Pérenniser l'entreprise face au risque cyber

De la cybersécurité à la cyberrésilience

CHAMBRE DE COMMERCE ET D'INDUSTRIE

1er ACCÉLÉRATEUR DES ENTREPRISES

CCI PARIS ILE-DE-FRANCE

REMERCIEMENTS

Les auditions effectuées ont représenté une matière irremplaçable lors de la phase d'investigation de cette étude. Nos plus vifs remerciements s'adressent à ceux qui ont apporté leur retour d'expérience*

Maxime ALAY-EDDINE, Fondateur & Président - CYBERWATCH

Nicolas ARPAGIAN, Directeur de la Stratégie - ORANGE CYBERDÉFENSE

Didier BARBOLLAT, Responsable Analyse & Anticipation - SOCIÉTÉ GÉNÉRALE

Marc-Henri BOYDRON, Fondateur et Dirigeant - CYBER COVER

Annabelle CHREBOR*, Co Fondatrice - E-TIPI LEARNING

Paola FABIANI*, Présidente - WISECOM

Jean-Philippe GAULIER, Principal Co Founder - CYBERZEN

Yassir KAZAR, CEO & Co Founder - YOGOSHA

Jérôme NOTIN, Directeur général - GIP ACYMA cybermalveillance.gouv.fr

Véronique PLESSIER CHAUVEAU*, Fondatrice et Dirigeante - EULEOS

Didier RAUCH*, Président - AVERA

Nous tenons aussi à adresser un remerciement particulier à Monsieur Joël THIERY, élu référent « Intelligence économique et cybersécurité dans les entreprises » pour ses précieux conseils.

Les échanges qui ont eu lieu en Commission Économie et Financement des entreprises de la CCI Paris-Île-de-France ont permis d'enrichir les travaux et les propositions. Nos remerciements particuliers à Messieurs Jean-Claude KARPELES, Pierre-Etienne DEHON et Jérôme FRANTZ.

Cette étude étant le fruit d'un travail collaboratif entre la CCI Paris Île-de-France et CCI France, nos remerciements s'adressent aussi à Philippe CLERC, CCI France, pour avoir partagé son expertise sur l'Intelligence économique et les questions de cybersécurité.

Enfin, nos remerciements vont aux personnes qui ont apporté le savoir et la compréhension nécessaires à la construction de cette étude et qui ne peuvent être ici citées pour des raisons de confidentialité.

Cette étude a été réalisée par Pierre-Arnaud MOREAU,

Département Prospective, CCI Paris-Île-de-France

dans le cadre du programme annuel d'études et de rapport des CCI piloté par CCI France

* Également Membres départementaux de la CCIR.

GLOSSAIRE

Concept/ Acronyme	Traduction/Signification
2FA	Authentification à deux facteurs
ACPR	Autorité de contrôle prudentiel et de résolution
AFNOR	Agence française de normalisation
ANSSI	Agence nationale de la sécurité des systèmes d'information
BaaS	Backup as a Service (Sauvegarde en tant que service)
BMC	Business Model Canvas
CCI	Chambre de commerce et d'industrie
Cloud computing	Accès à des services informatiques via des applications hébergées sur Internet ou un cloud
CNIL	Commission nationale de l'informatique et des libertés
COMEX	Comité Exécutif
CPS	Cyber Physical System
Cryptolockers	Verrouilleurs par cryptage
DaaS	Distribution as a Service : distribution de malwares tiers dans le cadre d'opérations de téléchargement
Darknet	Réseau superposé offrant des fonctions d'anonymat
DDOS	Attaque par déni de service
DEVOPS	Contraction de développement applicatif (Dev) et administration des infrastructures informatiques (Ops)
DEVSECOPS	Contraction de développement applicatif (Dev), sécurité (Sec) et administration des infrastructures informatiques (Ops)
DRaaS	Disaster Recovery as a service (récupération de désastre en tant de service)
DSI	Direction des services d'information
ENISA	European Union Agency For Cybersecurity
FSN	Fournisseur de services numériques
IoT	Internet of things (objets connectés)
IP Address	Adressage Internet Protocol
Maas	Malware as a Service
Maching Learning	Apprentissage automatique d'une intelligence artificielle
OIV	Opérateur d'importance vitale

OSE	Opérateurs de services essentiels
PCA	Plan de continuité d'activité
Phishing	Hameçonnage
RaaS	Resilience as a Service ou, dans l'économie parallèle, Ransonware as a Service
Ransomware	Rançongiciel
RGPD	Règlement européen sur la protection des données personnelles
RSSI	Responsable de la sécurité des systèmes d'information
SDLC	Software Development Lifecycle (SDLC) ou cycle de vie du développement logiciel
Spear Phishing	Harponnage (variante de l'hameçonnage avec une dominante d'ingénierie sociale)
Token	Actif numérique pouvant être transféré sans duplication entre deux acteurs sur Internet, sans nécessiter l'accord d'un tiers
UBA	User Behavior Analytics ou analyse du comportement utilisateur
VPN	Réseau privé virtuel
WAF	Web Application Firewall ou sécurité applicative

RÉSUMÉ

Pérenniser l'entreprise face au risque cyber, c'est savoir prendre soin des deux faces d'une même pièce. La première, faciale, représente la valeur de l'entreprise et les actifs qu'elle doit protéger. La seconde, fiduciaire, représente la confiance dans le dispositif de protection et l'avenir de l'entreprise.

Dans l'hypothèse d'une cyberattaque, la question est alors de savoir si l'entreprise risque ou non de perdre toute la pièce ; à défaut de pouvoir protéger la valeur faciale, c'est la capacité à pérenniser l'activité et à durer dans le temps qui est, en effet, engagée.

Pour illustrer cette métaphore, un chiffre : 60 % des PME qui subissent des cyberattaques déposent le bilan sous six mois, autrement dit toute la pièce !

Le risque cyber est aujourd'hui permanent et presque inévitable comme a pu le montrer la recrudescence des attaques pendant la pandémie de la Covid 19 : une cyberattaque a lieu toutes les 39 secondes dans le monde[1] !

La *première difficulté* réside dans le fait que les TPE et PME continuent de considérer que « ça n'arrive qu'aux autres ». Aujourd'hui, tout est connecté et sujet à cybercrime : les surfaces d'attaque en sont élargies depuis les ordinateurs et smartphones des collaborateurs jusqu'aux machines connectées dans l'industrie 4.0 en passant par l'Internet des objets (IoT).

L'entreprise est la première victime du risque cyber. Pourtant, il n'y a pas de fatalité ! Et la crise du Covid illustre avec pertinence comment une entreprise peut changer la donne en reconnaissant et en acceptant ce risque comme étant la première menace réelle à son activité.

On voit qu'il y a là une question de sensibilisation des dirigeants de TPE et de PME voire de grosses PME (ETI) qui n'est pas complètement réglée quand bien même les outils de formation existent. Il y a donc des leviers tels que la certification ou l'assurance à mobiliser auprès des TPE-PME : 90 % des entreprises du CAC40 et 50 % du SBF120 sont déjà assurés contre ce risque tandis que plusieurs secteurs ou filières adoptent normes et certifications dans ce sens.

La *seconde difficulté* réside dans le fait que les chefs d'entreprise considèrent le risque cyber comme un sujet technologique. Or, la plupart des cyberattaques provient des failles de la part des utilisateurs qui sont souvent considérés comme la « passoire » des hackers. Le risque cyber est donc un sujet humain.

On voit là qu'il y a une question de compréhension : il faut pouvoir sortir de la technicité du sujet qui en fait un domaine réservé des experts pour entrer dans la logique *business* avec « des mots qui parlent » aux chefs d'entreprise.

Dans ce contexte, c'est à la question de la pérennité de l'activité et de l'entreprise que s'est attachée cette étude.

En effet, face à un risque cyber, une première approche, défensive et réactive, consiste à protéger les systèmes d'information (SI) de l'entreprise. C'est ce qu'on appelle la cybersécurité : elle passe par la mise en conformité avec les outils juridiques mais aussi par des outils technologiques (mise à niveau et bonne configuration des SI et bonne composition avec des solutions systèmes de type cloud).

Cette approche essentielle n'est, cependant, pas suffisante. Une entreprise ne peut entièrement se protéger en empilant antivirus et *firewalls* d'autant que cela peut alourdir les systèmes, monopoliser les ressources humaines et que la menace peut resurgir. Il faut aller plus loin car la cybersécurité ne garantit pas la continuité d'activité (perte de valeur faciale) ni la pérennité (perte de valeur fiduciaire).

Une seconde approche, offensive et proactive, consiste à accepter le risque, s'y préparer et s'organiser non seulement pour ne plus mettre en péril l'activité de l'entreprise mais aussi pour assurer la continuité d'activité. C'est ce qu'on appelle la cyberrésilience (comme une plus grande poupée russe qui inclut la cybersécurité comme prérequis). Celle-ci passe par :

[1] Selon les Nations Unies, 30 mai 2020.

- une adhésion de toutes les composantes de l'entreprise (directions, fonctions et collaborateurs) à la posture et à la stratégie adoptée en fonction de la cartographie des risques ;
- une prise en compte de l'écosystème (fournisseurs, clients et partenaires) dans cette gestion du risque et dans la construction d'une réponse pérenne ;
- et une gouvernance qui permet d'avoir des structures de décision agiles et réactives et de placer l'expertise de cyberprotection (RSSI) de façon appropriée dans l'organisation de l'entreprise.

Mais la cyberrésilience ne s'arrête pas là : elle est aussi une capacité à innover et à se transformer pour apporter la confiance et la performance de l'entreprise. Cette capacité à pérenniser son activité et améliorer sa performance par une politique cyberrésiliente peut constituer un véritable avantage concurrentiel pour l'entreprise.

C'est en intégrant le risque cyber comme composante du cycle de vie que les entreprises pourront s'en « affranchir » et que leur accompagnement par des organismes d'État et des corps intermédiaires, déjà largement investis sur ce terrain, pourra gagner en efficacité.

C'est cette culture de la cyberrésilience, valeur ajoutée pour les entreprises, que les Chambres de commerce et d'industrie (CCI) souhaitent faire éclore par cette réflexion.

SOMMAIRE

INTRODUCTION

Devant le constat que presque deux PME sur trois[2] déposent le bilan après une cyberattaque et que seulement une sur dix se dit apte à y faire face, CCI France et la CCI Paris Ile-de-France se sont saisies de la question du risque cyber pour les entreprises afin de souligner l'urgence de changer de posture.

La cybersécurité a longtemps été considérée comme un sujet d'experts dont la compréhension et la gestion étaient « chasse gardée » des Directions des systèmes d'information (DSI) et des apporteurs de solutions. L'évolution du cybercrime (risque exogène) mais surtout des usages dans l'entreprise (risque endogène) comme le fait de travailler avec son propre matériel (BYOD)[3] en font une préoccupation de tous. Les solutions technologiques employées sont le plus souvent optimales, mais l'esprit humain est toujours supérieur en créativité et en adaptabilité. Encore faut-il avoir les moyens de réagir.

Si chacun peut intervenir dans la prévention des cyberattaques, l'immunité n'existe pas. Il n'existe pourtant pas de fatalité et la prise en compte du risque cyber peut être l'occasion d'opportunités pour l'entreprise. C'est le sens de la cyberrésilience.

CCI France et la CCI Paris Ile-de-France ont voulu mettre en avant les mécanismes qui permettent aux entreprises de tirer profit des investissements et des ajustements qu'elles mettent en œuvre pour organiser une véritable résilience face au cyber risque. Le réseau consulaire national est le pivot pour faire le lien entre les acteurs et les outils qui sont autant de leviers de cyberrésilience.

Cette étude n'invite pas à changer le logiciel, selon l'expression consacrée, mais elle invite à faire évoluer la machine, logiciel compris. Il s'agit de procéder par une montée en puissance de la réponse : de la cybersécurité vers la cyberrésilience.

[2] Chiffres issus du Rapport cyber-sinistres, Hiscox, 2019.
[3] Buy Your Own Device.

PARTIE LIMINAIRE

PANORAMA DES CYBERATTAQUES ET DE LEUR IMPACT SUR LES ENTREPRISES

La numérisation des entreprises rend celles-ci de plus en plus vulnérables au risque cyber. Les attaques sont de plus en plus nombreuses et de natures de plus en plus variées. Cette situation est aggravée en temps de crise car le niveau d'exposition des entreprises aux risques cyber augmente à ce moment-là. La menace vient de toute part et touche n'importe quelle entreprise. Mais la réponse des entreprises est encore inégale et largement dépendante de leur maturité numérique.

Maxime ALAY-EDDINE
CYBERWATCH

« Des actions simples existent et peuvent être mises en œuvre selon le niveau de prise de conscience de chaque organisation.. »

A) LA MULTIPLICATION DES CYBERATTAQUES : DE L'INSAISISSABLE À L'INVISIBLE

1) Une évolution liée à deux facteurs : numérisation de l'économie et professionnalisation des cybercriminels

Les cyberattaques représentent aujourd'hui un phénomène d'une ampleur considérable[4]. En 2019, le système antivirus Kaspersky[5] a observé une croissance de plus de 500 % (523 % exactement) du nombre de menaces détectées. Quelque 100 000 codes malveillants sont générés par jour dans le monde.

a) Les cyberattaques croient avec la numérisation

L'augmentation des cyberattaques est étroitement liée à la digitalisation des activités et la capacité d'intrusion des hackers devrait encore augmenter avec l'ordinateur quantique. Toutes les protections seront cassables en quelques secondes maximum ! De même, l'usage d'imprimantes 3D connectées, le développement de l'Internet des objets dans l'industrie (IIoT) ou encore le déploiement de la 5G représenteront autant de portes d'entrée nouvelles pour la cybercriminalité. L'industrie 4.0 est, en effet, étroitement liée à la connectivité des machines, matériels, supports et systèmes.

Les cyberattaques touchent tous les secteurs qui ont numérisé leur activité ou leurs processus de production. Seules les activités totalement analogiques (non numériques) sont, en apparence, épargnées. Elles le sont en apparence car chaque activité est également tributaire de ressources extérieures du fait des interconnexions entre systèmes d'information. Elles peuvent ainsi être affectées par des externalités négatives dues à des cyberattaques par effet ricochet.

L'utilisation croissante des outils numériques pendant le confinement sanitaire (télétravail, téléconférence, etc.) en a aussi été une illustration, montrant qu'il existe aussi un caractère exogène à la cybermenace. Depuis décembre 2019, 50 % des noms de domaine créés en lien avec la Covid-19 sont, en effet, malveillants (générant une attaque directe et visible) ou intègrent des logiciels malveillants (générant une attaque indirecte et invisible). De plus, l'apparition de ces noms de domaine a suivi la progression géographique et temporelle du Coronavirus[6].

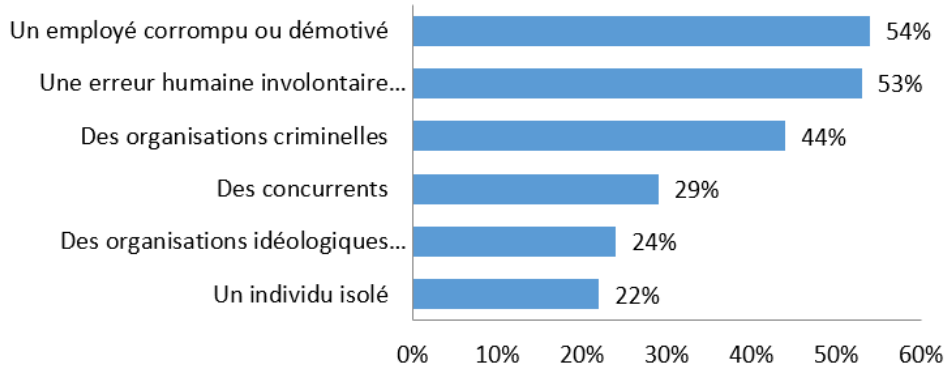
À chaque faille ou pratique à risque dans les systèmes informatiques, les cybercriminels déclenchent des attaques à grande échelle ou contaminent les systèmes. *« La guerre d'Internet continue pendant la crise épidémique et la prochaine épreuve de souveraineté dépassera en ampleur celle des masques»*[7]. On parle de cyber-ouragan[8] pour désigner cette perspective de crise mondiale majeure qui impacterait massivement et simultanément les entreprises qui ne se seraient pas « parfaitement » protégées[9].

[4] On entend par cyberattaque, l'atteinte aux systèmes informatiques réalisée dans un but malveillant.
[5] Kaspersky est une entreprise russe, leader mondial, de cybersécurité ; elle a été fondée en 1997.
[6] « Le COVID-19 : une nouvelle arme pour la cyber malveillance », Thalès, Note d'information, mars 2020.
[7] Alain Bauer, « Le prochain virus sera cyber », L'Opinion, 24 avril 2020.
[8] Pour reprendre ici l'expression du criminologue Alain Bauer.
[9] Cybermenace – avis de tempête, Étude, Institut Montaigne, novembre 2018.

b) Les cybermenaces profitent non pas tant des failles technologiques qu'humaines

La cybercriminalité ne s'appuie pas vraiment sur les failles de sécurité technologiques pour se développer. Elle prolifère surtout à partir des failles de sécurité humaines. C'est ainsi que 99 % des cyberattaques s'alimentent de failles résultant de l'action humaine. On peut voir dans la figure ci-dessous quelles sont les principales sources de failles humaines.

Répartition des principales sources de failles humaines



Source : Le baromètre cybersécurité 2019 par Sylob, L'Usine Nouvelle et Hub One

« *En 2019, 51 % des attaques ont eu recours à des techniques dépourvues de logiciels malveillants, contre 40 % en 2018, ce qui souligne la nécessité d'aller au-delà des solutions antivirus classiques* »[10].

La fréquence des « arnaques au Président » (escroquerie aux faux ordres de virement - FOVI) qui n'est pas une cyberattaque à proprement parler - montre à quel point l'humain est au cœur des failles, même les plus évidentes. Ainsi, « *plus de 23 milliards d'euros ont été volés par des cybercriminels depuis 2016, suite à la compromission d'emails centrés sur les individus* »[11], que ce soit via l'arnaque au Président, l'usurpation d'identité ou par rançonnage. C'est parce que les hackers en sont pleinement conscients que s'est développée l'ingénierie sociale, forme de cybercriminalité qui consiste à exploiter la nature humaine pour mieux la rançonner.

Parfois, ces failles sont occasionnées par des tiers appartenant au cercle intime des collaborateurs ou des dirigeants d'entreprise. Ainsi, des systèmes ont été pénétrés et ont perdu leur intégrité via les proches de dirigeants ou directeurs qui possédaient des droits étendus sur les systèmes d'information de l'entreprise. Un exemple connu est celui de la compromission d'un système par l'intégration d'un *malware* téléchargé par l'enfant d'un dirigeant : ce dernier cherchait à télécharger illégalement un film, via Bit Torrent, le logiciel légal de pair à pair *(peer-to-peer)*[12].

c) Les cyberattaques s'accroissent avec la professionnalisation de la cybercriminalité

Les cybercriminels ne connaissent qu'une maxime qu'ils vérifient à chaque cyberattaque : « *Quand on veut, on peut !* ». Mais cela va plus loin aujourd'hui avec une professionnalisation de plus en plus poussée de la cybercriminalité. Les outils des cybercriminels proposent un panel assez large pour que nulle activité ou nulle forme d'entreprise ne soit épargnée.

« *Les organisations cybercriminelles se sont développées en suivant les mêmes modèles économiques que le monde des affaires. Elles sont même structurées en domaines d'activité stratégique (business unit) avec : « un département dédié à la recherche de cibles sur les réseaux sociaux, un autre à la création d'emails de phishing, un autre faisant office de centre d'appels, un autre encore un pôle d'infographistes et même un département de recrutement ! »* »[13]. L'écosystème de la cybercriminalité se complexifie et atteint une maturité dont les codes et compétences sont transposés de l'économie traditionnelle avec des catégorisations servicielles :

[10] Loïc Guézo, « Déstabiliser l'économie mondiale de la cybercriminalité », Forbes France, 19 novembre 2019. 11 Global Threat Report 2020, CrowdStrike Intelligence.
[11] Global Threat Report 2020, CrowdStrike Intelligence.
[12] « Le code malveillant Dridex : origines et usages », ANSSI, 25 mai 2020.
[13] Loïc Guézo, op. cit.

- la chasse au « gros gibier » menée par des développeurs de logiciels rançonneurs ou *Ransomware as a Service* (RaaS) ;
- l'introduction de modules de *ransomware* par des développeurs de logiciels malveillants ou *Malware as a Service* (MaaS) ;
- la distribution de *malwares* tiers dans le cadre d'opérations de téléchargement ou *Downloading as a Service* (DaaS).

Cette économie connaît ainsi les mêmes mécanismes que l'économie traditionnelle et les mêmes contraintes d'adaptation et de concurrence. À titre d'exemple, le marché des programmes malveillants sur le *Darknet* contraint les cybercriminels à adopter des offres différenciantes. Or, pour se défendre contre les menaces, les entreprises doivent avoir conscience de ce « facteur humain ». Si le cybercrime devient à la portée de tous, il est potentiellement capable d'affecter tout le monde à travers une seule et même vague offensive.

2) L'impossible identification des cybermenaces

a) Les cyberattaques n'ont pas de cible définie : toute entreprise est concernée

Il n'y a pas de cible définie ou identifiée par les cybercriminels, à l'exception de cas précis comme le cyberespionnage (intrusion à des fins géopolitiques) ou l'ingénierie sociale (intrusion à partir de l'exploitation de la nature humaine) pour mieux cibler les dirigeants afin de les rançonner. En d'autres termes, seule la cible est possiblement non définie lorsqu'il s'agit d'attaques de rançon, bien que l'entreprise, en tant que telle, soit la cible privilégiée.

Toutes les entreprises, indépendamment de leur taille, organisation, activité, statut, etc. peuvent être confrontées à ces cyberattaques. Certes, on a observé, depuis 2019, un nombre croissant de cyberattaques visant à rançonner les grandes entreprises[14] mais les PME et les TPE ne sont pas à l'abri de telles attaques, loin s'en faut.

En fait, la cible des cyberattaques ne se dégage ou n'apparaît qu'après une cyberattaque à grande échelle (campagne de masse). D'une manière générale, la démarche des cybercriminels est de diffuser un message qui atteindra le plus grand nombre possible de personnes sans tenir compte des activités, des marchés ou des tailles d'entreprise. Enfin, l'attaque d'un cybercriminel ne protège pas des autres attaques et cybermenaces. Il peut y avoir de multiples atteintes de manière synchrone, y compris par négligence interne.

b) Les cybermenaces ne sont pas identifiables

• Les cybermenaces ne sont pas identifiables dans leur nature et dans le temps

Les cyberattaques peuvent être frontales (cyberattaques constatées) mais elles peuvent aussi être invisibles (intrusions non détectées). Elles peuvent survenir sur des éléments compromis dans la chaîne d'approvisionnement (plus de 40 % des cyberattaques ciblent celle-ci)[15] ou sur les fonctions support externalisées de l'entreprise. Par exemple, un prestataire, qui se voit confier la gestion de la climatisation d'une usine, devra se connecter sur le réseau de cette usine et pourra être un point d'entrée pour les hackers afin d'attaquer le donneur d'ordre ou le sous-traitant.

Elles peuvent aussi survenir du fait d'une inadaptation concurrentielle de l'entreprise aux plans technologique ou juridique. Ainsi, un sous-traitant qui ne se serait pas mis en conformité avec le RGPD pourra être à l'origine d'une fuite de données ou de la violation du secret des affaires, ce qui constitue un point de départ pour une menace de fraude de la part des cybercriminels.

Enfin, les cyberattaques ne sont pas identifiables dans le temps ; elles peuvent ainsi être le fruit d'attaques éclairs exploitant des failles de sécurité des systèmes dès leur identification par les cybercriminels. Elles peuvent aussi être le résultat d'intrusions de longue date, dormantes et prêtes à être activées pour générer, à un moment donné, des dégâts de plus grande ampleur. En effet, 30 % des problèmes cyber ne sont pas couverts dans les entreprises par les solutions classiques[16]. Les victimes d'attaque n'en sont pas forcément conscientes.

[14] 2020 Global CrowdStrike Threat Report, CrowdStrike Intelligence.
[15] "Responsables de la Supply Chain : saurez-vous identifier votre maillon faible ?", Accenture, 2017.
[16] Propos tenus par Alain Bouillé, Directeur du CESIN, Présentation du 5ème baromètre du CESIN, 11 mars 2020.

• Les cybermenaces ne sont pas identifiables par la provenance du cybercriminel

Il n'est pas davantage possible d'identifier la provenance géographique des cyberattaques. Reposant sur l'interconnexion des systèmes d'information et Internet en particulier, les frontières et les spécificités juridiques ne sont, en effet, plus respectées même au sein d'une même entreprise lorsqu'elle est implantée sur plusieurs zones géographiques. Par conséquent, la localisation des cyberattaquants est extrêmement difficile. Elle peut, cependant, être effectuée avec les cybercriminels les moins talentueux ou nécessite de déployer des moyens beaucoup plus importants. Il est aussi possible de pister les adresses IP. En 2018, 35 % des cyberattaques recensées étaient associées à des adresses IP situées aux États-Unis et en Chine, 6 % au Japon et 5 % en France[17].

• Les cybermenaces ne sont pas identifiables par le profil du cybercriminel

Les outils des hackers criminels sont, de plus, impersonnels : hameçonnage (*phishing*), logiciels rançonneurs (*ransonware*), vol de mot de passe, logiciels malveillants, faux sites Internet, etc. Si « *les cybercriminels affûtent leur capacité à rester incognito à l'intérieur des entreprises dans lesquelles ils se sont introduits et font évoluer leurs attaques pour contrer les efforts de riposte* »[18], le panel des cybercriminels est à l'échelle du phénomène et recouvre les réalités les plus diverses.

Cela peut aller du parent d'élève mécontent qui va lancer un envoi massif de messages à une adresse mail (*mailbombing*) sur une boîte électronique d'un enseignant, d'un déni de service sur le site d'une école, jusqu'à un État qui infiltre les opérateurs de services essentiels d'un autre État. Ainsi, les pirates africains, comparables aux pirates d'antan, ont des méthodes rudimentaires reposant essentiellement sur l'ingénierie sociale alors que les hackers russes sont spécialisés dans la haute technologie et le codage digne des meilleurs films d'espionnage.

Pour tout individu ayant un accès à l'Internet caché (*Darknet*), il est également possible d'acheter des attaques pour 100 $ telles que les attaques par déni de service (DDoS)[19] ou de souscrire pour environ 50 $ un abonnement à un logiciel rançonneur dans l'économie parallèle (*Ransomware as a Service* ou RaaS)[20] qui va lui permettre d'attaquer les entreprises de son choix.

Les autres profils qui travaillent en réseau sont, quant à eux, structurés et suivent des logiques organisationnelles et des méthodes très précises.

Profil des cybercriminels

Source : Institut Montaigne, Cybermenace – avis de tempête
Compléments CCI France en bleu

[17] 2019 Global Threat Intelligence Report – GTIR, NTT Security,
[18] Carbon Black, Quarterly Incident Response Threat Report (QIRTR), Quarter 2, 2018.
[19] Ces attaques visent à empêcher l'accès à un service (site, web application, etc.) par les utilisateurs légitimes et engendrer ainsi une perte d'activité pour l'entreprise.
[20] Pour mieux comprendre le phénomène : « Ransomware-as-a-Service (RaaS) : une activité illicite qui a désormais pignon sur rue », Vade Secure, 19 mars 2020.

B) UN IMPACT CROISSANT SUR L'ENTREPRISE, SES RESSOURCES ET SON ACTIVITÉ

1) Les entreprises confrontées aux cyberattaques

a) La perception du cyber-risque par les entreprises

Le risque de cyberattaque est devenu, ces dernières années, l'une des préoccupations majeures du monde contemporain. Ce cyber-risque est passé, en 2020, en tête des principaux risques selon les entreprises françaises[21] comme le montre le tableau ci-dessous qui intègre aussi, au titre de ce risque, les conséquences des cyberattaques (atteinte à la réputation, interruption d'activité, vol, fraude, etc.).

La prise en compte de ces conséquences peut expliquer pourquoi il est aujourd'hui au premier rang mais aussi illustrer une évolution vers une meilleure perception par les entreprises car les faits montrent effectivement un nombre croissant d'entreprises faisant l'objet de cyberattaques ainsi qu'un impact croissant sur les ressources, l'activité voire la performance de l'entreprise.

Les dix principaux risques selon les entreprises françaises

Classement	Risque	Pourcentage	Classement 2018	Tendance
1	Incidents cyber (ex : cyber crimes, défaillances informatiques, violations de données…)	41 %	2	Hausse
2	Interruptions d'activités (y compris les perturbations de la chaîne logistique)	40 %	1	Baisse
3	Incendies, explosions	29 %	3	Stable
4	Catastrophes naturelles (ex : tempêtes, inondations, tremblement de terre)	28 %	4	Stable
5	Évolutions législatives et réglementaires (ex : changement de gouvernement, sanctions économiques, protectionnisme, Brexit, désintégration de la zone Euro…)	26 %	4	Baisse
6	Évolutions de marché (ex : volatilité, concurrence accrue, nouveaux entrants, fusions/acquisitions, fluctuations de marchés)	18 %	6	Stable
7	Nouvelles technologies (ex : impact de l'interconnectivité, nanotechnologies, intelligence artificielle, impression 3D, blockchain, etc.)	18 %	8	Hausse
8	Atteinte à la réputation ou à l'image de marque	12 %	9	Hausse
9	Défaillance de qualité, défaut de série, rappel de produits	12 %	7	Baisse
10	Vol, fraude et corruption	10 %	9	Baisse

Source : Allianz Global Corporate & Specialty

Note : les chiffres représentent un pourcentage de toutes les réponses (participants : 86 ; réponses : 106). Plus d'un risque et plus d'une industrie pouvaient être sélectionnés. Les chiffres ne totalisent pas 100 % car trois risques pouvaient être sélectionnés

[21] Baromètre des risques 2020, Allianz Global Corporate & Specialty, 14 janvier 2020.

b) De plus en plus d'entreprises font l'objet de cyberattaques

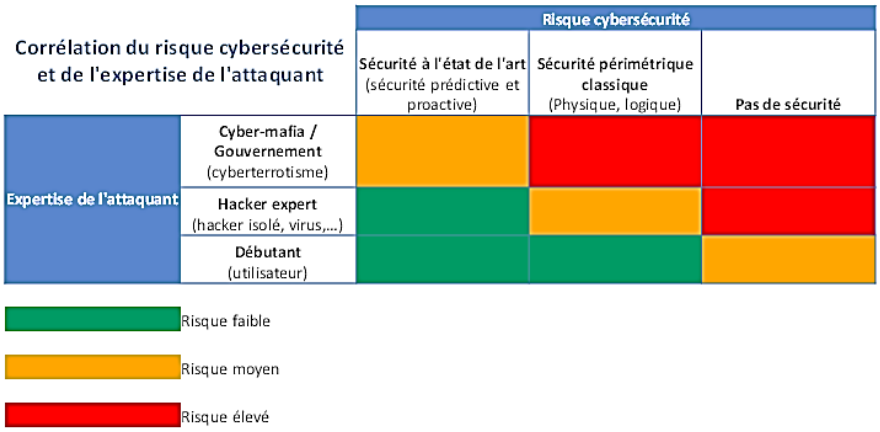
Si les trois quarts des grandes entreprises ont été la cible de cyberattaques, un peu moins de la moitié des TPE et PME se déclarent affectées. Cela s'explique notamment par le fait que les TPE-PME n'ont pas conscience des tentatives d'attaque ou des attaques avortées à leur encontre mais aussi par le fait que les TPE de l'artisanat ne disposent pas de ressources connectées parce qu'elles en ont moins besoin.

Quand elles ont un Responsable de la sécurité des systèmes d'information (RSSI), les entreprises ont une meilleure conscience des attaques : ainsi, 80 % des entreprises françaises en ayant un ont déjà constaté une cyberattaque[22].

Au-delà du nombre d'entreprises qui font l'objet de cyberattaques, c'est la fréquence des attaques sur une seule entreprise qui est marquante : 10 % des répondants au baromètre du Club des experts de la sécurité de l'information et du numérique (CESIN) disent subir 15 cyberattaques pas an[23].

L'impact sur l'entreprise est, enfin, étroitement corrélé à l'expertise du cyberattaquant et du niveau de maturité de l'entité attaquée. On voit sur le schéma ci-dessous que plus le niveau de maturité cyber de l'entreprise ou de l'institution est élevé, plus il faut une expertise technique au hacker pour atteindre son but. Inversement, une piètre préparation de la cible facilite la tâche du hacker.

Corrélation du risque de cybersécurité et de l'expertise de l'attaquant



Source : La loi de programmation militaire, un cadre juridique de la politique de cyber défense nationale française, 2015, CIO Advisory by SIA Partners

Source : « La loi de programmation militaire, un cadre juridique de la politique de cyber défense nationale française », CIO Advisory by SIA Partners, 2015

c) Un coût de plus en plus élevé

Le coût moyen des cyberattaques est évidemment exorbitant pour les TPE/PME. Si une attaque peut générer, pour le cybercriminel, un bénéfice compris entre 30 000 € et 50 000 €, elle peut coûter entre 10 000 € et 100 000 € pour une entreprise. Chiffre nettement plus alarmant, 70 % des PME qui subissent une attaque déposent le bilan.

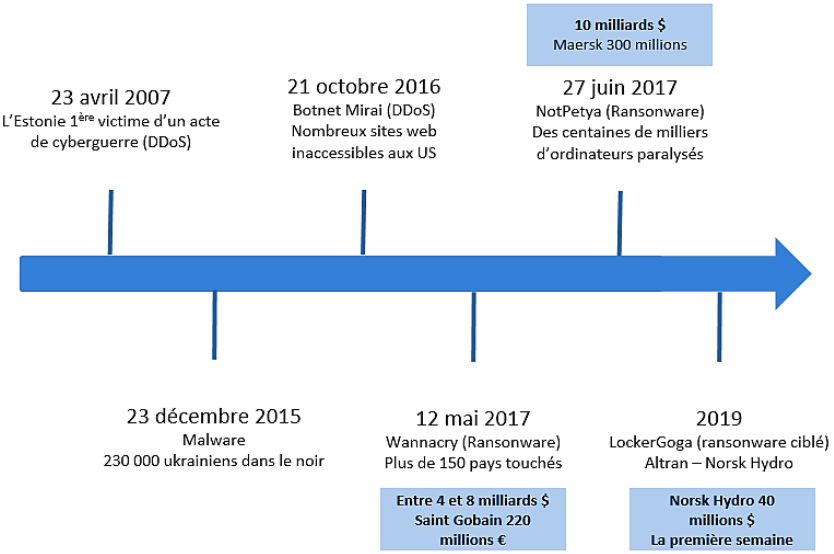
Véronique PLESSIER CHAUVEAU
EULEOS

« Toutes les entreprises savent ce qu'il faut faire mais peu le font »

Les chiffres deviennent vertigineux lorsqu'il s'agit de grandes entreprises : Saint-Gobain a perdu jusqu'à 220 millions € de son chiffre d'affaires[24] après avoir subi l'attaque du *ransomware* NotPetya en juin 2017.

[22] 5ème édition du Baromètre annuel du Cesin, Analyse exclusive de la cybersécurité des grandes entreprises françaises, 2020.
[23] Ibid.
[24] « Saint-Gobain évalue à 250 M€ les dégâts liés à l'attaque NotPetya », 1er août 2007, LeMondeInformatique.fr.

Cyberattaques marquantes incitant à la prise de conscience



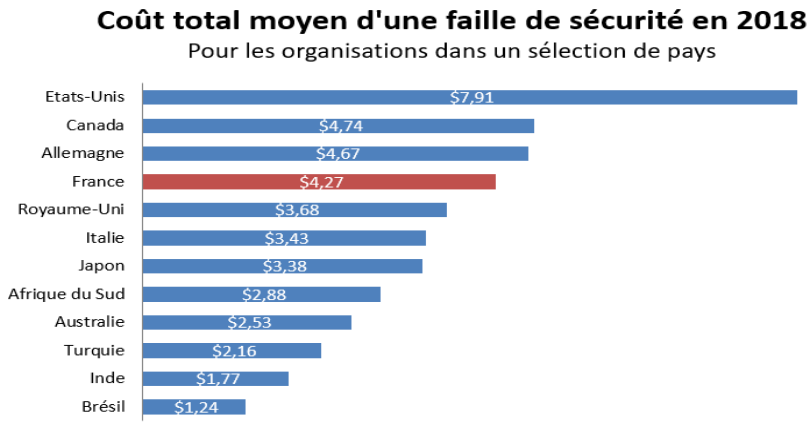
Certaines études estiment ce coût jusqu'à 97 000 € par entreprise compromise en 2019, soit une doublement en un an[25]. En outre, l'impact financier d'une cyberattaque peut durer sur plusieurs moins ou années.

Il faut aussi compter avec la perte de valorisation boursière pour les entreprises cotées : 63 % des sociétés ayant connu un incident entre 2008 et 2017 ont vu « *leur valeur boursière affectée avec, en moyenne, plus d'un an après l'incident, une perte de la valeur patrimoniale de 10 %, et même de 20 % pour les entreprises les moins réactives et les moins bien préparées (ce qui représentaient 40 % de l'échantillon), qui se retrouvaient donc « affaiblies structurellement* »[26].

On voit sur le graphique ci-dessous que les coûts moyens sont nettement plus importants dans les pays développés qui ont fait émerger de véritables écosystèmes d'entreprise. D'une part, les mises en réseau entre donneurs d'ordre et sous-traitants peuvent entraîner des coûts supplémentaires en cas d'attaque. D'autre part, ce sont les pays à forte création de valeur dans l'économie de l'immatériel qui subissent les coûts les plus importants.

Coût moyen total d'une faille de sécurité (millions $)

(pour les organisations dans une sélection de pays)



Source : IBM Security - Ponemon Institute, « Vol de données personnelles -*Le coût des failles de sécurité », Statista, 16 juillet 2018*

[25] Cyberattaque : quel coût pour une TPE/PME ? Hiscox Assurances, 1er août 2019.
[26] Selon une étude PwC France citée in : Guy-Philippe Goldstein & Philippe Trouchaud, « La valeur de l'entreprise à l'épreuve des cyber-attaques », HBR France, 9 mai 2018.

Au-delà du coût des cyberattaques, c'est aussi l'impact sur l'activité, la performance et les ressources de l'entreprise qu'il faut observer.

2) L'impact sur l'activité, la performance et les ressources

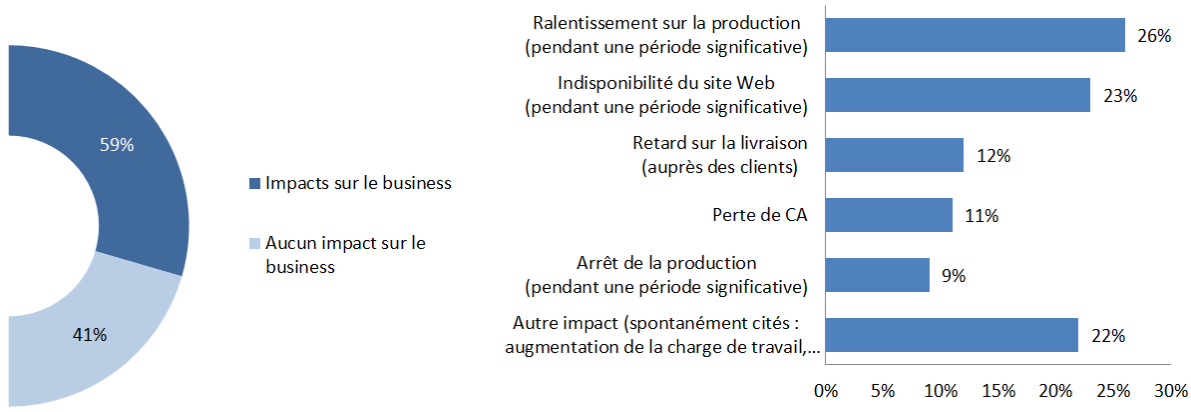
S'agissant des activités et de la performance de l'entreprise, on observe un impact important des cyberattaques sur la production et le site web. L'impact est plus modéré sur la distribution/livraison et le chiffre d'affaires.

Le CESIN note que 59 % des entreprises ont constaté un impact des cyberattaques sur l'activité de l'entreprise, notamment par un ralentissement de la production (26 %) ou même un arrêt (9 %). Certaines entreprises enregistrent même plusieurs impacts sur différents postes pour une ou plusieurs cyberattaques, confirmant ainsi le caractère tentaculaire et imprévisible des cybermenaces.

Dans les cas de *ransomware*, de déni de service, etc. qui conduisent au blocage des systèmes, les ressources et fonctions de l'entreprise peuvent être neutralisées ; mais, avec une sauvegarde, elles peuvent être restaurées facilement. Dans les cas d'ingénierie sociale (*phishing*, arnaque au président, usurpation d'identité), les pertes en flux monétaire peuvent être importantes mais les services informatiques ne sont compromis.

Dans les deux cas, ces attaques entraînent un surcroît de travail considérable sur un ensemble de postes comme le montre la figure ci-dessous.

Impact des cyberattaques sur les activités de l'entreprise



Source : 5ème baromètre du Cesin, 2020

Le même baromètre du CESIN montre également des impacts (spontanément cités par les RSSI) qui portent sur les ressources non technologiques comme l'augmentation de la charge de travail des collaborateurs et les ressources humaines (RH). On peut donc parler d'impacts croisés sur l'entreprise en cas de cyberattaque ; la quantification dépend de la préparation, de la formation et de la personnalité même des collaborateurs et, avant tout, du dirigeant de l'entreprise.

Les conséquences des cyberattaques sont aussi souvent inconnues et négligées. La métaphore de l'iceberg illustre tout-à-fait les implications cachées d'une cyberattaque qui possède, à la fois, une face éclairée et une face cachée voire sombre.

Impact d'une cyberattaque : partie émergée et partie immergée

PARTIE ÉMERGÉE Coûts financiers les plus connus	Enquêtes techniques
	Notification client d'intrusion
	Mise en conformité réglementaire
	Horaires d'avocat et frais de justice
	Sécurisation des données « post-incident »
	Relations publiques
	Amélioration des dispositifs de cybersécurité
PARTIE IMMERGÉE Coûts financiers cachés ou moins visibles	Augmentation des primes d'assurance
	Augmentation des coûts de la dette
	Impacts liés à la perturbation ou à l'interruption des activités
	Érosion du chiffre d'affaires liée à la perte de contrats clients
	Dépréciation de la valeur de la marque
	Perte de propriété intellectuelle
	Perte de la confiance accordée par le client

Source : Tableau réalisé à partir de "Beneath the surface of a cyberattack - A deeper look at business impacts", Deloitte, 2016

En cas d'attaque, les entreprises naviguent généralement à vue car elles isolent des systèmes informatiques les fonctions qui sont compromises. Il est, cependant, possible d'observer l'impact sur les fonctions principales des entreprises.

On voit sur le schéma ci-dessous que les cyberattaques portent sur les différentes fonctions de l'entreprise sans en épargner une seule. On observe une tendance plus marquée vers les attaques de sites web, quelle que soit la zone géographique dont l'attaque est originaire. Notons aussi que les fonctions génératrices de valeur (finance et technologie) sont en ligne de mire des cyberattaquants.

Catégorie de cyberattaques : par secteur, par type et par origine

Secteur	Attaques types	Sources types
Finance 17%	Attaques Web 46% Attaques de service spécifique 28% DoS/DDoS 8%	Etats-Unis 42% Chine 8% Grande-Bretagne 6%
Technologies 17%	Identification 20% Brute-Force Attacks 17% Source non certifiée 14%	Chine 37% Etat-Unis 21% Russie 5%
Commerce et B2B 12%	Attaques Web 42% Dos/Ddos 20% Source non certifiée 15%	Etats-Unis 26% Chine 15% France 10%
Education 11%	Brute-Force Attacks 47% Attaques Web 18% Identification 16%	Etats-Unis 25% Pays-Bas 16% Vietnam 15%
Administration 9%	Attaque de Service spécifique 27% Identification 21% Dos/DDoS 16%	Etats-Unis 37% Allemagne 14% France 13%

Source : 2019 Global Threat Intelligence Report - GTIR, NTT Security
DOS : Denial of Service ; DDoS : Distributed Denial of Service

Enfin, l'on voit que les familles d'attaque, ici définies par l'ANSSI *(Tableau Infra)* ne sont pas homogènes quant aux moyens et aux impacts sur l'entreprise. Il est, d'ailleurs, notable que les attaques les plus fréquentes ne sont pas obligatoirement celles qui occasionnent un coût élevé pour l'entreprise. Les cyberatteintes à l'entreprise les plus fréquentes et ayant l'impact le plus important sont des attaques reposant sur une réponse humaine à une sollicitation malveillante, soit pour ouvrir une faille, soit pour permettre le crime. Il est donc difficile de définir des stratégies par destination pour parer ces attaques, quelle que soit leur nature.

On comprend alors que si toute entreprise est une cible potentielle de cyberattaques, les répercussions dépendent de sa capacité de réponse. Pour toutes ces raisons, il est indispensable de circonscrire, avant tout, le cyber-risque par le bouclier de la cybersécurité (Partie I) pour passer, ensuite, à une posture de résilience (Partie II) qui pourra constituer, à terme, un avantage comparatif, voire un levier de transformation de l'entreprise. Reste que l'exercice n'est évidemment pas un long fleuve tranquille : toutes les actions et mesures qui pourront faciliter ce cheminement de l'entreprise sont les bienvenues (Propositions).

Familles de cyberattaques et leurs impacts sur l'entreprise

			de 1 à 4*	de 1 à 4*	de 1 à 4*	en M$	en € ou en $
Famille	Risque	Perte/ blocage	Impact en cas de survenance	Fréquence de survenance	Degré de compromission des SI	Coût moyen pour l'entreprise (monde)	Coût moyen pour l'entreprise (FR)
Atteinte à l'image	Déni de Service Abus de privilège	Blocage	4	2	2	1,7	154 323 € par entreprise (550 millions €/toutes entreprises)
Cybercriminalité	Ransomware	Blocage	2	3	1	0,7	Entre 12 750 € et 286 500 €
	Botnets	Blocage	1	1,5	2	0,4	-
	Ingénierie sociale	Perte/ blocage	4	1,5	1	1,4	Entre 10 000 $ et 100 millions $
	Phishing, SPAM, Fraude au Président	Perte	4	4	1	-	Entre 100 000 € et 2 millions €
Espionnage	Malware	Perte/ blocage	4	4	4	2,6	38 000 €
	Web Application Attacks	Perte	3	2	4	2,3	-
	Spear-Phishing	Perte/ blocage	4	4	1	-	Jusqu'à 7 220 930 €
	Scripts et fichiers PE exécutables	Perte	2	2	3	1,4	-
	Chevaux de Troie téléchargeurs Adware	Perte	4	1	3	1,6	-
Sabotage	Blocage de l'architecture réseau, Failles d'exploitation et packs d'exploitation	Blocage	2	2	4	-	-
	Dégâts physiques Vols, perte	Perte	4	1	2	1	-

* 1 correspond à l'impact, la fréquence ou le degré le moins élevé et 4 au plus élevé

Sources : « cyberattaques les plus courantes », Baromètre CESIN - The Cost Of Cybercrim, Ninth Annual Of Cybercrime Study Unlocking The Value Of Improved Cybersecurity Protection, Institut Ponemon - Accenture 2019 - Kapersky - lemondeinformatique.com - Chekpoint - Cybercover - Journal du Net

PARTIE 1

LA CYBERSÉCURITÉ : LA SÉCURITÉ CONSTRUITE À PARTIR D'UNE DÉMARCHE DÉFENSIVE ET RÉACTIVE

Dans une posture de cyberrésilience[27], un premier passage obligé est la cybersécurité. Celle-ci pose les jalons d'une continuité d'activité en cas d'attaque ; sans elle, il ne peut y avoir de résilience. Elle est un peu à l'image d'un accident cardio-vasculaire : les mesures de prévention sont indispensables à la santé et à la pérennité de l'entreprise mais ne peuvent empêcher l'attaque ni même restaurer la situation antérieure ; la sphère de la cybersécurité entraîne donc l'entreprise dans un état de maintien grâce aux mesures réactives.

A) LA CYBERSÉCURITÉ : UNE BOÎTE À OUTILS POUR PROTÉGER LES SYSTÈMES ET LES DONNÉES

La cybersécurité est *« la combinaison de personnes, de politiques, de processus et de technologies employés par une entreprise pour protéger ses cyber-actifs »*.[28] C'est une stratégie définie au niveau des chefs d'entreprise pour équilibrer les ressources en vue de protéger les données et les systèmes d'information (ergonomie, capacité de gestion et quantité de risques afférents).

1) Où commence et où finit la cybersécurité ?

Le champ de la cybersécurité couvre notamment la sécurité des systèmes d'information (SSI), des objets connectés (IoT), des services d'information (qui relève de la DSI) et des technologies d'exploitation (OT). Ces composantes, qui relèvent de la technologie et de la politique de sécurité, sont gérées selon les protocoles en vigueur. Il en résulte que la cybersécurité est souvent considérée comme un système "automate" : elle passe par la mise en place de procédures de sécurité basées sur des algorithmes de réponse qui sont non exhaustifs et statiques. Or, cette première approche se heurte à deux écueils.

Premier écueil : un processus d'automatisation est toujours porteur d'espoirs mais aussi de craintes ; on le voit aujourd'hui avec l'industrie 4.0 où les systèmes cyberphysiques[29] permettent la traçabilité, la reconfiguration en temps réel des chaînes de production… mais représentent aussi des sources de faille supplémentaires en matière de cybersécurité.

Certes, le *machine learning* ou apprentissage automatique (technologie d'intelligence artificielle permettant aux ordinateurs d'apprendre sans avoir été programmés explicitement à cet effet)[30] fait que les systèmes d'information peuvent être adaptés aux comportements des utilisateurs et enrichis en temps réel par des expériences tierces.

Second écueil : la réponse à la cybermenace demande une agilité et une adaptabilité constantes et durables compte tenu de la montée en puissance des attaques. Or, la cybersécurité est vue comme un moyen de protéger des attaques, c'est-à-dire de circonscrire le système d'information pour éviter des attaques. L'image représentative de cette approche serait celle d'un bâtiment clos et hermétique où chaque entrée serait verrouillée et où les failles seraient le fruit de la négligence des utilisateurs. C'est là une vision relativement étroite et rigide de la cybersécurité.

Par conséquent, une autre approche de la cybersécurité consiste à contrer les attaques, c'est-à-dire à penser le système d'information comme devant contrecarrer les attaques. L'image représentative de cette approche serait

[27] La Cyberrésilience sera entendue dans cette étude comme « une posture, une stratégie et une organisation visant à absorber les cyberattaques en minimisant les pertes pour l'entreprise tout en poursuivant l'activité et en transformant l'entreprise. Elle vise principalement à protéger l'activité de l'entreprise. » Le périmètre et la définition seront développés ultérieurement au cours de cette étude.
[28] Pour paraphraser ici la définition donnée par Gartner in : "Information Technology", Gartner Glossary.
[29] Cyber Physical System ou CPS.
[30] "Machine Learning et Big Data : définition et explications", Big Data Magazine, 6 juillet 2018.

celle d'une pieuvre qui renvoie toutes les attaques qui lui sont lancées par des réactions adaptées à chaque menace. C'est là une vision plus ouverte et évolutive de la cybersécurité.

En réalité, une approche idéale ou plus complète de la cybersécurité consisterait à combiner les deux visions. C'est, d'ailleurs, vers cela que tendent les solutions actuelles dont l'esprit est de refermer, une à une, toutes les portes des systèmes pour protéger des attaques.

In fine, la cybersécurité peut être entendue comme la mise en œuvre des moyens techniques pour protéger les systèmes d'information, ces derniers étant alimentés par les outils juridiques qui servent à définir les normes en la matière. Dans cette course à la "bonne sécurité", le bon élève est l'entreprise qui tire parti de la mise en place et de la configuration optimale des outils technologiques pour aller plus loin que les normes.

C'est ce niveau plus avancé de protection qui fait entrer l'entreprise dans la cyberrésilience pour lui permettre d'assurer et de pérenniser l'activité alors que dans la cybersécurité, celle-ci se contente d'une configuration stable destinée à simplement protéger le système d'information et les données.

2) Quelques "cyber-idées" reçues

Quelques idées persistent dans l'imaginaire des chefs d'entreprise et des collaborateurs en matière cyber. Pourtant, la réalité est souvent moins tranchée ; ces idées reçues méritent d'être clarifiées.

• n° 1 : mon portable à usage strictement personnel est coupé de mon activité professionnelle

La plupart du temps, les smartphones se connectent sur les réseaux WIFI des entreprises et, parfois, sur les « parties dédiées » aux employés. Le bornage GSM permet de localiser son utilisateur dans l'entreprise et peut l'identifier comme une proie en ingénierie sociale. Aussi, pour permettre de conserver son smartphone non contaminé, convient-il de privilégier les réseaux WIFI sécurisés, pour des utilisations professionnelles comme personnelles, d'effectuer les mises à jour de sécurité et d'utiliser des solutions de sécurisation VPN, *firewall*, antivirus, etc.

• n° 2 : les hackers choisissent leurs victimes

La plupart des hackers procèdent par des scans de ports réseaux pour détecter les réseaux d'entreprise qui présenteraient des failles. Ils vont, ensuite, choisir des entreprises parce qu'elles leur offrent la possibilité de rentrer dans leur système. Cependant, certaines entreprises sont ciblées pour des raisons d'espionnage industriel ou bien sont identifiées comme ayant des ressources et une potentialité de payer des rançons.

• n° 3 : la menace vient de l'extérieur

Les hackers procèdent souvent à distance en effectuant des scans pour identifier des failles ou s'attaques aux serveurs distants pour bloquer l'activité des sites Internet. À noter que les utilisateurs internes sont souvent ceux qui laissent les brèches ouvertes pour de potentielles intrusions et ce sont eux qui laissent les indices et le matériel indispensables à une ingénierie sociale.

• n° 4 : il suffit d'installer un logiciel de sécurité pour être protégé

Une bonne configuration des logiciels de sécurité et leur mise à jour couvrent la plupart des risques d'attaque mais pas les plus fatals. Il existe toujours des failles non-découvertes par les éditeurs de logiciels qui rendent les sites et les systèmes fragiles.

• n° 5 : il faut faire la police auprès des collaborateurs

Les collaborateurs sont des vecteurs d'intrusion lorsque les comportements de sécurité ne sont pas intégrés par l'utilisateur ; il est alors nécessaire de restreindre les accès et les droits des utilisateurs. Pour limiter cela, une bonne campagne de sensibilisation permet de diminuer drastiquement la fragilisation par les utilisateurs ; une culture de la cybersécurité permet aussi une autorégulation des comportements qui finissent par être intégrés par les collaborateurs.

• n° 6 : une sauvegarde hebdomadaire permet de retrouver les données

Une sauvegarde hebdomadaire permet de récupérer des entrepôts de données avec une antériorité suffisante. Il faut, cependant, prendre garde aux périodes de suractivité qui peuvent nécessiter des sauvegardes plus rappro-

chées dans le temps. Dans l'idéal, plusieurs strates de sauvegarde sont conseillées : 1/ une sauvegarde du système à une date de confiance dans le risque de contamination du système, 2/ une sauvegarde hebdomadaire et 3/ une sauvegarde journalière (mode connexion / déconnexion utilisateur). Il ne faut pas hésiter à dissocier les supports de sauvegarde en fonction de la sensibilité des données et des fonctions de l'entreprise[31].

B) LES OUTILS QUI ENTRENT DANS LE CHAMP DE LA CYBERSÉCURITÉ

1) Les outils juridiques

a) RGPD et cybersécurité

Depuis le 25 mai 2018, toutes les entreprises sont concernées par le Règlement européen sur la protection des données personnelles (RGPD) dès lors qu'elles « traitent » (collectent, enregistrent, conservent...) des données personnelles. Celui-ci impose aux entreprises de mettre en place des mesures efficaces pour sécuriser ces données.

Cela s'impose notamment en cas de « *faille de sécurité, des données traitées ou stockées permettant d'identifier une personne physique (salarié, client, prospect, fournisseur...), qui ont pu faire l'objet d'une destruction, d'une altération ou, le plus souvent, d'une communication à un tiers non autorisé (un hacker, un concurrent...)*[32] ».

Pour sécuriser les données, le RGPD rappelle aux entreprises qu'elles doivent s'appuyer sur diverses opérations principalement technologiques (chiffrement des données et connexions, authentification plus forte, accès facilité aux données stockées en cas d'incident physique ou technique, évaluation de la performance des mesures techniques et organisationnelles de sécurisation des traitements, vision globale du système informatique, etc.).

Pour se mettre en conformité, les entreprises peuvent aussi recourir à des prestataires extérieurs qui proposent, via le cloud, d'externaliser et d'automatiser les processus d'application du cadre légal en vigueur ; c'est ce qu'on appelle la conformité comme un service (*Compliance as a Service)*[33].

b) Certification AFNOR et cybersécurité

La certification AFAQ ISO/IEC 27001 vient valider la mise en place d'un Système de management de la sécurité de l'information (SMSI).

Cette certification est construite sur la base de la norme internationale de référence ISO 27001. Elle définit une méthodologie pour identifier les cybermenaces, maîtriser les risques associés aux informations cruciales des entreprises et organisations, mettre en place les mesures de protection appropriées afin d'assurer la confidentialité, la disponibilité et l'intégrité de l'information[34].

En affichant la certification AFAQ ISO 27001, les entreprises peuvent ainsi montrer « *patte blanche partout dans le monde* » pour reprendre ici les termes de l'AFNOR. Dès lors, la certification apparaît comme un atout dans la définition de la stratégie de l'entreprise en matière de sécurité. Selon l'AFNOR, cette norme permet notamment de :

• identifier les menaces et les dangers pesant sur le système d'information d'une entreprise ;

• mobiliser les équipes autour d'un projet commun ;

• améliorer les pratiques pour sécuriser le système d'information ;

• maîtriser les coûts liés à la sécurité et à la cybersécurité ;

• pérenniser l'activité de l'entreprise ;

• accroître la confiance des clients et répondre à leurs exigences en matière de sécurité.

[31] « 8 conseils pour éviter une cyberattaque », Stratégies, 21 novembre 2018.
[32] RGPD - Le comprendre et l'appliquer, Chambre de commerce et d'industrie de Paris Île-de-France, septembre 2018, https://www.cci-paris-idf.fr/sites/default/files/etudes/pdf/documents/guide-rgpd.pdf
[33] Service dans le cloud permettant aux entreprises d'externaliser et d'automatiser les processus d'application du cadre légal en vigueur.
[34] Certification ISO 27001, Afnor Certification, https://certification.afnor.org/numerique/certification-iso-27001

c) La certification de CCI France «Référent cybersécurité en TPE/PME» en CCI.

CCI France a créé en 2018 le réseau de formation «Initiative Data Compétences». Ces formations interviennent dans le cadre des certifications enregistrées par la Commission Nationale de la Certification Professionnelle. Elles couvrent des compétences transverses répondant aux besoins de montée en compétences des salariés de TPE-PME.

La certification «Référent cybersécurité en TPE/PME». Déposée avec l'appui de l'ANSSI et de la DGE-SISSE, elle atteste des compétences de maîtrise des enjeux et outils de la cybersécurité dans l'entreprise, permettant ainsi aux TPE/PME de se doter d'un véritable «sauveteur secouriste cybersécurité».

Cette certification est complétée par les certifications «Mettre en œuvre le RGPD en TPE/PME» et «Devenir délégué à la protection des données (DPO) en TPE/PME». Avec le RGPD, une entreprise ou une organisation a besoin d'un véritable «chef d'orchestre» pour piloter la gouvernance des données personnelles et la conformité RGPD.

Les formations spécifiques de référents cybersécurité des CCI pour intervenir en PME/TPE, de mise en œuvre du RGPD et de DPO sont dispensées par les CCI et leurs centres de formations.

Dès lors, avec ces éléments, on commence à entrer dans la cyberrésilience.

2) Les outils technologiques

a) La mise à niveau des systèmes

La première étape de la cybersécurité est une phase de mise à niveau ou de « calibrage » des dispositifs de sécurité informatique. En cas de cyberattaque, il faut donc adapter les barrières pour retarder et minimiser les attaques des cybercriminels en s'appuyant sur des configurations avancées, normes et certifications.

C'est précisément cette posture qui permet de se protéger des intrusions et des vols de données. En effet, il ne suffit pas d'installer une solution logicielle pour compliquer le travail de cybercriminels. Il faut accompagner l'évolution et la mise en œuvre des solutions informatiques en suivant quelques recommandations de base[35] :

Joël THIERY
COREFIM

« Il y a une vraie pertinence à réaliser des tests d'intrusion et à sensibiliser le plus largement possible les collaborateurs non spécialisés par l'intermédiaire des MOOC, dont ceux qui sont réalisés et mis en ligne par l'ANSSI. »

- reconfigurer les identifiants par défaut ;
- ne pas retarder la mise à jour des logiciels ;
- ne pas appliquer les mêmes mots de passe sur différents périphériques ;
- faire attention à la mauvaise configuration des interfaces à distance ;
- enregistrer quotidiennement l'activité des systèmes d'information et identifier les intrusions qui offrent la fameuse « cape d'invisibilité » des hackers.

Par ces diverses actions sur la technologie, on voit apparaître une variable non-automatisable et non-prévisible par les cybercriminels qui est l'humain. Lorsqu'on observe l'origine des cyberattaques sur les entreprises, la dimension purement technologique, sans intervention d'un utilisateur, est mineure.

b) La bonne configuration des systèmes

La mise à jour est une action-clé pour se protéger en matière de cybersécurité : elle doit porter sur les éléments traditionnels (logiciel et matériel), mais également normatifs (certifications, conformité à la législation) et humains (mise à niveau des compétences).

Cependant, il ne faut pas se limiter à une mise à jour logicielle ou des logiciels internes des outils TI (Technologies de l'information). Il ne suffit pas non plus d'installer des systèmes, il faut aussi une bonne configuration pour les adapter aux exigences de sécurité et à l'activité de l'entreprise.

[35] « Les options de configuration : la boîte de Pandore des cybercriminels », Undernews, 7 avril 2020.

Il est, en effet, indispensable de se doter d'une activité de contrôle sur les mises à jour, savoirs et pratiques des utilisateurs et performance des systèmes : configuration, autorisation d'accès, architecture réseaux...

Marc-Henri BOYDRON
CYBERCOVER

« Il faut s'interroger afin de savoir si les standards relatifs à une bonne hygiène informatique sont respectés (mises à jour, sauvegarde, sensibilisation, etc.). L'entreprise peut avoir la solution mais cette dernière peut parfois être mal voire insuffisamment déployée. »

Lors de la passation ou du renouvellement de contrat avec un apporteur de solutions (courtier d'assurance cyber, par exemple), il est également important que l'entreprise-cliente veille au respect de ses contraintes et exigences en matière de cybersécurité. À titre d'exemple, des porteurs de solutions ont dû revoir entièrement leur modèle d'affaires par désaffection d'un client qui exigeait les garanties qu'ils n'étaient pas en mesure de fournir lors de la négociation du contrat. Cela a eu des conséquences financières importantes en termes de chiffre d'affaires ; mais cela a eu aussi l'effet vertueux de relever les standards des solutions proposées aux entreprises.

c) La bonne composition avec des solutions systèmes : l'exemple du cloud

Les solutions traditionnelles visant à adjoindre des antivirus et des pare-feux (*firewall*) sont aujourd'hui largement déployées par les Directions des systèmes d'information (DSI) dans les entreprises et les configurations sont, désormais, maîtrisées. Mais elles montrent leurs limites face à des cyberattaques de plus en plus élaborées, intrusives et destructrices : la capacité d'intrusion des hackers sera démultipliée lorsque l'ordinateur quantique arrivera dans un avenir proche. Elles montrent également leurs limites lorsque la cybermenace n'est pas criminelle, mais le résultat d'un acte de négligence. La perte de données en est un exemple significatif.

En effet, aucun utilisateur n'est infaillible et ne peut se prétendre à l'abri d'une erreur de manipulation. Ainsi, l'utilisateur peut être à la source d'erreurs comme : la suppression accidentelle de fichiers ou de dossiers, l'écrasement involontaire de sauvegarde ou de données, les erreurs de saisie entraînant une altération des données et le reformatage involontaire de dispositifs de stockage.

Au demeurant, de nouvelles solutions se développent, via le cloud notamment. Celles-ci semblent aujourd'hui mieux répondre à la problématique de récupération de données en cas de cryptage de ces dernières. C'est ce qu'on appelle la sécurité applicative ou logicielle qui comprend :

- le DRaaS *(Disaster Recovery as a service)* : la récupération en tant que service est une catégorie de cloud utilisée pour protéger une application ou des données d'une éventuelle catastrophe (crash système, sinistre incendie, etc.) ;
- le RaaS[36] *(Resilience as a Service)* : la résilience en tant que service est une catégorie de cloud utilisée pour reconstruire un système après une attaque ;
- le BaaS *(Back-up as a Service)* : la sauvegarde en tant que service à la demande est réalisée, non sur site, mais via un cloud privé, public ou hybride géré par un prestataire.

Si les technologies semblent de plus en plus performantes, leur développement se heurte, cependant, à un critère majeur qui est celui de la confiance des entreprises dans ce type de solutions.

D'une part, la perte de contrôle physique (sur le support des données et les ressources de protection) par une migration vers le cloud donne un sentiment de perte de maîtrise. D'autre part, les plateformes américaines (GAFAM) dominent le champ commercial en matière de cloud, ce qui laisse planer un doute quant à l'utilisation des données et au respect des législations européennes et françaises (RGPD, secret des affaires, etc.). C'est la question-clef de la souveraineté numérique[37].

En matière de cloud public, il demeure aussi une suspicion de perte de données soit par des failles de sécurité au profit d'un tiers, soit par la perte de souveraineté au profit des hébergeurs en vertu des conditions générales d'utilisation (CGU). C'est une crainte légitime car on a enregistré, au cours du second semestre 2019, plus 160 milliards de documents exposés via le cloud public[38]. Ce risque peut, là encore, être réduit grâce au *Machine Learning* et à l'expertise humaine qui permettent de détecter les « fuites » de manière assez fine.

[36] À ne pas confondre avec le Raas de l'économie informelle traduit par Ransomware as a Service.
[37] À cet effet, le Cybersecurity Act, en tant qu'acte juridique européen de portée générale et devant être adapté en droit local par tous les États européens, marque une véritable avancée dans le sens de la souveraineté numérique européenne.
[38] « Comment CybelAngel détecte les fuites de données à l'extérieur du périmètre IT de l'entreprise », CybelAngel, Dossier spécial.

Tout cela explique pourquoi il existe plusieurs degrés de maturité quant à l'usage du cloud :

• le niveau 1 : le cloud vu comme une menace ;

• le niveau 2 : le cloud vu comme une opportunité ;

• le niveau 3 : le cloud non considéré comme un partenaire de confiance ;

• le niveau 4 : le cloud considéré comme un partenaire de confiance.

C) OÙ EN SONT LES ENTREPRISES DANS L'ADOPTION D'UNE POSTURE DE CYBERSÉCURITÉ ?

1) La cybersécurité reste une priorité de second rang au sein des entreprises

Si la cybersécurité est une préoccupation pour les trois quarts des entreprises (76 %)[39], le cyber-risque et les enjeux de sécurité sont encore mal appréhendés. Preuve en est : 71 % des responsables de la sécurité des systèmes d'information (RSSI) considère les cyberattaques comme « *un domaine assez opaque, et ne savent ni quand ni comment celles-ci pourraient affecter leur organisation* »[40].

Nombre d'entreprises restent dans le déni quant à l'importance et à l'impact du phénomène[41] alors que ces dommages pourraient être minimisés, dans une certaine proportion, si des politiques de cybersécurité étaient mises en place.

Yassir KAZAR
YOGOSHA

« Il reste un frein psychologique lié au « ça n'arrive qu'aux autres » qui ralentit l'effort d'investissement en matière de cybersécurité. Cela dépend aussi du niveau de maturité de départ en matière de cybersécurité »

Les capacités à prendre des risques et à gérer les priorités qui sont le propre de l'esprit d'entreprise sont, à cet égard, ambivalentes : elles peuvent conduire à négliger la mise en place de mesures fortes de cybersécurité. En outre, les dispositifs réglementaires et les outils technologiques à disposition, bien qu'ils doivent faciliter et assurer la sécurité de l'entreprise, sont souvent perçus comme des contraintes ou des outils opaques pour l'entreprise.
Cette faible considération pour la cybersécurité se traduit de deux façons : au plan budgétaire et au plan organisationnel (autour de l'expertise de protection).

a) La question budgétaire

Maxime ALAY-EDDINE
CYBERWATCH

« Le marché agit essentiellement en réaction aux attaques plutôt qu'en prévention, car les menaces sont nombreuses et difficiles à appréhender. »

Si les entreprises s'équipent en outils technologiques nécessaires à la sécurité des systèmes d'information, le budget cybersécurité ne représente encore que 5 % du budget dédié aux technologies de l'information alors que 10 % des répondants au baromètre du CESIN affirment subir 15 cyberattaques par an[42]. Il en résulte que le Responsable de la sécurité des services d'information (RSSI) est en cellule de crise permanente.

En outre, il s'agit d'un budget qui est généralement affecté à la DSI et non d'un budget à part entière. Un budget propre à la cybersécurité (avec des investissements matériels et immatériels en plus des équipes en place) permet aussi de lutter contre l'obsolescence des outils, sensibiliser/former les collaborateurs et construire une différenciation de l'entreprise sur son marché.

Enfin, toutes les entreprises n'ont pas les moyens et la capacité de mettre en place un RSSI qui a l'expertise de la protection cyber.

[39] "Les PME face aux enjeux de sécurité informatique", IFOP pour Kaspersky Lab & Euler Hermès, novembre 2018.
[40] « Le paysage des cybermenaces en 2018 », Accenture, 28 novembre 2018.
[41] La Grande consultation des entrepreneurs (enquête OpinionWay pour CCI France, La Tribune et Europe 1) d'octobre 2018 sur la cybersécurité.
[42] 5ème édition du Baromètre annuel du Cesin, Analyse exclusive de la cybersécurité des grandes entreprises françaises, 2020.

b) L'organisation de l'expertise de cyberprotection

Quand les entreprises se dotent d'un RSSI, un certain nombre de problèmes organisationnels peuvent apparaître. Le RSSI, qui a l'expertise de la cyberprotection, assure les besoins essentiels de sécurité de l'entreprise pour conserver la disponibilité d'accès aux ressources et des données, l'intégrité des données et leur non-corruptibilité et l'accès restreint (ou confidentialité) aux personnes autorisées.

Son rôle est notamment de :

· évaluer et prioriser les ressources à protéger ;

· informer la direction sur les risques ;

· mettre en œuvre des contrôles appropriés ;

· anticiper et réagir aux incidents ;

· adapter ses décisions en fonction de l'organisation en fonction de ses spécificités.

Plus largement, il coordonne les actions en matière de sécurité, que ce soit sur les mesures à prendre, les investissements à réaliser ou la transmission d'une culture de la sécurité.

En réalité, le RSSI est le trait d'union entre la Direction des systèmes d'information (DSI) qui protège les systèmes et l'entreprise qui a un besoin de protection de l'activité ; il n'est pas censé privilégier les systèmes mais la poursuite d'activité. Dans les faits, il est plus souvent l'adjoint sécurité de la DSI. Il faut dire que la notion de RSSI est quelque peu ambivalente : elle comprend, à la fois, les termes responsabilité et sécurité. Autrement dit, celui-ci doit avoir l'oreille du dirigeant comme celle du DSI. De même, le DSI doit soutenir le RSSI et lui donner les moyens d'assurer ses missions.

En outre, les mesures mises en place par les RSSI sont souvent déconnectées des besoins et des préconisations d'autres fonctions telles que la Direction commerciale, la Direction juridique, les Directions de la Communication ou du Marketing, etc.

Tout cela souligne une certaine dissonance entre la couverture des risques exigée aujourd'hui par le degré de risque et la hauteur de la réponse mise en œuvre.

2) Les entreprises n'ont pas le même degré de maturité en matière cyber

Il est intéressant de voir, à cet égard, comment les entreprises peuvent être structurées au regard de la maturité en cybersécurité. On peut distinguer cinq familles de maturité en matière de cyber (les trois premières relèvent de la sécurité ; les deux dernières de la résilience). C'est lorsque les entreprises sont entrées dans une approche élargie que l'on peut considérer qu'elles vont être réceptives à une stratégie de cyberrésilience.

Classement des entreprises par famille de maturité en cybersécurité[43] :

- **une approche réactive** : les organisations gèrent l'urgence et se mettent à niveau au plan technologique (mises à jour) et réglementaire (mise en conformité) sans mettre en place une politique élaborée de sécurité ;

- **une approche basique** : les organisations se mettent à jour et procèdent à des évaluations de sécurité sur leurs systèmes ; cette démarche est souvent peu flexible et non évolutive ; elle est longue à mettre en place et les correctifs sont chers et complexes ;

- **une approche élargie** : les organisations intègrent un niveau d'automatisation dans la sécurité tout au long du développement ; le système de sécurité informatique et cyber est alors confronté à des tests d'intrusion manuels permettant de corriger le système; cette approche peut être éprouvée par les démarches Agile[44] et DevOps[45] qui révèlent les lacunes de manière plus flagrante ;

[43] Classification issue de : La cybersécurité à l'usage des dirigeants, Livre blanc, Clusif et Ossir, 29 janvier 2020.
[44] Méthode qui repose sur les interactions constantes entre le client et l'équipe du projet dans le but d'adapter constamment le produit ou le concept. Cette méthode s'adapte aux autres métiers (Définition Start/Les Échos)
[45] Méthode et pratique technique visant à l'unification du développement logiciel (dev) et de l'administration des infrastructures informatiques (ops) dans toutes les étapes de création d'applications et de logiciels.

- **une approche avancée** (déjà sur le terrain de la cyberrésilience) : les organisations protègent chaque composante de la phase de développement jusqu'à celle de production en passant par l'assurance qualité par exemple ; cela offre un modèle plus rentable et une meilleure protection ; les dernières tendances en matière de DevSecOps[46], qui consiste à penser à la sécurité des applications et de l'infrastructure, vont dans ce sens ;

- **une approche prospective et communautaire** (au cœur de la cyberrésilience) : les organisations anticipent les externalités et les impacts non immédiatement identifiables ou visibles dès la genèse des produits ou services (lorsque cela est possible). Cette approche qui repose sur le partage d'expérience et la mutualisation des ressources avec des partenaires de confiance est indispensable pour gagner en compétence et en efficacité. Sécurité et résilience font alors partie du développement de la production tout au long du cycle de vie.

3) L'approche par les leviers reste pertinente

a) Les évolutions législatives et réglementaires

Les normes ou évolutions réglementaires sont un premier levier pouvant peser dans l'évolution de la maturité de l'entreprise. Les dirigeants d'entreprise ne voient pas toujours ces évolutions de normes comme des opportunités. Pourtant, les développements précédents ont montré que le respect et la conformité aux standards (par application stricte de la loi ou par certification) peut représenter un véritable avantage comparatif (*Voir Infra*). Certains grands groupes ne s'y sont pas trompés et sont même allés jusqu'à influencer des réglementations sectorielles, nationales voire européennes.

Dans ce même élan, un an après l'entrée en vigueur du RGPD, les entreprises ont investi dans l'analyse de leurs données et de leurs systèmes d'information afin de renforcer la sécurité de leurs systèmes. Les entreprises estiment que la sécurisation des extrémités du réseau (32 %) et l'amélioration de la surveillance du trafic DNS (29 %) sont les meilleurs moyens d'assurer la protection des données, outre l'ajout de pare-feux (22 %).[47]

Les acteurs institutionnels, tels les collectivités locales, ont aussi renforcé leurs exigences en matière de conformité aux réglementations en lien avec la cybersécurité dans le cadre des appels d'offre. Tout cela montre l'impact positif du RGPD sur la protection des données dépassant le seul cadre juridique et une transposition concrète dans le quotidien de l'entreprise. De même, les contraintes et normes liées à des secteurs économiques sont des véritables passages obligés pour accéder à des marchés. C'est particulièrement vrai pour les ETI qui s'appuient sur les certifications pour accéder aux marchés.

Dans un même esprit de levier pour l'économie, la Directive « NIS » (National Information Security), transposée en 2018, permet à l'Union Européenne « de faire face aux risques de sécurité dans le monde numérique pour les années à venir. Cette législation est une pierre angulaire pour que l'Europe devienne un acteur mondial en matière de cybersécurité »[48]. Cette réglementation apporte un capital de confiance essentiel pour la santé économique de l'Industrie en Europe. Elle est renforcée depuis le printemps 2019 par le Cybersecurity Act offrant un « cadre de certification de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification »[49]. Le règlement donne notamment toute sa place à l'Agence européenne chargée de la sécurité des réseaux et de l'information (European Union Agency For Cybersecurity ou ENISA), notamment pour la délivrance de certificats qui bénéficieront d'une reconnaissance mutuelle au sein de l'Union européenne (UE).

b) Le rôle des apporteurs de solutions et organismes de conseil

Par ailleurs, des organismes de conseil jouent un rôle d'influenceur en termes de solutions et standards à adopter : ils créent les tendances et la confiance en apportant leur caution à certaines solutions. Le problème est qu'en l'espèce, les caractéristiques marketing du produit recommandé par les conseils sont souvent mises en avant au détriment des caractéristiques techniques. Ce n'est pas la protection du système de l'entreprise (finalité) qui va orienter le choix mais la technologie préconisée et ce, d'autant

Jérôme FRANTZ
GICEF

« Travailler pour les PME, c'est travailler pour tous les maillons de la chaîne de valeur. Les filières industrielles vont à l'avenir se resserrer sur des territoires plus courts. Il faut donc imaginer un système pour sécuriser les filières »

[46] Contraction de développement applicatif (Dev), sécurité (Sec) et administration des infrastructures informatiques (Ops).
[47] IDC 2019 Global DNS Threat Report, publié par EfficientIP en partenariat avec IDC, 2019.
[48] https://www.oodrive.fr/blog/reglementation/cybersecurity-act-ou-comment-repondre-plus-efficacement-a-la-cybermenace-en-europe/
[49] Source ANSSI : https://www.ssi.gouv.fr/administration/reglementation/cybersecurity-act/

plus facilement que cette dernière est souvent opaque aux yeux des dirigeants ou des DSI. Le rôle des réseaux de RSSI est de véhiculer les bonnes pratiques dans l'objectif de cybersécurité.

c) Le rôle des intra et interrelations des entreprises

Si cela n'apparaît pas de manière évidente, des entreprises tierces (clients, partenaire) peuvent jouer aussi le rôle de levier en exigeant des garanties en matière de cybersécurité. Par ailleurs, tous les protagonistes d'un écosystème sont dépendants de la sécurité de chacun des partenaires. Ainsi, les vérifications des standards de chaque acteur au sein de sa chaîne de valeur peuvent constituer un levier pour les entreprises (interconnexions des systèmes d'information).

d) Les externalités négatives

Il existe, enfin, des éléments extérieurs qui permettent de favoriser l'activité des entreprises, spécialement en temps de crise, qu'elle soit d'origine cyber ou autre. La crise du coronavirus a révélé des facteurs favorables à la résilience des entreprises et transposables aux attaques cyber. Dans le cas de la pandémie, on observe que la résilience a été le résultat de l'action du dirigeant et des collaborateurs. Dans un scénario de cyberattaque, c'est la même règle qui s'applique : la confiance des collaborateurs dans la reprise (normalité) et dans la continuité de l'activité (nouvelle normalité) permet de résorber les effets de la crise et ses dégâts.

Pour capitaliser sur les externalités négatives (ou effets pervers vertueux), c'est tout l'écosystème de l'entreprise qui doit être sollicité. Le dirigeant et son responsable cyber doivent être attentifs aux signaux forts ou faibles dans l'idée de capitaliser sur tout nouvel événement de son environnement.

En résumé, une posture de cybersécurité présente un certain nombre d'avantages ; l'adoption du cadre juridique requis agit, *a minima*, comme un protecteur et, au mieux, comme un marqueur de confiance auprès des clients et partenaires.

De même, les outils technologiques apportent le rempart nécessaire contre les menaces connues ou prévisibles mais ils ne sont souvent qu'un empilement de solutions qui ne sauraient préparer à celles qui ne sont pas prévisibles, ce qui est le propre du cyber-risque.
Depuis 2017, les grandes attaques successives, via des logiciels crypto-verrouilleurs (*cryptolockers*) qui consistent à coder les données les rendant inaccessibles, ont montré que les plans de sécurité informatique, de continuité d'activité ou de continuité d'entreprise ne suffisaient plus pour répondre à une cyberattaque de grande ampleur et redonner, à l'entreprise, une santé économique pérenne. On arrive alors à un état où la cybersécurité dépasse le cadre de la responsabilité de l'expert pour devenir un projet d'entreprise impliquant l'ensemble des ressources de l'entreprise et tout particulièrement les ressources humaines. C'est la fin du modèle expert et l'avènement du *risk management*.

Enfin, un des travers est de croire que la cybersécurité est une question technique, voire technologique. C'est un point de vue répandu : même le RGPD repose sur des éléments techniques lorsqu'il évoque la cybersécurité. Or, cette dernière est, avant tout, une question humaine. Par conséquent, la cybersécurité est le premier étage d'un dispositif de réponse d'une entreprise au risque cyber ; les limites de cette posture réactive et défensive doivent inciter les entreprises à passer à une approche proactive et offensive ; c'est tout le sens de la cyberrésilience.

PARTIE 2

LA CYBERRÉSILIENCE : LA SÉCURITÉ CONSTRUITE À PARTIR D'UNE DÉMARCHE OFFENSIVE ET PROACTIVE

Le changement de démarche en matière de réponse au cyber-risque provient le plus souvent de la confrontation à la cybermenace et d'une prise de conscience que le risque est structurel. La compréhension de la cyberrésilience est aussi largement dépendante du degré de maturité de l'entreprise face au risque cyber comme on a pu le voir précédemment.

La cyberrésilience n'échappe pas aux outils technologiques : ceux qui relèvent de la cybersécurité (mise à niveau et bonne configuration des systèmes et composition avec des solutions systèmes) mais aussi ceux qui permettent de passer à un stade supérieur de sécurité. Mais elle va évidemment bien au-delà. La cyberrésilience est une approche globale qui sollicite toutes les forces de l'entreprise.

A) QU'EST-CE QUE LA CYBERRÉSILIENCE ?

La notion de résilience est largement usitée aujourd'hui. Elle est souvent assimilée à la résistance de l'entreprise face à une crise.

Certains considèrent la cyberrésilience comme un dispositif de barrières technologiques à mettre en place pour se protéger des cyberattaques et ne pas être affecté par ces attaques. D'autres la considèrent comme une posture, une stratégie et une organisation visant à absorber les cyberattaques en minimisant les pertes pour l'entreprise tout en poursuivant l'activité et en transformant l'entreprise. C'est cette définition plus large que l'on retiendra ici.

1) La cyberrésilience est une posture, une stratégie et une organisation

La cyberrésilience est donc, à la fois, une posture, une stratégie et une organisation.

a) C'est une posture

La cyberrésilience repose sur les trois principes suivants :

• **considérer l'échec comme une expérience :** la résilience invite à considérer l'échec comme source d'expérience voire comme « le fruit du risque »[50] ; il s'agit de tirer les leçons d'une situation non voulue ou non attendue, en l'occurrence une cyberattaque, et de prendre en compte l'entreprise elle-même comme paramètre de cette situation (valorisation de l'échec).

• **admettre le risque et lâcher prise :** la résilience appelle aussi au lâcher prise ; en cas de crise grave lors d'une cyberattaque, il importe de ne pas laisser la situation s'enkyster dans le mental de l'entreprise, tel un traumatisme. Il faut accepter le nouvel état dans lequel la perte n'est pas récupérable et rechercher un nouvel équilibre. La dynamique de l'entreprise constitue le moteur du recouvrement de l'activité et de pérennité de l'entreprise (acceptation et adaptation).

Paola FABIANI
WISECOM

« La cyberrésilience : c'est se préparer à la perte de données. C'est se mettre en position de répondre et de continuer après une attaque »

• **rebondir et innover :** une fois les leçons tirées et le risque accepté, la résilience consiste à rebondir et innover, avec son écosystème et son marché, jusqu'à transformer le modèle d'affaires (continuité et transformation). "En perma-

[50] CCI Entreprendre, Développer vos capacités de résilience, 12 août 2016.

nence, il faut pouvoir identifier, protéger, détecter, répondre à l'incident et récupérer les systèmes pour garantir la continuité de l'activité et rebondir"[51] (anticipation).

En conséquence, la cyberrésilience est un processus, non une situation, visant à assurer la continuité et la transformation. Le chemin est toujours plus long lorsqu'on ne le connaît pas. En cas d'impréparation, la gestion de l'incident se déroule à vue et dans l'urgence. Lorsqu'elle est préparée, la gestion est balisée et définie. Ses effets peuvent être mesurés et planifiés.

Nicolas ARPAGIAN
ORANGE CYBERDEFENSE

« Le cyber ne doit pas se résumer à de l'informatique et à de la sécurité. Elle exige une implication opérationnelle des responsables métiers »

La posture de résilience est donc une « exigence de pensée » à chaque niveau, sur l'activité et sur le produit. C'est une approche cycle de vie de l'activité de l'entreprise (approche avancée en termes de maturité) (Voir Partie 1). La cyberrésilience est alors dépendante de l'adhésion de tous.

Elle n'est plus seulement l'affaire de la DSI qui ne peut voir sa charge de travail augmenter de façon illimitée, ni du RSSI qui ne pourra parvenir à restaurer la situation antérieure à une attaque. La cyberrésilience doit être étendue à d'autres services ou champs d'action.

b) C'est une stratégie

Acquérir une posture cyberrésiliente passe par une réflexion stratégique du dirigeant d'entreprise et du Comité de direction sur un ensemble de décisions à prendre pour protéger et gérer les actifs de l'entreprise en vue de permettre la continuité d'activité et la pérennité de l'entreprise. La personnalité des dirigeants, managers et porteurs de la cyberrésilience sera déterminante.

Une stratégie de cyberrésilience consiste notamment à identifier les actifs stratégiques (physiques ou immatériels), évaluer la capacité de continuité de l'activité et évaluer l'impact sur la pérennité de l'entreprise et son *business model*.

• **Identifier les actifs stratégiques :** il faut identifier les actifs les plus importants, physiques ou immatériels pour l'entreprise (détermination de leur valeur). Le dirigeant doit ainsi se poser un certain nombre de questions essentielles qui ont trait à la valeur[52] :

- systèmes d'information et réseaux : quel serait l'impact de leur inaccessibilité sur l'activité ?
- données stratégiques : quelles seraient les conséquences en cas de vol d'informations à caractère sensible (contrats avec des partenaires et des fournisseurs, *business plan*, etc.) ?
- données à caractère personnel : quelle est leur valeur pour l'entreprise, pour les hackers ?

En effet, le but n'est pas de mettre en place des niveaux de sécurité de 100 % - au demeurant impossibles avec la sophistication croissante des cyberattaques - mais plutôt de se préparer, anticiper les failles et limiter les impacts sur les actifs les plus importants, y compris sur la réputation de l'entreprise par exemple.

La Direction générale, en lien avec les autres directions et métiers, doit également pouvoir identifier les données et déterminer la valeur des données. Il faut, par exemple, hiérarchiser les données à protéger et non pas chercher à protéger toutes les données sans distinction.

• **Évaluer la capacité de continuité de l'activité dans un scénario de cyberattaque :** cela signifie recenser des actions nécessaires pour mettre en adéquation les systèmes informatiques avec les besoins d'activité (mise à niveau du système de sécurité) mais aussi mettre en place toutes les conditions nécessaires à la continuité de l'activité : gestion de crise, audit qualité, procédures de restauration, adaptation des postes et méthodes de travail pour assurer une qualité équivalente à celle existante avant une attaque potentielle.

Le dirigeant doit aussi apprécier la continuité d'activité sur le moyen terme en intégrant le fait que les répercussions financières d'une cyberattaque peuvent courir sur des mois, voire des années, générant des obligations

[51] "De la cyber-sécurité à la cyber-résilience", Les Échos, 19 mars 2018.
[52] Laurence Duarte, « Pourquoi le cyber-risque est devenu un incontournable de votre stratégie d'entreprise », HBR France, 20 février 2019.

financières pour l'entreprise. Enfin, dans cet exercice, la qualité et la nature de l'offre de l'entreprise (produits ou services) doivent être maintenus.

• **Évaluer l'impact sur la pérennité de l'entreprise et son business model :** au plan financier, le dirigeant doit trouver le bon équilibre entre coûts et risques car une approche cyberrésiliente nécessite de nouvelles ressources et une nouvelle affectation de celles-ci (retour sur investissement, répartition des coûts, etc.) ; il doit aussi étudier et analyser l'impact d'une démarche de cyberrésilience sur le modèle d'affaires (business model), voir quelles composantes sont affectées ou doivent potentiellement être repensées, etc.

Au terme de cette phase, il peut envisager de faire de la cyberrésilience un levier de transformation de ce modèle ou, à tout le moins, imaginer un moyen de rentabiliser ses investissements. Il peut ainsi réfléchir plus largement à la manière dont il peut valoriser (au sens de création de valeur) les investissements, innovations et réorganisations opérés au titre de la cyberrésilience (Voir Infra) en tant qu'avantages comparatifs et sources de revenus.

c) C'est une organisation

La cyberrésilience passe aussi par une organisation flexible et compétitive, exploitant l'expérience et saisissant les opportunités : « *une organisation résiliente est une organisation qui ne se contente pas de survivre sur le long terme, mais qui s'épanouit, passant l'épreuve du temps* »[53]. C'est une organisation qui permet de gérer la crise, assurer la continuité d'activité, transformer l'entreprise dans un processus continu.

Une organisation résiliente s'entend d'une organisation qui sait allier la continuité et la transformation pour s'adapter aux nouvelles contraintes, tant internes que propres au marché. Il faut imaginer une organisation où les structures vont pouvoir « *composer en permanence avec les éléments* (...) »[54]. Tout cela passe par une plus grande transversalité et agilité.

Une organisation résiliente s'entend aussi d'une organisation qui fluidifie le partage d'informations. Il est important, par exemple, que le Comité de direction soit non seulement informé mais qu'il le soit aussi rapidement. Dans certaines entreprises, les membres du Comité de direction n'entendent même jamais parler de cybermenaces. Les remontées d'information - notamment celles qui sont recueillies par la pratique de mises en relation - doivent aussi être facilitées.

C'est une organisation qui doit, enfin, permettre le partage d'expérience et la mutualisation des ressources avec des partenaires de confiance. L'acquisition de l'information peut et doit ainsi passer par les acteurs institutionnels de l'écosystème cyber qui sont autant de *hubs* de veille d'information et d'intelligence économique permettant d'accroître la réactivité des cellules de crise en cas de cyberattaque. C'est un nouvel écosystème socio-économique qui est créé à ce stade avec l'échange de bonnes pratiques, d'outils de veille et de *business intelligence* dans l'appréhension du risque cyber. On passe alors à un degré de maturité supérieur (*Voir Partie 1*).

2) Des outils pour la continuité et la transformation de l'activité/entreprise

a) La cartographie des cyber-risques

Dans une approche résiliente, chaque entreprise doit réaliser sa cartographie des cyber-risques, des failles système et des failles utilisateurs car chaque activité et chaque structure sont spécifiques. Par exemple, le risque de déni de service n'est pas le même selon que l'entreprise est une banque ou un fleuriste. Pareillement, un *ransomware* ne touchera pas de la même manière une société d'expertise comptable et une supérette ; l'une possède une activité qui repose sur la gestion des données sensibles alors que l'autre possède des données enregistrées et non-sensibles.

Les champs sensibles ou pouvant être impactés par les cyberattaques doivent être identifiés. Il est aussi nécessaire, dans cette cartographie, d'avoir la pleine connaissance des fonctions, outils et ressources disponibles ainsi que celles mobilisables en cas de survenance d'un incident cyber. La cartographie portera aussi sur les acteurs qui interviennent sur la chaîne de valeur de l'entreprise (fournisseurs, partenaires....) d'autant qu'aujourd'hui, les entreprises sont souvent intégrées dans des

Annabelle CHREBOR
E-TIPI LEARNING

« Les cyberattaques visent également les plateformes métiers qui sont interfacées avec les systèmes d'information des Grands groupes. Il est primordial de prendre en compte les enjeux Sécurité tout au long de leur développement et déploiement. »

[53] Selon Howard Kerr, Directeur de BSI Group, groupe de certification britannique in : La résilience organisationnelle : exploiter l'expérience, saisir les opportunités, Livre blanc, BSI Group.
[54] « De la cyber-sécurité à la cyber-résilience », Les Échos, 19 mars 2018.

schémas d'externalisation de certaines fonctions support (finance, comptabilité, relation-client) mais aussi dans des schémas de chaînes d'approvisionnement (supply chain) fortement digitalisés.

Cela implique de cartographier le recours de l'entreprise à des prestataires de solutions numériques extérieures. En effet, des réseaux externes viennent s'interconnecter au réseau de l'entreprise et peuvent constituer potentiellement des portes d'entrée pour des intrusions cyber pour tous leurs utilisateurs légitimes réciproques. Ce réseau IT de l'ombre (*shadow IT*) résulte du besoin croissant de solutions numériques que la DSI d'une entreprise ne peut offrir seule (ajout de solutions tierces à son propre réseau).

La cartographie des risques peut être un levier de transmission de la cyberrésilience d'autant plus puissant qu'elle intégrera les remontées des mises en situation : *crash tests* (y compris sur les plans de continuité d'activité et d'entreprise), campagnes anti-*phishing* ou simulations de crise… Ces pratiques permettront de faire remonter les failles et d'améliorer la résilience.

Enfin, elle permettra d'identifier les actions de prévention et de résilience pertinentes en termes de mise à niveau des systèmes et de sécurisation, de sensibilisation et d'acculturation, d'organisation et de gouvernance. Pour mieux comprendre, le tableau ci-dessous met en correspondance les points d'entrée des cyberattaques avec les actions préventives pour les empêcher et les champs de résilience pouvant être sollicités en cas de scénario de réalisation.

Leviers d'action de la cyberrésilience identifiés grâce à la cartographie des risques

Famille	Risque	Champ de cyberattaque : point d'entrée			Champ de cybersécurité : solution préventive			Champ de cyber-résilience			
		Collaborateurs	Système IT	Écosystème	Solution préventive 1	Solution préventive 2	Solution préventive 3	RSSI	PCA	Gouvernance	Gestion RH
Atteinte à l'image	Déni de service, abus de privilège		X		Mise à jour	Authentification forte		X	X		
Cyber-criminalité	Ransonware	X	X		Sauvegarde	Mise à jour	Sensibilisation	X	X	X	X
	Botnets		X		Mise à jour	Authentification forte		X	X		
	Ingénierie sociale	X		X	Sensibilisation	Authentification forte	Organisation et processus de décision	X	X		X
	Phishing, SPAM, fraude au Président	X		X	Sensibilisation	Authentification forte	Organisation et processus de décision	X	X	X	X
Espionnage	Malware		X		Mise à jour	Sauvegarde		X	X		X
	Web application attacks		X		Mise à jour	Sauvegarde		X	X		X
	Spear-Phishing	X	X		Sensibilisation	Authentification forte	Organisation et processus de décision	X	X	X	X
	Scripts et fichiers PE exécutables		X	X	Mise à jour	Sauvegarde		X	X	X	
	Chevaux de Troie téléchargeurs , Adware	X	X	X	Sauvegarde	Mise à jour	Sensibilisation	X	X		
Sabotage	Blocage de l'architecture réseau, failles exploitation et packs exploitation	X	X	X	Authentification forte	Sensibilisation	Organisation et processus de décision	X	X		
	Dégâts physiques, vol, perte	X		X	Authentification forte	Sensibilisation		X			X

Sources : tableau réalisé à partir du baromètre Cesin, TheCost of Cybercrime Ninth Annual Cost of Cybercrime Study Unlocking The Value Of Improved Cybersecurity Protection, Institut Ponemon, Accenture 2019, Kaspersky, Le Monde Informatique, Checkpoint, Cybercover et Journal du Net.

Commentaires : il faut garder à l'esprit que les cyberattaques ne compromettent pas toutes les fonctions de l'entreprise, ce qui implique des postures responsives différenciées.

Point d'entrée : le point fort qui émerge de toutes les observations recueillies pour cette étude, c'est que, quelle que soit la configuration mise en place, il y aura toujours un cybercriminel qui pourra attaquer. Les points d'entrée des cyberattaques n'ont pas de configuration-type. Les porteurs de solutions et les cybervictimes témoignent du fait

que les point d'entrée des cyberattaques reposent principalement sur l'humain (sa vigilance ou sa défaillance), sur les failles techniques et sur l'organisation de l'entreprise qui peut, elle-aussi, créer des failles (standards non mis à jour, non-conformité des partenaires dans l'écosystème).

Cybersécurité : les solutions préventives visent à permettre la réaction humaine la plus adaptée pour limiter l'attaque, voire l'enrayer. On passe de solutions de type mise à jour, authentification forte, etc. à des solutions liées à l'organisation et aux processus de décision/exécution de l'entreprise.

Cyberrésilience : l'attention humaine reste la base pour s'assurer des mises à jour et bonnes configurations, d'une part, et de la sensibilisation et de l'adoption de bonnes pratiques, d'autre part. Les réponses impliquent le RSSI dans la résolution du problème et la mise en place du Plan de continuité d'activité (PCA) dans la plupart des cas. On optera pour une réponse encore plus solide en intégrant le management des ressources humaines et les structures de gouvernance de l'entreprise.

b) Le Plan de continuité de l'activité et sa reconfiguration

L'un des outils essentiels en matière de cyberrésilience est évidemment le Plan de continuité de l'activité (PCA). Toutefois, il apparaît que les plans de continuité des activités ne sont pas aussi robustes que les plans informatiques associés[55]. Ces plans « *cultivent l'illusion du contrôle* », constate Nicolas Gouzien, Directeur au sein du groupe Square. L'incapacité de poursuivre la production dans l'industrie ou la prestation de service met souvent à terre ces Plans de continuité d'activité.

Les PCA sont souvent conçus en deçà des attentes, notamment par sous-évaluation des risques. Il peut donc être utile d'entrer, là encore, dans une démarche de certification des PCA pour s'assurer de leur robustesse avec, par exemple, la norme ISO 22301 reconnue comme principale norme de continuité des activités.

Jean-Philippe GAULIER
CYBERZEN

« L'approche pragmatique doit toujours guider l'audit et la transformation de l'entreprise »

c) L'intégration de l'écosystème dans la cyberrésilience

Dans une approche cyberrésiliente, l'écosystème de l'entreprise doit aussi être pris en compte car il est apporteur de solutions.

L'interaction des données et des systèmes d'information doit être appréciée simplement afin de configurer les accès aux données et de classifier le risque sur ses caractéristiques tolérables, indispensables au fonctionnement du système ou soumis à authentification.

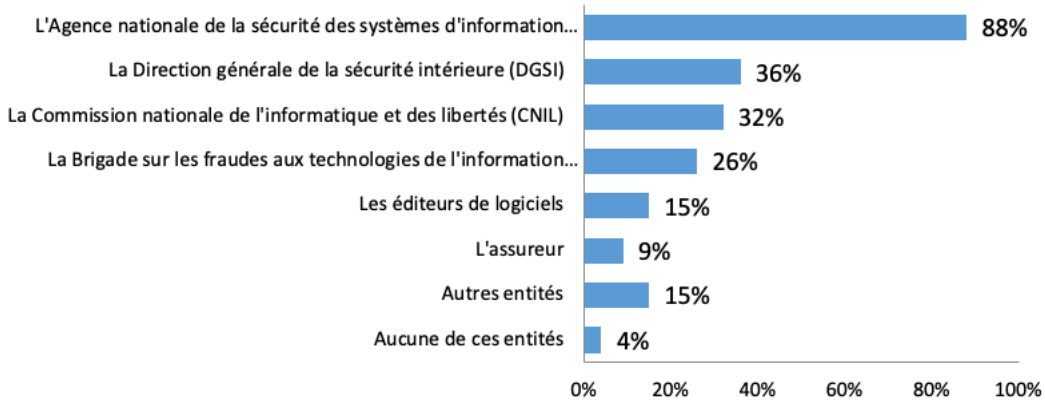
• **Un premier écosystème à intégrer est celui de la protection de l'activité :** on pense évidemment aux apporteurs de solutions techniques mais cela s'entend aussi de la couverture d'assurance, des audits de sécurité des systèmes d'information (SSI) et des certifications. Les solutions utilisées et les couvertures juridiques et d'assurance employées en cas de sinistre seront des éléments attendus, voire exigés, par les clients et/ou donneurs d'ordre dans la chaîne de valeur.

• **Un deuxième écosystème à intégrer est celui de ses clients et fournisseurs :** on pense ici à la consolidation de tous les partenaires (fournisseurs, sous-traitants et clients) qui constituent la chaîne de valeur autour de l'activité de l'entreprise. Il s'agit pour elle de créer un écosystème propre à sa production ou à son service en insufflant la sécurité et la résilience comme le prisme permanent d'alimentation de cette chaîne de valeur. La communauté de clients peut être très importante dans cette gouvernance de produit/service repensée, comme l'emblématique exemple Lego peut l'incarner : les utilisateurs y apparaissent comme force d'innovation et comme moteur d'e-réputation sur les réseaux sociaux.

• **Un troisième écosystème à intégrer est celui des organismes d'accompagnement :** dans ce processus de résilience, l'accompagnement d'un « tuteur transitionnel »[56] permet d'apporter protection, assurance et sécurisation ; c'est le rôle que jouent ainsi des acteurs comme l'ANSSI, la CNIL et les CCI (Voir Glossaire) en tant que pivots dans la sortie de crise mais aussi dans l'anticipation du cyber risque. L'ANSSI, en sa qualité d'autorité nationale, peut ainsi accompagner les entreprises de taille modeste, peu dotées en managers des services d'information dans leurs choix par la qualification et la certification de solutions de sécurité. Il faut aussi reconnaître l'action de l'État en matière de cybersécurité tant au niveau des tuteurs transitionnels (ANSSI) que de la Gendarmerie nationale. Mais il en existe bien d'autres encore.

[55] John Cray, "How to Ensure You Have the Right Business Continuity Plan in Place", Industry Week, June 9, 2020.
[56] Pour reprendre ici l'expression de Boris Cyrulnik.

Écosystème des partenaires institutionnels



Source : 5ème baromètre du Cesin, 2020

B) LA CYBERRÉSILIENCE PASSE, D'ABORD, PAR LES COLLABORATEURS

Une posture cyberrésiliente repose sur un socle qui possède une part technologique mais surtout sur une part non technologique relève de l'humain.

La posture cyberrésiliente est une question d'adoption mais aussi d'appropriation des enjeux sécuritaires par tous les collaborateurs, au-delà des Directions des services informatiques (DSI). On est là dans le management et la formation des ressources humaines. Si ces dernières sont bien formées, elles peuvent même endiguer une cyberattaque.

1) L'indispensable acculturation des collaborateurs

Véronique PLESSIER-CHAUVEAU
EULEOS

« La sensibilisation doit porter sur tout le monde et pousser chacun à adopter des réflexes simples de comportement. La répétition des recommandations est pour l'instant le moyen le plus efficace »

On a pu voir précédemment que les attaques envers les entreprises sont souvent rendues possibles, non pas par erreur ou faute, mais par défaut de vigilance ou encore par méconnaissance des règles de sécurité par l'utilisateur (« *ce qui se trouve entre l'écran et la chaise* »)[57].

C'est la raison pour laquelle il est absolument essentiel que, dans une stratégie de cyberrésilience, l'entreprise s'appuie sur ses collaborateurs afin qu'ils comprennent tous les enjeux. Cependant, depuis quelques années, le principe consistant à « ne faire confiance à personne » (ou *zero trust*) a, d'ailleurs, investi le champ de la sécurité. Les apporteurs de solutions ont aussi fait largement campagne sur l'excellence de leurs produits tout en expliquant les intrusions par un facteur qui sortait de leur champ : le collaborateur (ou ses cercles proches) au risque de faire de celui-ci le bouc émissaire, créateur de failles dans une technologie autosuffisante.

Alors qu'il existe des marqueurs de confiance dans les usages du quotidien[58], rien n'existe sur les usages et la sécurité numérique qui sont laissés à la discrétion des politiques de sécurité des entreprises et sans autre repère dans la sphère privée.
Aussi les collaborateurs vont-ils rechercher des réponses à leurs besoins lorsque ceux-ci ne sont pas proposés par l'entreprise. L'exemple fameux en la matière est celui de l'interdiction des usages de stockage USB (vecteurs de contamination en termes de virus et de logiciels malveillants). Les utilisateurs passent alors par des espaces de stockage en ligne, le plus souvent conseillés par leurs collègues ou collatéraux. Dès lors, cela pose un problème sur les aspects juridiques liés à l'hébergement des données et plus largement à la souveraineté des données.

[57] Pour reprendre ici une expression parfois employée.
[58] Par exemple, l'Agence nationale de sécurité du médicament et des produits de santé.

Dans le cadre des campagnes de *phishing*, il faut aussi se poser la question de l'efficacité des solutions de filtres anti-spam et anti-hameçonnage avant d'incriminer l'utilisateur. Certaines campagnes sont si bien faites que même informés et sensibilisés, les utilisateurs en seront victimes. C'est une des raisons pour lesquelles 95 % des attaques se font par l'intermédiaire du mail car le lien direct entre l'assaillant et la victime échappe au contrôle technologique.

2) Les différentes voies d'acculturation

L'acculturation des collaborateurs à une posture résiliente passe, d'abord, par des messages répétés de sensibilisation sur les règles de bonne conduite à suivre :

- attacher et verrouiller les dispositifs informatiques pour éviter l'intrusion et le vol ;
- éviter l'usage de périphériques de stockage USB dont l'origine n'est pas certifiée par le RSSI ;
- appliquer l'authentification à deux facteurs (2FA) à tous les utilisateurs à titre de mesure de base ;
- crypter les données et chiffrer les mails selon les normes définies par la politique de sécurité des données ;
- favoriser l'emploi d'actifs numériques (*token*) pouvant être transférés sans duplication entre deux acteurs sur Internet et sans nécessiter l'accord d'un tiers ;
- mettre en place des programmes de sensibilisation pour combattre la menace persistante associée au phishing et aux techniques d'ingénierie sociale connexes.

Didier BARBOLLAT
SOCIÉTÉ GÉNÉRALE

« La sensibilisation va du Coffee&Learn convivial au e-learning obligatoire en passant par des vidéos ou une semaine dédiée à la sécurité »

Elle doit aussi se traduire par une adoption de méthodes de travail (VPN ou réseaux privés virtuels, nomenclature des données) et d'usages du numérique (chiffrement des données, élimination des supports contaminant type USB), y compris en dehors de la sphère professionnelle (sécurisation des ressources personnelles, non-connection sur les réseaux non sécurisés).
Avec un coût relativement faible, la sensibilisation et la formation réduisent aussi massivement les comportements inadaptés et peuvent enrayer une cyberattaque même élaborée. Elles passent le plus souvent par l'organisation de séminaires permettant d'acquérir bonnes pratiques et bons réflexes.

Cette acculturation passe, ensuite, par des tests de mise en situation dans lesquelles les technologies numériques sont aujourd'hui d'un soutien précieux. Ces tests consistent à tendre l'hameçon aux collaborateurs et de voir s'ils y mordent. Le cas échéant, une phase de débriefing permet de revenir sur les erreurs commises et les phases de sécurité qui ont mal été réalisées. Il s'agit alors d'une phase dite *name and shame* (faire savoir ce qui a été mal fait) durant laquelle certains collaborateurs peuvent se montrer plus rétifs aux règles et usages de sécurité.

Le double avantage de ces mises en situation est de permettre aux collaborateurs de bien réagir en cas de crise (à l'image des tests de sécurité « incendie ») en les plongeant en terrain connu : en général, un tiers des collaborateurs se fait piéger lors d'un premier test de mise en situation[59]. Mais l'année suivante, seuls 3 à 5 % du personnel sont encore concernés[60]. Ces mises en situation identifient également les comportements qui sont des freins ou des blocages à la reprise d'activité. En effet, ces phases de test permettent de jauger l'assimilation des bonnes pratiques, l'adhésion à la culture sécuritaire et résilience (trop sécuritaire ou trop laxiste).

Une autre tendance se développe : basée sur les neurosciences, elle vise à rendre acteurs les collaborateurs dans la compréhension des failles de sécurité qu'ils créent eux-mêmes. Dans une simulation en réalité virtuelle ou augmentée, les collaborateurs sont ainsi mis dans la peau d'un cybercriminel qui cherche à trouver les éléments qui lui permettront de trouver le mot de passe d'un ordinateur de bureau. À partir des éléments usuels de personnalisation de l'espace de travail, ils peuvent alors retrouver ledit mot de passe, montrant tous les éléments que chaque individu laisse en accès aux cyberattaquants pour alimenter l'ingénierie sociale.

[59] Marc Lafleuriel, « La cybersécurité à l'épreuve des utilisateurs », MagIT, 25 novembre 2019.
[60] Un chiffre qui reste stable au fil des ans compte tenu du turnover possible dans l'entreprise.

Enfin, faire appel à l'intelligence artificielle (IA) peut également aider à contrôler les failles et les comportements des collaborateurs de l'entreprise. L'analyse du comportement utilisateur ou *User Behaviour Analytics* (UBA) portera sur trois composantes : analyse de données, intégration de données et présentation[61]. L'UBA est un instrument de détection préventif des attaques et des comportements contraires aux règles de sécurité internes. En mettant en place une telle analyse, les RSSI peuvent réagir plus vite et sans interruption d'activité. Cependant, rien ne remplace la prévention par des sensibilisations simples sur les points sensibles[62].

En intégrant la sécurité comme nouvel usage, voire comme nouvelle norme de travail, les collaborateurs de l'entreprise pourront augmenter leurs propres standards de sécurité. Pour autant, l'accent mis sur l'utilisateur dans cette démarche de résilience ne saurait exonérer d'autres actions.

C) LA CYBERRÉSILIENCE AU CŒUR DE LA GOUVERNANCE

La gouvernance de l'entreprise doit être organisée de manière à réagir rapidement en cas d'attaque, appliquer le plan de continuité qui va garantir la reprise d'activité, faire les arbitrages en termes d'investissements, etc. Cela permet aux dirigeants de prendre des risques mesurés et avec confiance, de répondre rapidement et de façon adéquate aux menaces et aux opportunités.

1) Mettre en place des structures de gouvernance agiles et flexibles

« *Conseil d'administration et direction doivent non seulement communiquer leur soutien à ce type de stratégie mais doivent aussi disposer de toutes les connaissances en matière de cyber-risque* »[63].

C'est tout l'enjeu du partage d'informations autour du cyber-risque : les différentes directions de l'entreprise doivent, en effet, avoir une compréhension partagée du cyber-risque. Le dirigeant étant le pilote de la résilience, il doit disposer d'une plateforme pour mobiliser et articuler les actions.

Pour ce faire, il faut des structures de gouvernance légères et efficaces pour avoir une gestion proactive des cybermenaces. Le cas échéant, certaines entreprises font le choix de créer une cellule de crise (entre Comité de direction et Directions métier) généralement coordonnée par la DSI, auquel cas il est important d'améliorer ses processus de décision. D'autres vont plus loin encore avec un Comité d'adaptation aux cyber-risques.

2) Déterminer la place du RSSI

De plus en plus d'entreprises, spécialement les grands groupes, désignent un RSSI en leur sein. Il est important que le positionnement du RSSI soit clair et audible dans la gouvernance de l'entreprise.

Il ne doit pas forcément servir de fusible en cas de cyberattaque destructrice mais peut être force de proposition sur la politique à mettre en place et les dispositifs à mettre en œuvre. Il doit proposer des solutions techniques et schémas d'organisation permettant de concilier les exigences de sécurité et les impératifs des directions métiers.

Didier BARBOLLAT
SOCIÉTÉ GÉNÉRALE

« Il y a une homogénéisation des politiques RSSI entre les grands groupes. Les fonctions se structurent et se pérennisent. »

a) Le RSSI, premier collaborateur du dirigeant dans la politique de cyberrésilience

Les développements précédents ont montré que la sécurité relevait auparavant des DSI qui devaient monter des barrières face aux cybermenaces. L'arrivée d'un RSSI dans l'entreprise est une avancée significative puisqu'il va être rattaché à une fonction essentielle qui n'est plus la seule continuité de l'activité numérique, mais bien l'intégration des règles de sécurité au cœur de l'activité économique globale.

Il faut souvent (re)penser la place du RSSI dans l'entreprise, son organisation voire sa gouvernance, pour avoir un véritable impact en matière de cyberrésilience. Le RSSI doit être un collaborateur en prise directe avec le dirigeant pour qu'il soit écouté et pour avoir la maîtrise de la sécurité.

[61] Valéry Marchive « L'analyse du comportement utilisateur, nouvel eldorado de la sécurité », LeMagIT, 28 avril 2015.
[62] Comment la pandémie du COVID-19 a radicalement changé le monde de la cybersécurité, Undernews, 8 avril 2020.
[63] « Cybersécurité : la résilience, un incontournable », EY, 8 novembre 2019.

b) Une vision collaborative du travail du RSSI

Mais le RSSI doit travailler de concert avec la politique de sécurité décidée par la Direction générale et la Direction des systèmes d'information (DSI) qui est chargée de la continuité de l'activité numérique de l'entreprise. Il doit aussi travailler de manière transversale, notamment avec les services juridiques afin de veiller à la conformité des processus internes avec les exigences légales.

Alors que les cybercriminels sont organisés et travaillent de manière collaborative, il est essentiel que le RSSI soit, en outre, intégré dans un réseau professionnel pour faciliter son échange de connaissances et de compétences au-delà de la formation ou de la veille personnelle.

c) Une porte d'entrée au CODIR

Si le RSSI est un cadre dirigeant, son appartenance au Comex est loin d'être systématique. Au demeurant, il est essentiel qu'il y ait une porte d'entrée et la possibilité d'influer, le cas échéant, sur l'agenda de ce dernier. Cela pointe instantanément une difficulté accrue pour les PME/TPE qui ne possèdent pas de Comex, voire de Direction des systèmes d'information (DSI) et encore moins de RSSI.

Le RSSI : place dans la gouvernance de l'entreprise

Il existe autant de configurations dans l'organigramme de l'entreprise qu'il y a de combinaisons entre rattachement fonctionnel et rattachement opérationnel entre le RSSI et son autorité de rattachement : Direction Générale, Direction des systèmes d'information, Direction de la sécurité, Direction de la qualité, Direction des opérations, etc.

Certains grands groupes disposent d'un RSSI sous l'autorité fonctionnelle du DSI avec un rattachement opérationnel au Directeur de la sécurité, mais rapportant régulièrement et directement à la Direction générale.

Certains grands groupes sont également passés à la vitesse supérieure en créant un Directeur de la cyberrésilience, en sus du Directeur de la sécurité et du RSSI. Son rôle est d'insuffler la résilience dans chaque étape de la production de l'entreprise. Alliant pédagogie, veille et conseil, il coordonne les mises en situation et les tests à échelle réelle en matière d'intrusion et cybermenace.

D) LA CYBERRÉSILIENCE, PRODUCTRICE DE VALEUR

Une démarche cyberrésiliente n'est pas sans influencer la valeur de l'entreprise et son modèle d'affaires[64]. Ainsi, les ressources-clés vont être affectées par les investissements en solutions et l'intégration des collaborateurs dans la démarche cyberrésiliente. De même, les structures des coûts vont être modifiées par l'impératif de maîtrise de coûts (ROI).

La cyberrésilience impacte les différentes composantes du Business Model Canvas (BMC)

<table>
<tr>
<td rowspan="2">Partenariats clés

Courtiers en cyberassurance

Porteurs de solutions de cybersécurité

Sous-traitants et fournisseurs (respect du cahier des charges cyberrésilient)

Mais aussi intégration de l'écosystème de veille et de business intelligence (réseau cyberrésilient)</td>
<td>Activités clé

Intégration de la cyberrésilience dans le cycle de vie de l'activité (offre de produits et de services)</td>
<td rowspan="2">Proposition de valeur
Valeur ajoutée apportée par la certification et le respect prouvable de normes strictes (recherche de garantie cyber), la confiance résultant de la stratégie du dirigeant, des performances et des innovations</td>
<td>Relations clients

Possibilité d'entamer des relations dématérialisées (via le cloud) et automatisées, interconnexion sécurisée des systèmes d'information entre entreprises</td>
<td rowspan="2">Segment clients
Hiérarchisation et protection des segments-clients précieux en fonction de la marge, des revenus, de l'importance stratégique et des obligations contractuelles
Nouveaux marchés via des appels d'offre incluant des exigences de cyberrésilience
Nouveaux segments de clientèle pouvant être intéressés par une proposition de valeur cyberrésiliente</td>
</tr>
<tr>
<td>Ressources clés

Matériels et logiciels mis à jour, sensibilisation et formation des collaborateurs, etc.</td>
<td>Canaux

Référencement et gestion de réputation

Innovation de structure de la production</td>
</tr>
<tr>
<td colspan="3">Structure des coûts
Augmentation des coûts (avec les investissements réalisés au titre de la cyberrésilience), retour sur investissement (ROI)</td>
<td colspan="2">Flux de revenus
Monétisation de la cyberrésilience via ses avantages comparatifs, y compris innovations de produit, de service ou de process</td>
</tr>
</table>

Si l'entreprise gagne en cyberrésilience, le *business model* gagne aussi en valeur. Il y a alors des avantages comparatifs à rentabiliser.

1) Rentabiliser la cyberrésilience dans le modèle d'affaires

À un stade de maturité avancé, l'entreprise prend conscience que son approche proactive par rapport au risque cyber peut constituer un avantage comparatif qu'elle peut valoriser. « *Cette exposition aux risques devient (…) une source d'avantages concurrentiels* »[65]. Tout l'enjeu est alors de faire de sa capacité de cyberrésilience un élément différenciateur sur le marché.

Nicolas ARPAGIAN
ORANGE CYBERDEFENSE

« Il faut faire de la cyberrésilience un élément de création de valeur de l'activité des entreprises en identifiant le risque ainsi que les données et la valeur de celles-ci.. »

[64] Guy-Philippe Goldstein et Philippe Trouchaud, "La valeur de l'entreprise à l'épreuve des cyber-attaques", HBR France, 9 mai 2018.
[65] Rami Feghali, Guy-Philippe Goldstein, Philippe Trouchaud, « Le défi de l'entreprise cyberdigitale, allier innovation et maîtrise des risques », HBR France, 29 mars 2018.

L'entreprise cherchera à valoriser son investissement matériel et humain visant à protéger ses actifs-clefs mais aussi d'autres éléments immatériels comme le schéma d'organisation résiliente, la réactivité de la gouvernance face au cyber-risque et l'intégration de ce risque dans le cycle de vie de l'entreprise.
Cette approche par la création de valeur est d'autant plus importante que les investissements exigés par la résilience peuvent être très onéreux (tous actifs confondus). Il faut optimiser la valeur de ces investissements et réduire l'exposition aux risques.

« L'analyse économique doit permettre de dégager également des opportunités de création de valeur en particulier sous un angle compétitif de mieux-disant de cyber-sécurité qui pourront intéresser les autres parties prenantes, y compris les actionnaires, ayant une vue de long terme et pour lesquels la qualité des opérations joue un rôle primordial »[66].

La cybersécurité peut être valorisée par tout mode qui va permettre de se démarquer de la concurrence ou d'apporter une nouvelle proposition de valeur au client : différenciation, performance, innovation, etc. Cela pose la question du mode de rémunération (faire payer l'investissement cyber, le proposer comme un service, l'intégrer à la valeur du produit/service...) mais aussi celle de la détermination du prix (*pricing*) pour générer de nouveaux revenus.

a) La cyberrésilience comme facteur de différenciation

Si la mise en conformité (*compliance*) de l'entreprise aux normes et aux réglementations (RGPD) relève du champ de la cybersécurité, elle peut, néanmoins faire partie des éléments à valoriser, auprès de ses partenaires et clients, comme facteur différenciant et/ou comme garantie. Elle permet de renforcer la réputation de l'entreprise par des garanties démontrables de résilience telles que les certifications. Ainsi, la certification 27001, qui atteste la mise en place d'un Système de management de la sécurité de l'information (SMSI) efficace et construit sur la base de la norme internationale de référence, offre une garantie majeure aux clients. Certes, à mesure que la certification se généralise dans les entreprises, son avantage différenciant diminue mais elle reste un facteur important dans la construction d'un avantage comparatif. On a observé trois fois plus de certifications en 2018 par rapport à l'année précédente, portant à 223 le nombre de certifications couvrant 925 sites au total. On observe la même évolution au niveau mondial où les certifications sont passées de 39 500 en 2017 à 60 000 en 2018 selon l'AFNOR.

b) La cyberrésilience comme facteur de confiance (valorisation boursière)

Les entreprises qui démontrent leur capacité à gérer une crise, en retrouvant une activité normale affichent, parfois, de meilleures performances et bénéficient alors d'une prime de confiance : enrichissement de l'expérience, capacité du dirigeant d'entreprise à emmener les collaborateurs dans la reprise de l'activité, proximité avec les partenaires-clefs directs et indirects dans la gestion de la crise sont autant d'éléments qui contribuent à la confiance et qui peuvent, là aussi, peser dans la valorisation des actifs de l'entreprise.

Les entreprises leaders en matière de cyberrésilience sont celles qui sont « *plus performantes que les autres en ce qui concerne le nombre d'incidents de sécurité, la rapidité d'identification des incidents, le temps de rétablissement après une attaque et l'étendue des dommages causés par ces attaques* »[67].

Pour des entreprises cotées, la cyberrésilience est indispensable pour restaurer la confiance et retrouver de la valeur en bourse.

c) La cyberrésilience valorisée comme facteur d'innovation

Enfin, en intégrant la sécurité dès la conception, c'est-à-dire directement dans le code source d'une application ou d'un site web par exemple (ce qu'on appelle *Security by Design*), on gagne évidemment du temps : si un code n'a pas été sécurisé à la conception, le temps nécessaire pour le faire après sera plus long ; la démarche peut aussi être un vecteur d'innovation.

Aujourd'hui avec une connectivité croissante des objets, des appareils ou des machines, « *tous les acteurs sont attentifs au Security by Design pour maintenir les marchés ou en conquérir de nouveaux : tout se jouera sur la confiance, qui permet aux utilisateurs d'accepter d'adopter le produit. Le 'Security by Design' produit un avantage compétitif»*[68].

[66] « Cyber-risques : enjeux, approches et gouvernance", Ifaci, juin 2018.
[67] Bilan 2019 de la cyberrésilience, Accenture, octobre 2019.
[68] « Security by Design, un avantage compétitif pour les entreprises », La Tribune, 21 septembre 2019.

La recherche d'alternatives dans les process et les méthodes pour assurer la continuité de l'activité conduit aussi à de réelles innovations. On le voit, par exemple, dans l'automobile connectée, où la prise en compte du cyber-risque dans la conception d'un véhicule apporte de l'innovation dans la recherche de solutions.

2) Repenser le *business model* à partir de la cyberrésilience

Au-delà de la rentabilisation des avantages comparatifs issus d'une posture cyberrésiliente, un second schéma apparaît où la cyberrésilience amène l'entreprise à faire évoluer son *business model* non pas tant pour modifier son activité (produit/service) que pour inventer des alternatives à son exécution. Le passage des restaurateurs, pendant la crise sanitaire, d'une logique de service à table à une logique de livraison/vente à emporter est un exemple d'exécution alternative.

Dans ce cas de figure, la cyberrésilience, en tant que choix stratégique, sera poussée jusqu'à réinventer l'entreprise et son modèle économique.

Pour l'heure, on n'observe pas de remise en question notable du modèle d'affaires par la cyberrésilience. Mais il y a de plus en plus de modèles qui se disent résilients par rapport à un ensemble de risques, et notamment le risque cyber.

Faire de la cyberrésilience un levier de compétitivité et de transformation du modèle d'affaires pourrait donc être une prochaine étape de la cyberrésilience.

En effet, il ne suffit pas de s'armer des dernières cyber-technologies pour améliorer son modèle d'affaires. Dans l'innovation ou la transformation des modèles d'affaires, la technologie est juste un préalable ou un premier vecteur. Les entreprises créent une modèle économique puissant lorsqu'elles combinent les technologies et les nouveaux usages sur leur marché.[69]

[69] Building resilience, an introduction to business models, Chartered Global Management Accountant (CGMA) Report, Juillet 2013.

En conclusion, la cyberrésilience ne se décrète pas. Elle n'est ni une quête inaccessible ni un état de grâce. C'est une posture travaillée et entretenue qui repose sur des outils humains et organisationnels véhiculés par une culture au sein de l'entreprise.

Cette culture est le fruit d'un apprentissage sur le long terme qui n'est pas encore enraciné dans les différents corps de la population active à ce jour. À titre d'exemple, les générations nées depuis le début des années 1990 qui sont *digital natives* sont rompues aux outils numériques, mais pas elles ne le sont pas à la sécurité, notamment la sécurité des données personnelles : elles acceptent, par exemple, sur les sites Internet, des cookies en aveugle.

La sécurité numérique et la résilience seraient largement facilitées si une culture du numérique était transmise dès le plus jeune âge.

Seules les entreprises transmettent les bonnes pratiques du numérique, parfois de manière coercitive alors que le cadre domestique n'offre aucun support sauf en cas de confrontation à la cybermalveillance.

La culture de la cyberrésilience n'en est qu'au stade de la protoculture et sera encore profondément bousculée avec l'intelligence artificielle et l'ordinateur quantique qui transformeront les cyberattaques et modifieront probablement les rapports de force entre hacker/hacké, attaquant/attaqué.

In fine, la cyberrésilience est la réponse mais elle n'est pas la recette miracle au sens de boîte à outils, de solution clef en main qui dispenserait d'une stratégie voire d'une transformation. Elle n'est pas, *a contrario*, une démarche complexe, opaque et inaccessible : la cyberrésilience reste, en effet, de l'humain ! Elle est culturelle et repose sur des outils non technologiques, collaboratifs et organisationnels. C'est peut-être cela la bonne nouvelle pour les entreprises !

RECOMMANDATIONS

Comment aider les entreprises à passer de la cybersécurité à la cyberrésilience ?

A) RECOMMANDATIONS EN FAVEUR DES ENTREPRISES

1) À destination des dirigeants de TPE

1. Rendre la thématique cyber et ses enjeux accessibles et intelligibles aux TPE
2. Activer le levier de la cyberassurance pour faire entrer les TPE dans une prise de conscience
3. Guider les dirigeants de TPE par des rencontres « *one-to-one* » (avec des conseillers CCI par exemple)
4. Concevoir et proposer des diagnostics TPE de cyberrésilience et des tests d'intrusion (en lien avec l'ANSSI et la Gendarmerie nationale)
5. S'appuyer sur les écosystèmes locaux d'échanges entre entreprises (type Plato[70]) pour accompagner les TPE dans la sensibilisation et la protection des systèmes d'information et des interconnections

2) À destination des PME/ETI

1. Inciter les entreprises à pratiquer des tests d'intrusion, des diagnostics et des *crash-tests* pour devenir résilients face au risque cyber (tout comme on réalise des tests de sécurité incendie)
2. Organiser une prise en main de la problématique cyber par palier : prise de conscience (*coaching*) pour le dirigeant, entraînement (*training*) pour l'adjoint direct en charge du risque cyber (DRH, DAF, etc.) et formation pour les salariés de l'entreprise selon la taille de celle-ci

   - *Formation aux gestes "secouristes IT" avant de s'orienter vers l'équipe IT*
   - *Formation à la culture numérique et aux implications juridiques et opérationnelles des usages cyber (CGU, cookies, etc.)*

3. Activer le levier de la certification et de l'audit pour faire entrer les PME dans un degré de conscience cyber plus élevé
4. Inciter les entreprises à réviser leurs contrats d'assurance pour y inclure le risque cyber ou en vérifier la clause (soutenir la démarche de l'Autorité de contrôle prudentiel et de résolution - ACPR) dans sa proposition de clarification de la position des compagnies d'assurance et de redescendre tous leurs contrats sur des bases de couverture du risque cyber)
5. Faire une large campagne sur la mise à niveau des standards (obligations réglementaires) et des outils (mises à jour logicielles et configuration) de cybersécurité ; les normes et certifications peuvent être obligatoires mais donnent surtout accès à des marchés pour la plupart des ETI
6. Faciliter la mise en réseau des RSSI pour les PME

   - *Conclusion de partenariats de mutualisation des ressources et d'informations afin de pallier la pénurie de talents : la lutte contre des cybermenaces sophistiquées nécessite, d'abord et avant tout, des processus matures et des professionnels de la sécurité efficaces et dédiés 24h/24, 7j/7*

[70] Plato (CCI Ile-de-France) est un réseau qui rassemble des dirigeants de TPE PME sur un même territoire avec parrainage de cadres de grandes entreprises.

7. Mutualiser les expériences d'entreprises en matière de cyberrésilience et changer la culture du secret qui entoure l'attaque cyber (qu'elle ait ou non aboutie)

8. Fédérer des écosystèmes d'échange d'expérience à l'échelle industrielle (sur le modèle du Cluster Security Valley)[71]

B) RECOMMANDATIONS À DESTINATION DES CHAMBRES DE COMMERCE ET D'INDUSTRIE (CCI)

1. Faire monter en compétence les collaborateurs des CCI et notamment les conseillers entreprise sur la cybersécurité et la cyberrésilience

2. Renforcer le dispositif créé par CCI France destiné à la certification de conseillers et conseillères «Référent cybersécurité en TPE/PME» avec l'appui de l'ANSSI et de la DGE-SISSE, en introduisant la démarche de cyber-résilience.

3. Aller à la rencontre des dirigeants de TPE souvent accaparés par leurs fonctions en profitant de l'essor des visioconférences ou du *coaching* afin de démythifier le cyber risque ; dans ces rencontres, cibler prioritairement les entreprises qui n'ont pas de DSI

4. Pratiquer des tests d'intrusion et des campagnes de *phishing* (en partenariat avec les autorités publiques comme l'ANSSI et des porteurs de solution) à la demande des dirigeants pour donner corps à la prise de conscience

5. Proposer des sessions de prise de conscience ciblées par taille et par disponibilité de responsabilité :

   • *Sensibilisation du dirigeant* **:** *sur 1 à 2 heures*
   • *Sensibilisation du collaborateur délégué à la cybersécurité (RH ou DAF)* **:** *sur 2 à 3 heures*
   • *Sensibilisation des collaborateurs de l'entreprise via des modules progressifs (fonction du nombre de participants) : d'une demi-journée à une journée*

6. Apporter un soutien méthodologique et un appui aux entreprises afin de catégoriser et de valoriser les données, autrement dit aider à l'exploitation de données (*Data Mining*) qu'il s'agisse de données ouvertes (*open data*), de données interopérables, d'entrepôts de données[72] ou encore de données sensibles[73] ; cet appui pourrait se faire sur le modèle Digipilote[74]

7. Inclure la cyberrésilience dans toute la chaîne d'intelligence des risques (climatiques, industriels, incendie, inondation, terrorisme, cyber, économiques) et intégrer les compétences des CCI sur la maîtrise des risques dans cette approche dite de sécurité globale

8. Organiser la sécurité économique des territoires dans cette logique de sécurité globale (telle que définie dans le Plan d'action « Relance » de CCI France) pour une « *résilience en coopération* »[75]

[71] Pôle d'expertise dédié à la sécurité globale (dont cyber) dont l'objet est d'anticiper les crises et renforcer les mesures de protection et les capacités de résilience collective. La CCI Paris-Ile-de-France en est membre.
[72] Grâce aux données liées (linked data) en offrant une certification d'interopérabilité sur différents standards (IoT, GPS, Imprimantes 3D, etc.).
[73] En fournissant des grilles de niveau de cryptage pour les TPE.
[74] Conçu par CCI France et les CCI, il s'agit de la première plateforme numérique de pilotage et de management opérationnel de la transformation digitale de l'entreprise.
[75] Réussir la relance, CCI France, juin 2020.

C) RECOMMANDATIONS À DESTINATION DES POUVOIRS PUBLICS

1. Favoriser l'émergence des réseaux de sécurité au niveau des directions d'entreprise, des RSSI
2. Renforcer l'effort d'Identification du guichet unique ACYMA pour déclarer une cyberattaque
3. Renforcer la coopération européenne en matière de cybersécurité d'entreprise et mettre en place des coopérations internationales de cyberdéfense intégrant l'approche cyber résilience
4. Sensibiliser et accompagner les écosystèmes et *shadow IT* des entreprises dans la sécurisation des relations économiques, juridiques et opérationnelles
5. Transmettre une culture de sécurité dans les usages informatiques dès le plus jeune âge à travers l'éducation nationale et au-delà des cercles d'experts par un décryptage et un accompagnement des politiques publiques de concert avec le CyberCercle.

ANNEXE 1

Le cadre juridique de la cybersécurité

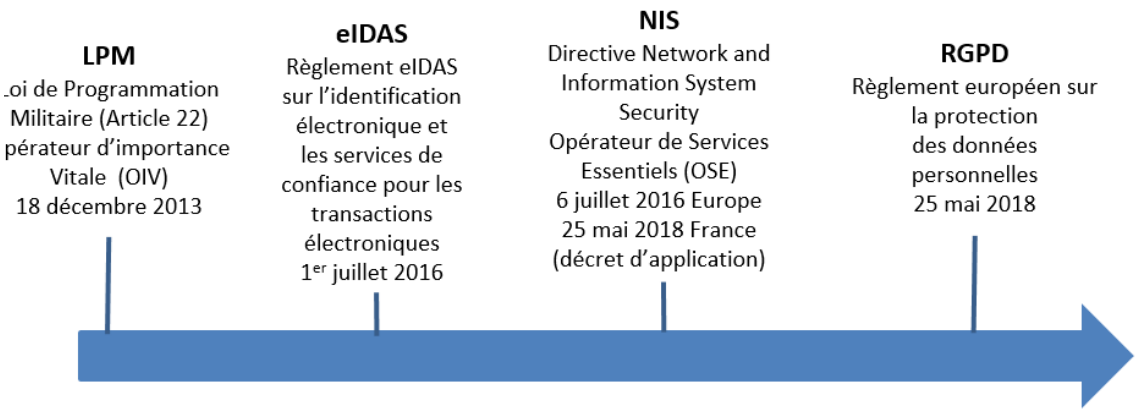
Il existait, avant 2018, des mesures destinées à « *assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne* »[76]. La Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité[77] a pour vocation de sécuriser les Opérateurs d'importance vitale (OIV).

Elle crée ainsi deux nouvelles catégories d'acteurs : d'une part, les Opérateurs de services essentiels (OSE) et, d'autre part, les Fournisseurs de service numérique[79] (FSN).

Cette transposition de la Directive « NIS » (National Information Security) « *permettra à l'UE de faire face aux risques de sécurité dans le monde numérique pour les années à venir. Cette législation est une pierre angulaire pour que l'Europe devienne un acteur mondial en matière de cybersécurité. Les consommateurs ainsi que l'industrie doivent pouvoir faire confiance aux solutions informatiques* »[80].

Par ailleurs, le *Cybersecurity Act*[81], adopté au printemps 2019 par le Parlement européen, offre un « *cadre de certification de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification* »[82]. Le Règlement donne notamment toute sa place à l'Agence européenne chargée de la sécurité des réseaux et de l'information (*European Union Agency For Cybersecurity* ou ENISA), notamment pour la délivrance de certificats qui bénéficieront d'une reconnaissance mutuelle au sein de l'Union européenne (UE).

Chronologie des réglementations sur la cybersécurité applicables en France



Source : Le coût des attaques et les réglementations stimulent la cybersecurité, Eric Debray, 9 avril 2019

[76] Cyber-sécurité : loi n°2018-133 du 26 février 2018 « sécurité des réseaux et des systèmes d'information », Linklaters, 2 mars 2018.
[77] Adoptée le 15 février 2018 et promulguée le 26 février 2018 transpose la Directive (UE) 2016/1148 du 6 juillet 2016, plus connue sous l'acronyme « NIS » (National Information Security) est directement inspirée de la loi n°2013-1168 du 18 décembre 2013 (dite « loi de programmation militaire »).
[78] Les opérateurs de services essentiels sont définis par l'Article 5 de la loi n° 2018-133 comme toute entité publique ou privée qui fournit un « service essentiel au maintien d'activités sociétales et/ou économiques critiques, tributaires des réseaux et des systèmes d'informations et dont le service serait susceptible d'être gravement affecté en cas d'incident de sécurité sur les réseaux ». Ces opérateurs seront désignés en France par le Premier ministre, dans des secteurs divers comme par exemple l'énergie, le transport, la banque, les infrastructures de marchés financiers, la santé et les infrastructures numériques. Cette liste est actualisée tous les deux ans.
[79] Les fournisseurs de services numériques désignent « les personnes morales fournissant un service numérique » et recouvrent trois types de services numériques» (Art. 9 de la loi n° 2018-133).
[80] « Cybersecurity Act, ou comment répondre plus efficacement à la cybermenace en Europe », Leading by Trust.
[81] Règlement d'application directe adopté par le Parlement européen le 12 mars 2019 puis par le Conseil de l'Union européenne le 7 juin.
[82] Voir Cybersecurity Act, ANSSI.

ANNEXE 2

Cyberattaque en entreprise : les différentes étapes de réaction

1. Premiers jours et semaines - Détection et réponse à la crise	
a.	Détection et identification rapide d'une cyberattaque majeure
b.	Classification de la menace
c.	Mise en place d'un centre de coordination pour une réponse urgente
d.	Notification d'alerte rapide
e.	Plan d'action opérationnel pour les forces de l'ordre ou autorités compétentes
f.	Enquête et analyse
g.	Fermeture du protocole d'intervention d'urgence

On retrouve, dans ce premier temps, les sept étapes de réponse aux cyberattaques définies par Europol. Le protocole d'Europol détermine « *les procédures, les rôles et les responsabilités des acteurs clés à la fois dans l'Union européenne et au-delà* ». Il permettra aussi de sécuriser « *les canaux de communication et les points de contact ouverts 24h/24, 7j/7, dédiés aux échanges d'informations importantes* ». L'intérêt de cette procédure est d'être applicable à tout type d'attaque sur toute cible.

Une première pratique pour lutter efficacement contre les cybermenaces sophistiquées consiste à détecter les intrusions en moins d'une minute, analyser et comprendre les menaces en moins de 10 minutes et contenir et éjecter le cyber-adversaire de l'environnement en moins de 60 minutes : c'est la règle « 1-10-60 ». Cette règle est optimum mais elle ne concerne que la jugulation de l'attaque cyber et non sa résolution, voire sa résorption.

2. Semaines et mois suivants – Gestion des impacts liés	
a.	Mise en place d'infrastructures ou activités temporaires
b.	Préparation des procédures juridiques
c.	Traitement des procédures réglementaires et vérifications
d.	Gestion des relations avec les clients, partenaires et autres parties prenantes

Cette phase correspond à une phase de relance de l'activité de l'entreprise à l'instar de ce que connaît une *start-up* en phase de création (structuration, investissement et gestion). Il s'agit généralement de gérer les dégâts immatériels pouvant représenter jusqu'à 40 % des dommages causés par une cyberattaque[83].

[83]"Beneath the surface of a cyberattack - A deeper look at business impacts", Deloitte, 2016.

3. Mois et années suivants – Rétablissement de l'activité durable de l'entreprise
a. Réparation des dégâts causés à l'entreprise
b. Refonte des procédures et des actifs
c. Investissement dans le renforcement des programmes de cybersécurité

ANNEXE 3

Les gestes barrière de cybersécurité : se prémunir face aux attaques[84]

Hameçonnage (*Phishing*)

1. Méfiez-vous des e-mails ou des fichiers envoyés par des inconnus. Évitez de cliquer sur des liens dans des e-mails non sollicités, et soyez particulièrement attentifs aux pièces jointes. Consultez les 10 règles de base de la sécurité sur l'Internet de l'ANSSI.
2. En cas de doute, fermez l'e-mail, recherchez et rendez-vous par vous-même sur le site de confiance afin d'accéder à la section nécessaire.
3. Utilisez des sources fiables - tels que des sites gouvernementaux légitimes - pour obtenir des informations à jour et factuelles.
4. Orientez-vous vers des sociétés reconnues et de confiance pour l'achat de produits de première nécessité. Vérifiez l'authenticité de l'organisme qui vous contacte ou sur le site duquel vous faites une démarche.
5. Ne révélez aucune information personnelle ou financière dans des e-mails, et ne répondez pas à ceux qui sollicitent de telles informations.
6. Avant d'effectuer un don, vérifiez l'authenticité de l'organisme caritatif.
7. Activez l'authentification à deux facteurs ou plus, ou des technologies de sécurité physique sur l'ensemble de vos sites compatibles.
8. Utilisez un gestionnaire de mots de passe reconnu et de confiance, et générez des mots de passe uniques et complexes sur les sites ne prenant pas en charge plus d'un facteur. N'utilisez jamais le même mot de passe sur plusieurs sites.
9. Soyez attentif aux questions de récupération de mots de passe - utilisez des informations qui ne peuvent pas être devinées ou recherchées, ou utilisez votre gestionnaire de mots de passe pour en recréer un de façon aléatoire.

Logiciels malveillants et piratage

1. Ne faites pas confiance à des inconnus vous demandant des informations sur votre entreprise.
2. Installez un antivirus réputé pour votre plateforme, et veillez à ce qu'il soit constamment à jour.
3. Gardez les logiciels et le système d'exploitation de votre ordinateur à jour.
4. Attention aux logiciels gratuits ; parfois, cette gratuité cache quelque chose, notamment en ce qui concerne les applications disposant d'accès critiques telles que les VPN.
5. Ne soyez pas le maillon faible de votre organisation : vérifiez que votre connexion au réseau de votre entreprise est sécurisée, et signalez toute activité suspecte, comme vous le feriez en travaillant au bureau.
6. Si vous êtes responsable des systèmes d'information d'une organisation, assurez-vous de bien appliquer les principes du modèle *Zero Trust* qui consiste notamment à ne faire confiance à personne. Vérifiez que les hackers ne peuvent pas pénétrer votre réseau sécurisé en profitant des failles créées par les employés travaillant à distance.
7. Concevez votre architecture logicielle et réseau en mettant en place des principes de contrôle des identités renforcés. En utilisant l'authentification en continu et des mécanismes stricts de vérification d'identité, vous compliquez considérablement la tâche des hackers, car ces derniers auront beaucoup de mal à se faire passer pour des membres du personnel, même si leurs identifiants venaient à fuiter.

[84] Source : Marc Rogers, « Comment la pandémie du COVID-19 a radicalement changé le monde de la cybersécurité », 9 avril 2020, https://www.silicon.fr

BIBLIOGRAPHIE

RAPPORTS/ÉTUDES/LIVRES BLANCS

- 2020 Global Threat report, Crowdstrike, 2020
- Agilité & sécurité numériques - Méthode et outils à l'usage des équipes projet, ANSSI, 2018
- Baromètre 2019 des risques émergents pour la profession de l'assurance et de la réassurance, Fédération Française de l'Assurance, 2019
- Baromètre de la cyber-sécurité des entreprises, CESIN & OpinionWay, janvier 2020
- Building Resilience: An introduction to business models, CGMA, Buzz eSanté, 2013
- Cartographie du système d'information - Guide d'élaboration en 5 étapes, ANSSI, 2018
- Cybersécurité des systèmes industriels - cas pratique, ANSSI, 2012
- Etat des lieux d'Internet : sécurité (2019, Une année passée au crible), AKAMAI, 2019
- Global Threat Intelligence Report, NTT Security, 2019
- Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures, ANSSI, 2017
- La cybersécurité à l'usage des dirigeants, CLUSIF OSSIR, Livre blanc, 2020
- La fin de la cybersécurité - Réagir face aux menaces, Harvard Business Review Avril-mai 2019
- La Résilience organisationnelle : Exploiter l'expérience, saisir les opportunités, BSI, 2016
- Le cognitif moteur de la transformation digitale : IoT + Cognitif : le carburant pour alimenter vos services digitaux, Serge Bonnaud et Christophe Didier, IBM, 2017
- Le Livre blanc du Cyberday 2020, Veille Magazine en partenariat avec EGE/AEGE Club Cybersécurité, 2020
- Maîtrise du risque numérique l'atout confiance, ANSSI - AMRAE, 2020
- Placement des charges applicatives dans l'environnement informatique : ce qui différencie les gagnants des perdants, Un livre blanc IDC parrainé par Dell EMC, Ashish Nadkarni et Richard L. Villars, 2019
- Revue Stratégique cyberdéfense, SGDSN, 1er février 2018
- Sécurité numérique des collectivités territoriales : L'essentiel de la réglementation, ANSSI, 2020
- Synthèse de la journée d'étude du GFII : « Données culturelles et Linked Open Data : valoriser le patrimoine public dans le web des données », Groupement français de l'Industrie et de l'Information (GFII), 26 mars 2013, Maison de l'Europe
- The Cost of Cybercrime - Ninth annual cost of Cybercrime Study (Unlocking the value of improved cybersecurity protection), Ponemon Institute, Accenture Security, 2019
- Ultimate Guide to Getting Started with Application Security, Veracode, 2018

NOTES

- 3 projets de gestion de crise, E guide, 2020, LeMagIT
- A Risk-Adaptive Approach - Realizing the Gartner Carta Framework In Present-day Security, Forcepoint, Gartner, 2017
- Bilan 2019 de la Cyber-résilience, Accenture Security, 2029
- Comment créer un plan de cybersécurité efficace, Malawarebytes, 2019
- Coronavirus: Five strategies for industrial and automotive companies, Joe Dertouzos, Heike Freund, Michael Mischkot, Asutosh Padhi et Andreas Tschiesner, McKinsey & Company, Mars 2020
- Cybersecurity tactics for the coronavirus pandemic, Jim Boehm, James Kaplan , Marc Sorel, Nathan Sportsman, et Trevor Steen, McKinsey & Company, Mars 2019
- Évolution du rôle des sauvegardes à l'ère des ransomware, VEEAM, Avril 2018
- Intelligence Artificielle et Cybersécurité : duo gagnant, E-handbook, LeMagIT, 2019
- IoT et Blockchain combinés: Quels sont les Usages?, Serge Bonnaud et Christophe Didier, Watson IOT & IBM, 2017
- La Sécurité applicative, Veracode, 2020
- Le Directeur Cybersécurité décrypté..., CESIN, 2020
- Le stockage objet dans le cadre d'une stratégie de protection cloud hybride, VEEAM, 12 novembre 2019
- Les Grandes tendances de la cybersécurité, Wolters Kluwer, Lamy, 2019.
- Protection généralisée : Permettre le travail sécurisé de n'importe où, Malawarebytes, 2020
- Rapport d'information fait au nom de la délégation aux entreprises sur l'accompagnement de la transition numérique des PME : comment la France peut-elle rattraper son retard ?, Pascale Gruny (rapporteur), Sénat, juillet 2019
- The Fourth Annual Study on the Cyber resilient organization, Ponemon Institute, IBM Security, 2019

ARTICLES

- Arthur Le Denn, Les réseaux informatiques des entreprises sont fragilisés par les objets connectés de leurs employés, L'Usine Digitale, 27 février 2020
- Chris Butler, La résilience d'entreprise, au-delà de la compétitivité, Les Échos, 15 octobre 2018
- Cyberguerre : La Cyber-résilience n'est pas le vaccin mais un bon contrepoison, Yannick Chatelain, Forbes France, 5 février 2019
- Dauphiné André, Provitolo Damienne, « La résilience : un concept pour la gestion des risques », Annales de géographie, 2007/2 (n° 654)
- La cyber-résilience devient un impératif business, Éric Boulay, Solutions numériques, 11 mars 2019
- Rémy Teston, Baromètre de la confiance des Français dans le numérique, ACSEL, 2 mars 2020

VIDÉOS

- CCI Entreprendre : Développer vos capacités de résilience
  https://www.youtube.com/watch?v=wJVS7HDDA1M
- Jérôme Barthélemy : La sérendipité : l'art de trouver ce que l'on ne cherchait pas
  https://www.youtube.com/watch?v=Egca7j76efs
- Philippe Gattet : La résilience : ces entreprises qui surmontent de graves crises
  https://www.youtube.com/watch ?v=U8BbgOM-nMM
- Philippe Gattet : Comprendre la sérendipité : quand le hasard ne doit rien au hasard
  https://www.youtube.com/watch?v=R_zcyxXf4MQ


CHAMBRE DE COMMERCE
ET D'INDUSTRIE
1er ACCÉLÉRATEUR DES ENTREPRISES
CCI PARIS ILE-DE-FRANCE