu ici, pour l'entreprise, est de se préparer à notifier ses clients et partenaires et à rassurer ses collaborateurs dans le moment de post-intrusion.

> La cyber résilience est donc bien un projet global d'entreprise qui doit être mené en parfaite collaboration.

Adopter les bons comportements : communiquer de manière transparente et proactive.

Se préparer à répondre aux questions de ses salariés, clients, partenaires, et plus largement, à communiquer sur une compromission de système par exemple, est la nouvelle doxa en matière de sécurité.

Après les mauvais réflexes et faux-pas commis par certaines grandes entreprises telles qu'Equifax en 2017 ou Garmin en 2020, les entreprises ont pris conscience que des messages trop tardifs, ou cherchant à minimiser au maximum l'attaque, étaient somme toute peu compréhensibles pour l'opinion publique et finalement contre-productifs quant à la capacité perçue à gérer l'événement.

Dans la gestion opérationnelle de la crise, manifester une mobilisation en demi-teinte, déconnectée de l'ampleur de l'attaque, est improductive en termes d'image.

Et ce d'autant plus que depuis quelque temps, l'attaque cyber n'est plus forcément vécue comme une maladie honteuse, les entreprises hésitent moins à les rendre publiques auprès d'une audience qu'elles ont choisie (clients, partenaires, interne). La culture de la honte et du secret disparaît au profit d'une communication plus assumée. On passe donc à une communication responsable, transparente et humble, davantage susceptible d'attirer l'empathie et ainsi préserver le capital réputation.

L'essentiel est de garder le lien avec vos publics

Au-delà des dommages purement financiers, les entreprises victimes d'attaques cyber subissent d'autres impacts importants en termes de réputation, de confiance des clients ou des salariés, et d'heures de travail perdues.

Selon l'étude réalisée par l'assureur Swiss Re, le coût moyen du plus long arrêt d'un système dans une entreprise après une attaque malveillante a été évalué à 762 231 dollars.

Il est important, d'une part, de sensibiliser en interne, et d'autre part, d'entraîner les équipes à gérer la situation, tant au niveau des moyens techniques que de la communication.

Quel rôle joue la sensibilisation dans une démarche de cyber résilience ?

Il faut savoir que le *phishing* représente 80 % des attaques cyber, soit des attaques misant sur l'usurpation d'identité pour pénétrer un système et obtenir des données privées et/ou confidentielles (selon le rapport de Statista sur les attaques les plus fréquentes en France – juillet 2021).

Les pirates comptent sur le facteur humain pour arriver à leurs fins, c'est pourquoi la sensibilisation est une étape essentielle, voire salvatrice, pour faire face à ces risques.

Ainsi, mettre en situation ses équipes à l'aide d'un exercice de simulation de crise cyber qui reproduit attaques et sollicitations de l'interne, des clients, des médias et de la société civile, génère des résultats immédiats.

En effet, à partir d'un scénario réaliste de crise bruyante (conjuguant visibilité et impact opérationnel pour l'entreprise) et adapté à la réalité de l'entreprise, il s'agit donc de tester pour les renforcer :

- les capacités de détection et de traitement des attaques cyber destructrices,
- les réponses à apporter en matière de maintien minimum d'activité tant sur un plan technique qu'auprès des collaborateurs,
- Les outils pour récupérer les données « offline » et relancer un mode dégradé d'activité,
- L'aptitude à garder le lien avec vos cibles internes (collaborateurs) et externes (clients, partenaires, médias), par l'élaboration de messages simples, clairs et pédagogiques.

La cyber résilience est donc bien un projet global d'entreprise qui doit être mené en parfaite collaboration entre la Direction Générale, la communication, les équipes techniques SI, les équipes métier et bien entendu les utilisateurs.

> Il ne faut pas croire que la crise cyber n'arrivera pas. Il faut se préparer à la gérer !

Regard

de Fabienne Lopez

Fabienne Lopez

La colonelle de gendarmerie Fabienne Lopez est la cheffe du Centre de lutte contre les criminalités numériques (C3N) depuis l'été 2019. Précédemment, elle a commandé la compagnie de gendarmerie départementale de Pamiers (09). Elle a ensuite été cheffe de division au sein de l'Office Central de Lutte contre les Atteintes à l'Environnement et à la Santé Publique (OCLAESP). À l'issue de cette affectation, elle a occupé le poste d'officier adjoint chargé de la police judiciaire, au sein du groupement de gendarmerie départementale à Versailles (78) et enfin elle a tenu le poste de commandant en second de la section de recherches de Bordeaux (33), avant d'intégrer le C3N.

Le C3N est l'unité de police judiciaire de la gendarmerie nationale chargée d'enquêter sur le haut du spectre de la cybercriminalité. Le C3N détient une compétence territoriale nationale qui lui permet d'agir sur l'ensemble du territoire. Il est également chargé d'appuyer les unités de terrain, que ce soit sur les plans procéduraux, techniques d'enquête ou à l'international. Pour permettre à la gendarmerie nationale d'offrir aux victimes une proximité, une écoute et une action judiciaire efficaces, le C3N anime et coordonne 11 antennes réparties dans les régions. Ces antennes sont constituées d'enquêteurs formés aux nouvelles technologies, ainsi qu'à certaines techniques d'enquêtes spécifiques à ce contentieux. Elles sont le prolongement des capacités d'enquête du C3N dans les territoires.

Depuis février 2021, le C3N a intégré le Commandement de la gendarmerie dans le cyberespace (COMcyberGEND). *Cette nouvelle formation administrative a pour mission de lutter contre la cybercriminalité sous toutes ses formes, en utilisant tous les leviers mis à sa disposition, depuis la prévention jusqu'à la répression. Le C3N en est la composante judiciaire.*

Les domaines d'actions prioritaires du C3N sont les atteintes aux traitements automatisés de données (ASTAD), incluant la thématique des rançongiciels, les trafics sur le darknet, les crypto-actifs, *les atteintes sexuelles sur mineurs sur internet et tous phénomènes d'ampleur ciblant la population dans son ensemble.*

> 77 % des infractions concernent des escroqueries en ligne, parfois pour des montants atteignant plusieurs millions d'euros.

Par qui le C3N est-il mandaté ? Combien de plaintes traite-t-il par mois ou par an ?

En tant qu'unité de police judiciaire, le C3N peut classiquement déclencher une enquête, dès lors qu'il est désigné par un parquet local saisi d'un fait criminel. **Il peut également se saisir d'initiative d'un fait dont il a connaissance.** Son engagement est ensuite confirmé par le parquet judiciaire compétent. Il agit sous le contrôle d'un magistrat.

Le nombre de plaintes est variable en fonction du type de contentieux. **Si l'on prend l'exemple des attaques par rançongiciels, contentieux prioritaire pour le C3N en raison des préjudices subis et de la capacité de déstabilisation qu'il représente, il est courant que nous soyons informés de plusieurs attaques dans une même semaine.** Ce contentieux est tout particulièrement suivi par le parquet cyber de la JUNALCO à Paris.

Les moyens, les résultats, exemple d'affaire :

Nos investigations intègrent des constatations techniques. Pour ce faire, le C3N s'appuie sur la division de l'appui aux opérations numériques (DAONUM) du COMcyberGEND. Cette dernière est armée d'experts et d'ingénieurs de très haut niveau.

Le volet international est également incontournable dans nos enquêtes. **Sur la thématique des rançongiciels, le C3N a été à l'initiative de groupes de travail incluant plusieurs partenaires étrangers.** Ces groupes permettent à l'ensemble des forces participantes de gagner en rapidité et en efficacité dans les enquêtes, par l'échange et le recoupement d'informations. **C'est ainsi qu'en à peine un an, nous avons pu procéder à l'interpellation d'individus impliqués dans une structure criminelle d'envergure qui s'était attaquée à plusieurs multinationales françaises.**

Observations menaces cyber, tendances, panorama :

L'année 2021 a été marquée par une croissance continue des infractions numériques, avec près de 130 000 faits enregistrés contre 104 000 en 2020 pour la seule zone gendarmerie, soit une augmentation de 20 %. En quatre ans, la cybercriminalité a ainsi doublé. L'année 2022 s'inscrit dans la même continuité en termes de procédures judiciaires recensées. Il ne faut cependant pas oublier qu'un grand nombre d'infractions ne font pas l'objet d'un dépôt de plainte auprès des forces de l'ordre et que le nombre de faits commis est beaucoup plus important.

77 % des infractions concernent des escroqueries en ligne, parfois pour des montants atteignant plusieurs millions d'euros, les atteintes aux systèmes de traitement automatisé de données ou le piratage représentent 10 % des infractions et 13 % concernent des atteintes aux personnes et la haine en ligne.

Cette évolution permet de constater la persistance de nombreux phénomènes cybercriminels, le perfectionnement structurel et technique de la cybercriminalité organisée, et notamment des groupes APT spécialisés dans les botnets et rançongiciels, contre lesquels la gendarmerie est particulièrement engagée.

Les cybermenaces demeurent donc un risque majeur pour les années à venir. **Les acteurs malveillants vont continuer à cibler des entreprises stratégiques, les administrations, mais également des entreprises de petite et moyenne taille, ainsi que les particuliers.**

L'écosystème de la cybercriminalité organisée est en constant renouvellement, notamment via les flux des acteurs d'un groupe à un autre, ou encore les nouvelles versions ou dénominations de souches de logiciels malveillants.

Les principaux secteurs ciblés par les rançongiciels sont l'industrie, le commerce, la santé, **les administrations, le bâtiment, l'informatique, la finance ou encore l'agriculture.**

Conclusion

Cette étude illustre que la sinistralité cyber a ses propres caractéristiques. Elle est principalement influencée par deux facteurs : l'étendue de la compromission du SI et la capacité de résilience de l'entreprise face à une attaque.

La réduction du niveau d'exposition passe donc nécessairement par la prévention de ce risque au travers des moyens de détection et de réponses à incident, de la capacité à redéployer son SI, le tout appuyé par un Plan de Reprise d'Activité robuste. Ces éléments sont aujourd'hui regardés avec la plus grande attention par les assureurs dont le niveau d'expertise technique s'est nettement renforcé en quelques années.

Au niveau assurantiel, cette étude souligne que les couvertures d'assurances cyber remplissent correctement leur objet. Le référentiel contractuel demeure encore hétérogène, ce qui n'a rien de surprenant si l'on considère que ce marché de l'assurance cyber en France a moins de 10 ans. Le cadre contractuel est voué à évoluer pour arriver à maturité.

Avec l'explosion de la sinistralité depuis 2019, le marché de l'assurance s'est par contre fortement contracté. Outre une baisse significative de la capacité disponible doublée de hausses tarifaires, les prérequis pour s'assurer se sont également renforcés. Face aux attaques *ransomware,* les assureurs sous-limitent les garanties sur ce risque et de nouvelles limitations sont annoncées pour traiter du risque systémique par exemple. La question se pose également d'exclure les conséquences d'actes cyber émanant de conflits entre États.

Pour les entreprises, ces évolutions ne sont pas à la hauteur de leurs attentes en matière de transfert de ce risque vers l'assurance, d'autant que le rebond des attaques cyber enregistrées depuis le 2e trimestre 2022 témoigne d'une menace cyber toujours très présente.

Face à cette situation, une étroite collaboration entre tous les acteurs de l'écosystème cyber est indispensable pour contenir ce risque à des niveaux acceptables. C'est certainement l'une des conditions pour que l'offre et la demande d'assurance soient en adéquation.

CB.IARD (commercialement dénommée « BESSÉ Industrie & Services »)
Ecrire à : 46 bis rue des Hauts Pavés – BP 80205 - 44002 Nantes Cedex 1
SAS au capital de 253 545 € - Siège social : 135 Boulevard Haussmann 75008 Paris - RCS Paris 873 800 023

Conseil et courtier en assurances (exerçant conformément à l'article L521-2-1°b) du Code des assurances)
N° Orias 07 022 453 – www.orias.fr | Soumis au contrôle de l'ACPR – 4 place de Budapest 75009 Paris
Liste des fournisseurs actifs disponible sur www.besse.fr
Toute réclamation ou demande sur les procédures de médiation peut être adressée par écrit au Service Réclamation BESSÉ Industrie & Services 46 bis rue des Hauts Pavés – BP 80205 - 44002 Nantes Cedex 1. Vous recevrez un accusé de réception sous 10 jours maximum et une réponse dans un délai maximum de 2 mois.

www.besse.fr — www.stelliant.com