ÉTUDE BESSÉ
NOVEMBRE 2020

Crise cyber : Quel impact sur la valorisation des entreprises non cotées ?

BESSÉ
CONSEIL EN ASSURANCES

Pierre Bessé
Président de Bessé

La généralisation du télétravail engendrée par la crise sanitaire a renforcé d'évidence la porosité des entreprises au risque cyber, ouverture des systèmes d'information et management à distance en sont sans doute les deux principales causes. Une porosité qui risque de s'accroître véritablement avec le déploiement désormais acté de la 5G en France… Ayant un impact à la fois stratégique, technique et financier, les attaques cyber affectent la viabilité des entreprises en France.

Pour autant, selon l'étude que nous avons réalisée l'an dernier, seuls 37 % des dirigeants d'ETI s'estimaient prêts à faire face à une crise cyber !

De la même manière que le monde n'était pas prêt à faire face à une pandémie au début de cette année, le risque cyber n'est-il pas, encore aujourd'hui, vraiment sous-estimé ? Ses conséquences ne seraient-elles pas, tout autant, voire encore plus désastreuses en affectant des entreprises déjà fragilisées par la crise que nous traversons ?

Hier, nous ne prenions pas au sérieux ceux qui, comme Bill Gates, alertaient en 2015 sur le risque d'une pandémie mondiale. Aujourd'hui, les nombreuses mises en garde des experts en cyber-sécurité restent, non pas lettre morte, mais ne sont pas prises à la hauteur de l'importance qu'elles représentent. Pourtant, les hackings se multiplient, causant souvent des millions d'euros de dommages. Personne n'est aujourd'hui à l'abri d'une attaque, grands groupes, PME, ETI ou organisations publiques, comme l'attestent de récents cas qui nous concernent plus directement dans l'industrie, le transport maritime, les médias, le secteur de l'assurance…

Je pense que ces signes avant-coureurs sont aujourd'hui au risque cyber, ce qu'est la grippe saisonnière à une pandémie. En effet, ces évènements n'ont pas mis à genoux ces entreprises, mais les ont perturbées quelques semaines.

Mais n'est-il pas envisageable qu'une attaque cyber, demain, dont pourrait être à l'origine un groupe terroriste, une organisation criminelle, un état hostile, un concurrent très virulent, puisse frapper un écosystème économique dans son ensemble, voire un pays tout entier ?…

D'un point de vue purement technologique, une telle crise est très probable.
Elle serait plus immédiate, beaucoup plus violente qu'une pandémie, sans doute plus courte… En revanche, dans l'intervalle, que de dégâts sur des organisations déjà fragilisées.
Il est donc impératif d'imaginer tous les scénarios de crises pour mieux s'y préparer.

C'est pourquoi, sans tomber dans le piège du catastrophisme, l'étude que nous avons réalisée cette année s'est concentrée sur les entreprises non cotées. Celles-ci sont fragilisées comme les autres par la crise sanitaire et je pense qu'elles ne sont pas totalement préparées pour faire face à une attaque cyber. Parce qu'elles n'y croient pas ? Parce qu'elles en sont conscientes, mais qu'elles ont d'autres priorités ?

Cette nouvelle étude souligne les conséquences inéluctables d'une attaque de ce type sur une entreprise et met en avant l'importance de la résilience, le rôle du management, et aussi de l'assurance sur le risque résiduel, tout en prenant en compte les effets sur leur réputation.

Je remercie sincèrement Guy-Philippe et tous les contributeurs à notre réflexion pour leurs analyses de grande qualité et ne doute pas de l'intérêt que ce contenu aura pour vous.

Excellente lecture !

L'état de la menace en quelques chiffres clés

76 %

des dirigeants d'ETI déclarent avoir subi au moins une incidence cyber en 2017.

Source : Étude Cyber Bessé - PwC

→

90 %

des entreprises françaises ont été victimes de cyber-attaques en 1 an.

Source : étude Forrester 2020, commandée par Tenable et menée auprès de 800 RSSI dont 104 français

↓

Ces attaques ont entraîné des dommages très divers :

une perte de productivité

→ pour **38 %** des RSSI français

des pertes de données clients

→ **33 %**

...et des pertes de données employés

→ **32 %**

Plus de

1100

victimes d'attaques par rançongiciel en France depuis le début de l'année 2020 (dont 26 % de particuliers).

Source : www.cybermalveillance.gouv.fr

5200

milliards de dollars.

Coût de la cyber-criminalité estimé par l'ONU pour l'économie mondiale entre 2020 et 2025.

Octobre 2020

12 %

des entreprises interrogées ont connu des attaques par rançongiciel, le vecteur d'attaque le plus préoccupant, avec pour 38 % d'entre elles un impact fort.

Enquête CLUSIF 2020
Entreprise de plus de 100 salariés

80 %

des entreprises françaises n'ont pas de plan de réponse aux incidents robustes : il est soit pas assez complet (24 %), soit pas assez formalisé (31 %), soit inexistant (25 %).

Source : IBM/Ponamon Institute

86 %

des entreprises sondées n'ont toujours pas souscrit de contrat cyber-assurance.

Enquête CLUSIF 2020
Entreprise de plus de 100 salariés

Caroline Ruellan
Présidente de Sonj Conseil

Docteur en droit privé et diplômée de la Harvard Law School, Caroline Ruellan est membre du Conseil de surveillance de Ardian France, membre de la Commission Consultative Epargnants de l'AMF, Présidente du Cercle des Administrateurs et Secrétaire général de l'Institut Aspen France. Auteure de « Droit commercial - Notions générales » (Dalloz, 2017), d'une chronique mensuelle dans Forbes et de nombreuses tribunes, notamment sur l'activisme actionnarial et la gouvernance, elle conseille les acteurs économiques, français et internationaux, en matière de gouvernance, stratégie, médiation et lobbying.

« Dans un monde en proie à l'inflation de l'information, le risque cyber ajoute à la complexité qui cerne le dirigeant en continu. »

Dans la cartographie des risques des entreprises, le risque cyber occupe une place particulière. À la croisée des technologies les plus sophistiquées, de l'intelligence économique et de la vie opérationnelle de l'entreprise, il ne s'inscrit dans aucune grille de lecture traditionnelle. Il constitue une crise aigüe appelant une gestion rapide et maîtrisée.
Il est donc essentiel de le « déconstruire » afin d'être en mesure de l'appréhender et d'en maîtriser autant que possible les conséquences nocives, redoutées par les entreprises – quelle que soit leur taille - et leurs dirigeants.

Une des particularités de ce risque résulte du fait que la cyber-attaque constitue une cyber-agression qui se rapproche plus du modus operandi militaire – le narratif « attaque » le rappelant – que d'une incursion économique ou boursière non désirée. Le dirigeant d'entreprise ne peut s'en remettre aux balises habituelles, devant agir hors-cadre en faisant fonctionner à plein son discernement.

La cyber-agression ne répond à aucun des codes conventionnels de l'affrontement : difficulté majeure d'identifier l'adversaire empêchant toute forme de dénonciation ou de saisine d'un régulateur, difficulté de concevoir une riposte quelle qu'en soit la forme, notamment réputationnelle. De son côté, le dirigeant ignore souvent les motivations de l'attaque, qui peut s'inscrire dans une stratégie plus large, un vol de données dans une bataille concurrentielle, une tentative de perturbation du lancement d'un produit innovant, une manifestation parmi d'autres dans un contexte de guerre économique entre deux pays ou encore, une contestation idéologique du core business de l'entreprise.

Par ailleurs, le client dont les données ont pu être dérobées ou altérées se considère à la fois victime de l'attaque subie par l'entreprise et victime de la négligence de cette dernière en ce qu'elle aurait échoué à préserver les informations qui lui ont été confiées. Le dirigeant endosse ainsi le double rôle, quelque peu paradoxal, de victime et de coupable, à l'égard de l'agresseur et du client. L'impossibilité d'identifier rapidement le pirate informatique augmente substantiellement la complexité de la gestion de crise, d'autant que l'inventivité des pirates informatiques rend impossible de prévoir où, quand et comment le risque cyber se réalisera.

Il se révèle extrêmement difficile pour l'entreprise et son dirigeant d'échapper

« Le dirigeant d'entreprise ne peut s'en remettre aux balises habituelles, devant agir hors-cadre en faisant fonctionner à plein son discernement. »

au procès en négligence car la réussite d'une cyber-agression signe par essence l'échec plus ou moins important des dispositifs de défense. S'agissant d'une obligation de moyens et non de résultats, l'entreprise doit donc rapporter la preuve qu'elle avait mis tout en œuvre pour faire face à une agression de cette nature.

Le rôle du dirigeant en amont de l'attaque est d'autant plus capital que l'inconnu est d'une magnitude importante. La vulnérabilité cyber, dont le conseil d'administration doit se saisir impérativement, exige ainsi une vigilance particulière. Il s'agit notamment de veiller à l'allocation d'un budget suffisant à la direction en charge des SI avec une mise en place d'une équipe dédiée compétente, à la sensibilisation continue des salariés au risque cyber, à la souscription d'une police d'assurance cyber, à la mise en place de stress-tests.

Son rôle en aval, quant à lui, se révèle vital. L'étude des comportements de marché et des consommateurs démontre que la confiance en l'entreprise qui réussit la gestion de « l'après-guerre », peut être restaurée. Ainsi, les dirigeants qui ont privilégié l'honnêteté, une communication intelligente ainsi que la transparence en mettant notamment en place une plateforme de dialogue avec les employés, les actionnaires et les consommateurs, ont pu être perçus comme diligents ex post facto.

Le défi des décisions complexes qui se posent au dirigeant lors d'une cyber-agression peut donc être énoncé dans les termes suivants : comment le processus décisionnel peut-il intégrer tous les éléments pertinents à la décision, dont certains sont par essence hypothétiques, voire inconnus ? Comment s'assurer de la pertinence de la décision et de son acceptabilité, constantes fondamentales de notre époque de redevabilité et de transparence ?
Le discernement semble être la clef de compréhension d'un paradigme délié des repères classiques auxquels le dirigeant pourrait se raccrocher. Force est d'admettre les limites des modèles modernes de prise de décision. Fondés sur la seule rationalité et la segmentation du savoir en respect de l'héritage de Descartes aux dépens de la pensée holistique de Pascal, ils ne permettent pas la prise en compte de la pensée complexe qui résulte des nombreuses zones d'incertitude et d'inconnu. Surtout, ils s'affranchissent de la capacité de l'individu à exercer un jugement imprévisible.

« Le dirigeant endosse ainsi le double rôle, quelque peu paradoxal, de victime et de coupable, à l'égard de l'agresseur et du client. »

Or, de façon contre-intuitive, la dématérialisation et la désincarnation de la cyber-agression placent l'humain en son centre, les capacités cognitives prenant le pas sur les compétences purement normatives. Certains en appellent à l'intuition comprise comme l'intelligence de l'émotionnel. Cependant, elle constitue une prise de conscience immédiate et individuelle et peut conduire à des erreurs d'appréciation. Nous lui préférons la notion de discernement, c'est-à-dire la faculté de « reconnaître » distinctement et d'arbitrer, notamment dans une situation de crise.

Dans un monde en proie à l'inflation de l'information, le risque cyber ajoute à la complexité qui cerne le dirigeant en continu. Le pouvoir et la légitimité n'appartiennent plus au sachant, à l'expert mais au dirigeant, tant public que privé, qui sait faire preuve de discernement en injectant notamment une vision et une faculté à appréhender des situations complexes.

L'étude que je vous invite à lire avec attention constitue sans aucun doute un précieux manuel d'aide au discernement dans le contexte du cyber risque.

En synthèse, ce qu'il faut retenir en **10 points clés**

1

Le risque cyber est stratégique et vital pour l'entreprise. La crise du covid-19 a révélé et amplifié l'accélération de la menace.

2

Le choc économique est généralement observé pour les entreprises cotées au vue de l'évolution de leurs cours de bourse.

3

Pour les entreprises non cotées, ce choc peut être évalué à l'aide de données clés telles que le score de défaillance et l'indicateur des jours de retard de paiement.

(Source : Altares - Dun & Bradstreet)

4

L'analyse de ces données pour un premier échantillon d'entreprises internationales non cotées montre que le risque de défaillance augmente en moyenne de 40 % à 50 % dans les trois mois après l'annonce d'un évènement cyber.

5

Sur l'échantillon des seules entreprises françaises, le risque de défaillance augmente en moyenne de 80 % sur la même période, chiffre étayé par une augmentation de 55 % du nombre de jours de retard 6 mois après.

6

Une première estimation de la dégradation de la valeur patrimoniale consécutive à cette augmentation du risque de défaillance ressort de l'ordre de 8 à 10 % de la valorisation de l'entreprise.

7

L'analyse des cas observés confirme que les entreprises non cotées les plus fragiles sont celles qui n'ont pas encore mis en place de politique de gestion des risques et de cyber-résilience.

8

Ces premiers tests sur un échantillon limité renforcent l'hypothèse déjà émergente de l'impact significatif des évènements cyber sur la stabilité économique et la valorisation de l'entreprise non cotée.

9

Parce qu'il touche directement à la réputation, l'actif immatériel le plus précieux, ce risque doit faire l'objet d'un processus de gestion et de communication approprié.

10

Face à ce risque systémique, la cyber-résilience organisée et démontrée deviendra un atout concurrentiel créateur de valeur pour l'entreprise au sein de son écosystème.

oints clés

PARTIE 01

L'impact de la crise cyber sur la valorisation des entreprises non cotées

01

Guy-Philippe Goldstein

Guy-Philippe Goldstein est enseignant à l'Ecole de Guerre Economique, contributeur au journal académique de l'Institute for National Security Studies à Tel-Aviv sur les questions de cyber-puissance et cyber-défense, et advisor pour PwC ainsi que pour ExponCapital, un fonds de Venture Capital. Il est également l'auteur de romans d'anticipation sur les questions cyber ainsi que d'un essai, « ***Cyber-défense et Cyber-puissance au XXI^{ième} siècle*** » (Balland, 2020)

La crise du Covid-19 : un révélateur de l'accélération de la menace

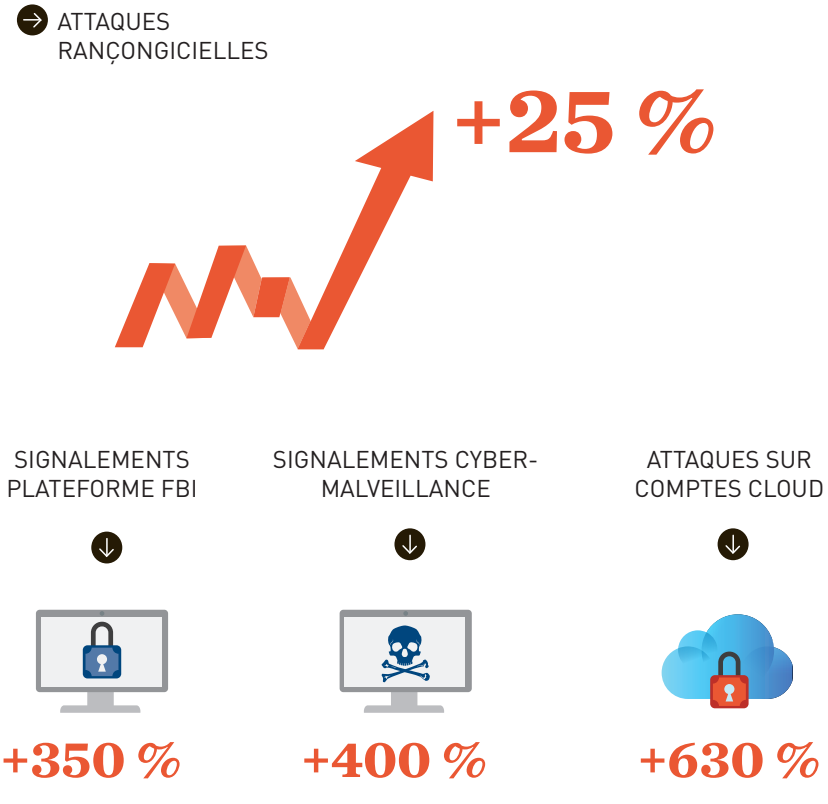
Quel est le coût réel des incidents de cyber-sécurité pour les entreprises ? Cette question a pris une importance nouvelle depuis le milieu des années 2010 alors que la prise de conscience de la question du cyber-risque a pris en ampleur[1].

D'autant que la Crise du Covid-19 démarrée au 1er semestre 2020[2] a amplifié ce risque. Le nombre d'attaques de rançongiciel aurait augmenté de 25 % au cours du 1er trimestre 2020. Les demandes d'aides face à des cyber-attaques sur les plateformes des autorités de sécurité publique aux Etats-Unis (« Crime complaint center » géré par le FBI) ou en France (« Cyber-malveillance ») ont augmenté à peu près de la même façon en mars 2020, à savoir environ d'un facteur x4[3]. En lien avec l'augmentation du trafic cloud et des activités de télétravail, les attaques externes sur les comptes cloud ont augmenté de 630 % de janvier à avril 2020[4].

Le risque cyber est inhérent à la digitalisation de l'entreprise et de son écosystème

Ce contexte de risque amplifié oblige donc à répondre à une question fondamentale et liée : quel est l'ensemble des coûts portés par l'entreprise lorsque celle-ci est victime d'une cyber-attaque – et comment avoir une vue exhaustive de l'impact ? En effet, si les approches par les coûts directs[5] sont importantes, il est nécessaire d'également inclure les effets indirects soit par exemple en termes de moral des équipes & rétention du personnel – et donc d'augmentation de la structure de coût et perte de productivité à moyen-long terme ; soit d'image de marque auprès des clients et donc de pertes potentielles de chiffres d'affaires également sur le moyen-long terme. Au final, ce sont tous ces facteurs pris ensemble qui vont impacter ce qui intéresse les parties prenantes de haut de bilan, à savoir à la fois l'évolution de la valorisation de l'entreprise et la capacité à éviter le défaut sur les dettes long terme. La question est d'autant plus importante qu'elle conditionne au niveau de la direction générale et du conseil d'administration le focus et les investissements à accorder aux cyber-incidents. Or, sans évaluation correcte, il est impossible de pouvoir précisément jauger des moyens à accorder. Et auquel cas, on risque de s'exposer à un risque non maîtrisé.

Augmentation du risque cyber pendant la crise Covid-19



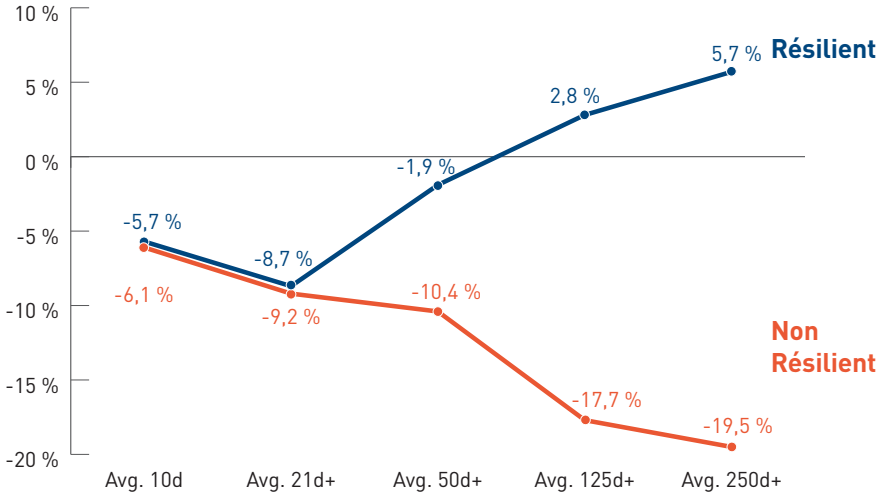
Le choc économique est observable pour les entreprises cotées via l'évolution du cours de bourse

Les entreprises cotées se prêtent évidemment plus facilement à cette évaluation, observable sur le temps court et long via l'évolution du cours de bourse. Plusieurs études publiées en 2018 aux Etats-Unis, au Royaume-Uni et en France finissent par montrer les impacts structurels en termes de pertes de valeur pour l'entreprise[6]. Par exemple, l'étude PwC France, réalisée avec G.P. Goldstein, sur 30 incidents, montre un impact significatif sur le cours de bourse. Dans 63 % des incidents, le cours de bourse baisse d'environ 9 % en moyenne au cours des 21 premiers jours de trading, soit environ un mois. Puis ce groupe d'entreprises se sépare en deux destins différents. 40 % des entreprises du panel poursuivent un long déclin de leur cours de bourse, qui les amène à une baisse de -20 % 12 mois plus tard comparé au cours avant l'annonce de l'incident. L'autre groupe, soit les 23 % restants, rebondit au bout d'environ 3 mois et finit par se rétablir à +6 % comparé au cours avant l'annonce de l'incident environ 12 mois après[7] (voir Fig.2). On note bien au total que les cyber-incidents semblent effectivement impacter la valorisation des entreprises cotées depuis la deuxième moitié de la décennie 2010. On note d'ailleurs que les effets sont plus importants sur le moyen-long terme que sur le court terme. C'est le signe de l'importance des coûts indirects évoqués plus haut (réputation vis-à-vis des employés et des clients), d'une magnitude bien plus importante que les coûts directs. Cet impact observable pour les entreprises cotées se retrouverait-il également pour les entreprises non cotées ?

Évolution du cours de l'action après l'annonce d'une cyber-attaque

Fig 2. Échantillon de 30 incidents
Moyenne du cours de 2007-2018 par période de jours de trading

Source : PwC/ GP Goldstein



Plusieurs travaux de recherche montrent qu'en effet les entreprises non cotées ont une exposition au risque de manière générale d'un ordre de magnitude comparable aux entreprises cotées, sinon parfois plus.

Le choc économique est-il de même nature et de même intensité pour les entreprises non cotées ?

Certes, il pourrait apparaître que les entreprises cotées soient plus exposées au risque de chocs externes que les entreprises non cotées. En effet, la valorisation des entreprises cotées est relativement sensible aux questions de réputation même si, en réalité, l'effet est en fait le plus important pour les très grands groupes[8].

Par contre, les entreprises non cotées peuvent, elles, avoir plus de difficulté que les entreprises cotées pour pouvoir avoir accès à des facilités de crédit court terme, et peut-être encore plus pour de la dette long terme. Dans ce dernier cas, lorsqu'elles sont en croissance, les entreprises non cotées sont forcées d'avoir une part plus importante de leur stock de dette composée de facilitées de court terme : ce désavantage comparé aux sociétés cotées les exposent évidemment à plus de risques en cas de choc[9] . D'autres études sectorielles démontrent également la facilité de l'accès au capital pour les entreprises cotées[10]. Enfin, plusieurs études américaines montrent que les entreprises non cotées sont plus réactives par rapport aux décisions d'investissement que des pairs cotées[11] et bénéficient également de moins d'obligation de transparence et de pression de divers actionnaires, ce qui leur permet d'avoir plus de latitude pour choisir des projets plus innovants comparés à des projets plus conventionnels[12]. Mais cet avantage constitue également une incitation à sélectionner un profil d'exposition plus risqué.

Au final, il ressort que si l'on met de côté le cas des plus grandes capitalisations cotées, une entreprise cotée devrait être relativement moins sensible à des chocs externes qu'une entreprise non cotée. Les résultats identifiés de chocs d'incidents cyber sur la valorisation des entreprises cotées devraient trouver une forme d'équivalent sur les entreprises non cotées. Comment néanmoins capter cette information par définition non disponible pour les entreprises non cotées ? Les pages suivantes proposent une méthodologie pour parvenir à une réponse – et les résultats clés qui ont été par la suite obtenus.

« À propos d'Altares »

Expert de l'information sur les entreprises, Altares collecte, structure, analyse et enrichit les données BtoB afin de les rendre « intelligentes » et faciliter la prise de décision pour les directions générales et opérationnelles des entreprises. Le groupe propose son expertise sur toute la chaîne de valeur de la data. Partenaire exclusif en France, au Benelux et au Maghreb de Dun & Bradstreet, 1er réseau international d'informations BtoB, Altares se positionne comme le partenaire de référence des grands comptes, ETI, PME et organisations publiques, en leur offrant un accès privilégié à ses bases de données sur plus de 360 millions d'entreprises dans 220 pays.

Comment analyser les entreprises non cotées ?
Proposition de méthodologie

Afin d'y parvenir, cette étude s'est tournée vers les informations de type Altarès / Dun & Bradstreet sur les scores de défaillance et paydex (jours de retard de paiement). Une analyse a été conduite sur 30 incidents entre 2017 et 2019, répartis à parts égales en France et à l'étranger, sur des entreprises non cotées couvrant de nombreux secteurs (industries, services, commerces) avec des tailles variant de la PME à la grosse ETI. La limitation de la taille de l'échantillon souligne l'objectif de cette étude : d'abord et avant tout, une première exploration « à grosse maille » de la réalité ou non de l'impact des incidents cyber sur le modèle économique des entreprises. Un focus particulier a été réalisé sur le panel français (15 entreprises) dont l'étroitesse plus importante a été cependant compensée par d'autres études sur l'analyse des jours de retards de paiement d'une part, et par l'analyse de « jumeaux », à savoir 3-5 entreprises de même taille et même secteur pour chaque entreprise « victime » évaluée – toujours avec l'objectif de confirmer ou d'infirmer la matérialité d'un lien cyber-incident et dégradation économique.

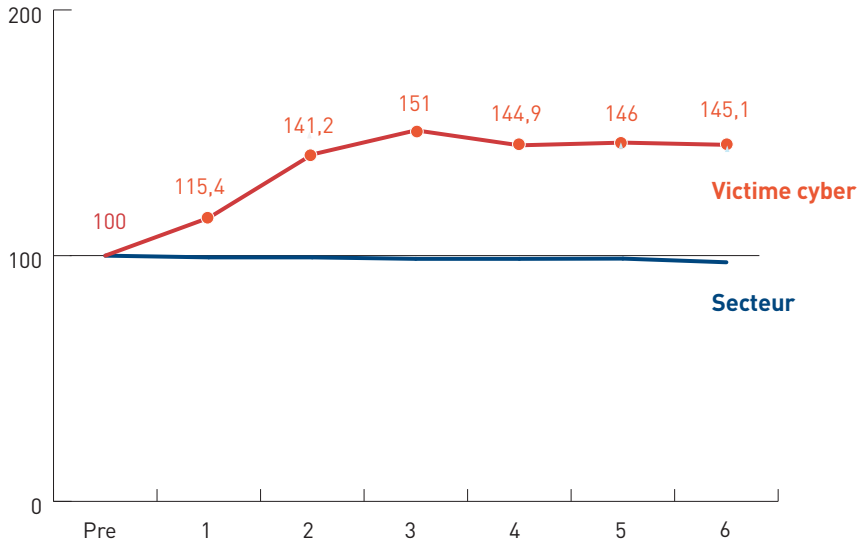
Le score de défaillance est un score de 1 à 20 (en France) et de 1 à 100 (dans le réseau mondial Dun & Bradstreet) estimant la probabilité d'un recours à une procédure collective visant l'entreprise évaluée. Ce score prend en compte plusieurs paramètres pour les entreprises commerciales. Entre autres : leur ancienneté, la nature de leur origine (création, rachat…), leur filière industrielle, leur taille, le nombre de jours de retard de paiement, l'analyse détaillée du bilan et du compte de résultat, l'existence d'évènements juridiques multiples, de dettes fiscales, la qualité financière de l'actionnaire majoritaire et un index d'activité. Ces éléments sont également complétés par d'autres en l'absence de documents comptables récents. L'ensemble forme donc un score composite, influencé par de nombreux facteurs relativement hétérogènes et offrant collectivement une bonne vision de la stabilité économique de l'entreprise – et de sa capacité à faire face à ses échéances.

Il s'agit de l'une des très rares données économiques disponibles permettant d'évaluer mois par mois l'évolution d'une entreprise non cotée ni du point de vue de son capital (suivi par les analystes et évalué par son cours de bourse), ni de celui des obligations de société (suivi par les agences de notations et également évalué par les marchés). Le score de défaillance pallie donc une absence d'information de marché, en particulier pour les petites et moyennes entreprises. Il est obtenu par analyse d'un réseau d'entreprises partenaires, incluant certains grands facturiers, qui permet par recoupement une couverture très large du tissu d'entreprises en France comme à l'étranger.

Entreprises non cotées : augmentation significative du risque de défaillance

Une première analyse sur la totalité de l'échantillon France & Etranger montre un impact significatif des cyber-incidents sur l'évaluation du risque de défaillance (voir Fig. 3). En prenant pour base 100 le mois avant l'annonce publique de l'incident (noté « pré ») – afin de s'assurer de la prise de connaissance par toutes les parties prenantes internes et externes de la situation de crise ainsi créée – on observe une dynamique forte qui démarre dès le mois de démarrage de la crise (mois « 1 ») puis augmente rapidement pour arriver à un maximum de la crise au mois «3 » avec une élévation du risque de défaillance de +51 % comparée à avant la crise. En comparaison, le panel représentant l'ensemble des entreprises du secteur (avec une sur-représentation des petites structures) montre une assez grande stabilité. Pour les entreprises victimes, la situation de dégradation semble d'ailleurs créer un état de fait relativement structurel, avec une augmentation du taux de défaillance qui reste dans l'étiage de +40 % / +50 % pour le reste des 6 mois qui suivent. Cette temporalité a quelques échos avec les études précédentes sur les entreprises cotées. Dans l'étude PwC Cyber Intelligence / GP Goldstein, la dégradation la plus importante est obtenue dans les 2-3 premiers mois, puis les entreprises dites « résilientes » vont entamer leur rebond pendant que les entreprises « non-résilientes » vont continuer leur descente.

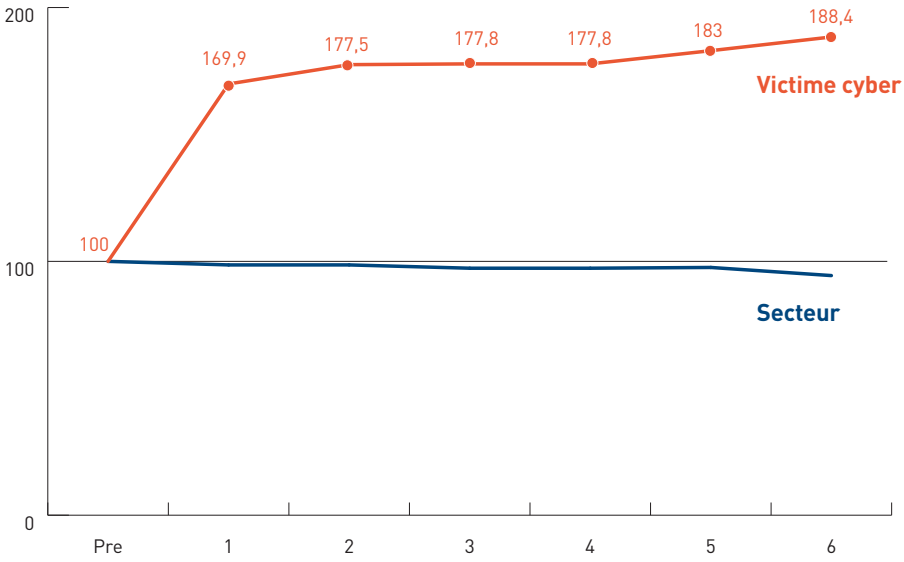
Fig 3.Évolution du risque de défaillance – Panel Monde
(Panel Monde / Base 100 : 1 mois avant cyber-incident)



Entreprises non cotées : focus sur l'échantillon des entreprises françaises

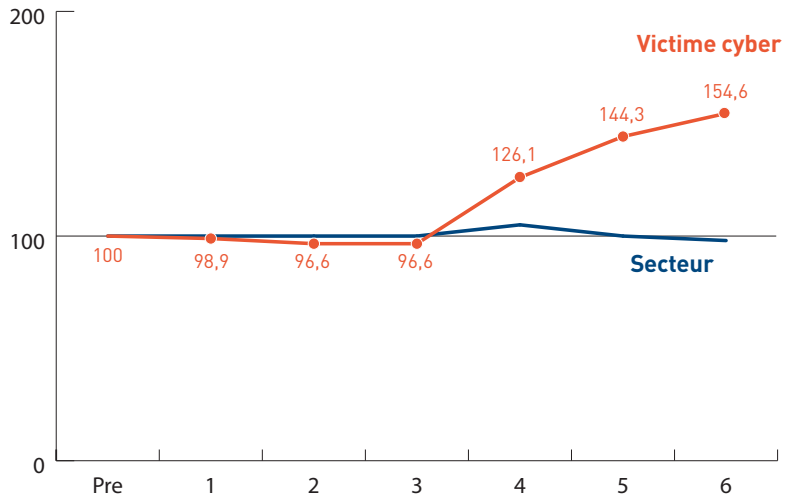
L'analyse de la situation sur l'échantillon français montre, elle, une dégradation plus rapide et plus importante de la situation. L'augmentation de la probabilité de défaillance comparée au mois avant l'annonce de l'incident est de 70 % dès le premier mois et atteint +88 % au bout du mois « 6 » dans une dynamique qui semble moins contrôlée que pour le groupe global - même si un « plateau » semble se dessiner très rapidement à +80 % entre quasiment le mois « 2 » et le mois « 5 ». On note de manière générale à la fois une accélération et une amplification de l'impact en France comparé à la situation au niveau global (voir Fig.4).

Fig.4 Évolution du risque de défaillance – Panel France
(Ens. du panel France / Base 100 : 1 mois avant cyber-incident)



Une analyse plus poussée a été établie sur le panel des entreprises françaises, permettant entre autres d'une part de faire une analyse complémentaire sur l'évolution du nombre de jours de retard de paiement (l'une des composantes du score de défaillance, même si ce dernier est composé de bien d'autres facteurs) ; et la comparaison avec des « jumeaux », c'est-à-dire 3 à 5 entreprises du même secteur et taille, sélectionnées par Altarès/ Dun & Bradstreet, afin d'arriver à une analyse comparative un peu plus poussée qui puisse renforcer (ou infirmer) la validation des résultats précédents sur l'échantillon des entreprises françaises de l'étude, par construction plus réduit (n=15). Ces deux « tests » complémentaires vont dans le sens d'un renforcement des résultats précédents, à savoir la vérification d'un impact réel et adverse des incidents cyber sur la stabilité économique des entreprises qui en ont été les victimes.

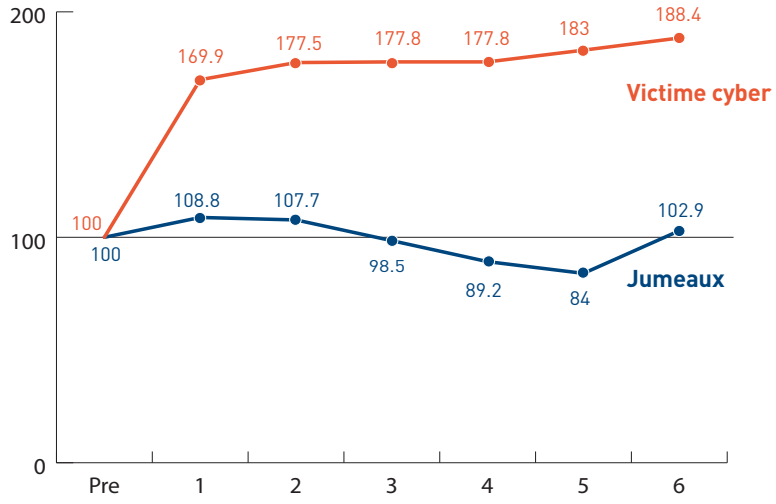
Fig.5 Évolution du nombre de jours de retard paiement
(Panel France/ Base 100 : 1 mois avant cyber-incident)



ÉVOLUTION DU NOMBRE DE JOURS DE DÉLAIS DE PAIEMENT SUR L'ÉCHANTILLON FRANCE

L'évolution du nombre de jours de retard de paiement semble elle aussi marquée par l'impact des cyber-incidents. L'augmentation du nombre de jours de retard de paiement est de +55 % au mois « 6 » comparé à la situation juste avant l'annonce du cyber-incident – une augmentation très significative (voir Fig. 5). Le délai observé (la dégradation ne commence qu'après le mois 3) est dû en grande partie à la manière dont est calculé l'indice : celui-ci est une moyenne mobile sur 8 mois, les effets d'un choc ne se liront pleinement qu'avec un retard de quelques mois. Néanmoins, ce facteur sur le paiement contribue clairement à la dégradation continue du score de défaillance sur la période : les deux poursuivent une dynamique ascendante à partir du mois « 3 », ce qui souligne une corrélation évidente et peut-être un lien de causalité.

Fig.6. Évolution comparée du Score de Défaillance Panel France & « Jumeaux »
(Base 100 : 1 mois avant cyber-incident)

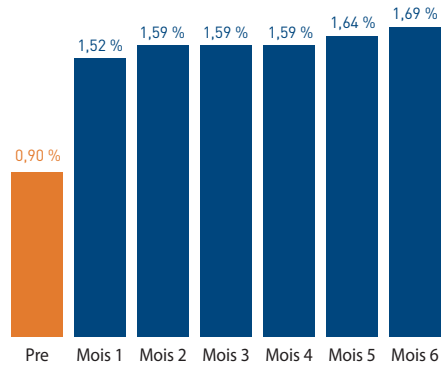


COMPARAISON AVEC LES ENTREPRISES « JUMEAUX »

Une analyse comparative a été établie avec des entreprises des mêmes secteurs industriels et tailles que chacune des entreprises de l'échantillon français (voir Fig.6)[13]. En comparant les évolutions à partir du même mois avant l'annonce de l'incident cyber, on peut distinguer si la dynamique observée sur les entreprises de l'échantillon « victime » est indépendante des chocs qui pourraient atteindre les secteurs industriels / les jeux compétitifs entre acteurs de même rang. La comparaison montre clairement une absence de corrélation positive entre la dynamique des entreprises « victimes » et leurs jumeaux industriels : cela renforce l'hypothèse que la dynamique de dégradation est liée à l'incident de cyber-sécurité. En outre, on observe pour ces jumeaux, qui sont également des compétiteurs potentiels des entreprises « victimes », une légère amélioration de leur situation économique au fil du temps alors que la situation de leurs compétiteurs « victimes », elle, se dégrade. L'hypothèse d'une amélioration partielle de la compétitivité des « jumeaux » aux dépens des entreprises « victimes » ne peut être écartée.

Aller plus loin : du risque de défaillance vers l'impact sur la valeur patrimoniale de l'entreprise

Fig. 7. Évolution de la probabilité de défaillance
(Echantillon France - comparaison « Pré » annonce incident, et 6 mois qui suivent)



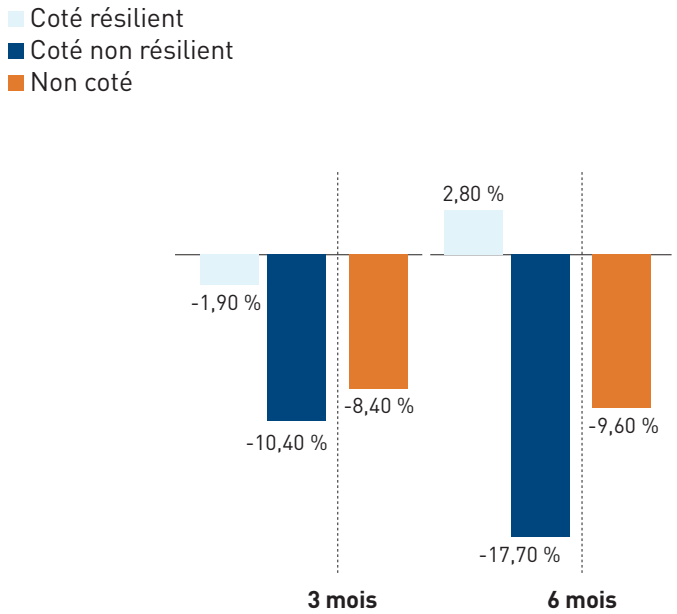
Le risque de défaillance (mesuré par le score de défaillance) non seulement est un indicateur clé pour les prêteurs de l'entreprise, y compris d'ailleurs au sujet de la dette long terme dans le haut de bilan ; mais également pour les actionnaires : en effet, il existe plusieurs liens pouvant signaler qu'une augmentation du risque de défaillance peut également entraîner une réduction de la valorisation de l'entreprise – à commencer par les liens via le modèle CAPM/ Capital Asset Pricing Model. D'autres modélisations plus récentes ont également essayé d'évaluer l'impact de l'augmentation de 1 % de la probabilité de défaut sur l'ensemble des composantes du haut de bilan, à savoir les dettes long terme et le capital et arrivent en particulier à des résultats de réduction de la valeur d'entreprise variant entre -8 % et -36 % au maximum[14] .

En retournant à l'échantillon français du panel, on obtient une évaluation moyenne en termes de probabilité de défaut de 0.9 % avant l'annonce jusqu'à 1.69 % au mois « 6 »[15].

En suivant l'analyse de Skogsvik (2016), en prenant l'incrément d'augmentation de la probabilité de défaut de 1 % à 2 % (afin de trouver une équivalence avec l'augmentation de 0.9 % à 1.69 %), sur la base d'une entreprise de croissance moyenne (3 %), on obtient une réduction de la valeur d'entreprise de -12.2 %. En appliquant un simple ratio équivalent à l'augmentation de 0.9 % à 1.59 % - 1.69 %, on atteint une évaluation moyenne de la perte de valeur d'environ -8.4 % et -9.6 % à partir du mois « 3 ». On notera d'ailleurs que cette évaluation se retrouve dans l'ordre de magnitude des sous-évaluations sur le moyen-long terme identifiées dans les études Comparitech et PwC / GP Goldstein sur les entreprises cotées.

Fig 8. Dégradation de la valorisation de l'entreprise après cyber-incident

Comparaison cotées / non cotées



Dans les faits : dans quelques cas, cessation d'activité et difficultés financières aigües...

Si les résultats quantifiés permettent d'avoir une vue générale, il est aussi important de comprendre dans le détail de certains des cas dans l'échantillon d'analyse les conséquences réelles d'un cyber-incident. Or, dans quelques cas de l'échantillon, ils ont mené à la cessation d'activité pure et simple – et cela, qu'il s'agisse d'un groupe américain de recouvrement de créances de plus de quarante ans, ou d'un petit détaillant en pièces de rechange du centre de la France.

CAS #1

Entreprise financière US de recouvrement de créances, avec une filiale spécialisée dans le recouvrement de créances sur factures médicale.

La maison-mère avait plus de 40 ans d'existence au moment de l'incident. Elle a été obligée de déposer le bilan quelques semaines seulement après que la filiale médicale ait été victime d'une large fuite de données, découverte au printemps 2019 et révélée trois mois plus tard. La société avait en effet été victime d'une cascade de fuites de données touchant plusieurs laboratoires d'analyse médicale de plusieurs millions d'usagers – plus d'une dizaine de millions au total. La société a en outre reconnu que ses difficultés de cyber-sécurité avaient peut-être démarré neuf mois plus tôt après la découverte : elle aurait donc fait preuve d'une forme de négligence, qui lui sera reprochée par justiciables et clients. En effet, dans la foulée, la maison-mère va connaître une compression commerciale brutale en termes de perte de clients ainsi que la multiplication de plus d'une douzaine d'actions en justice. En effet, au cœur de son activité, la filiale médicale gère des données très sensibles de santé – ce qui augmente l'exposition au risque de pénalités judiciaires. En outre, la nécessité de réduire drastiquement les accès informatiques pour cause d'identification des sources de la fuite ont terriblement contraint les opérations de l'entreprise. À cela s'est accompagné au moins plusieurs millions de dépenses IT, mais également de coûts de notification mail et communications. Au final, l'entreprise a réduit le nombre d'employés d'une centaine en 2018 à hauteur d'une vingtaine juste avant l'été 2019, jusqu'au moment où la conjugaison de tous ces éléments ont fini par conduire l'entreprise à la procédure de mise en faillite dans le cadre du chapitre 11 du code américan des faillites.

ANALYSE

Le Cas #1, très emblématique dans les conséquences catastrophiques d'une mauvaise gestion de la crise cyber, illustre certains points clés que l'on retrouve dans les entreprises cotées qui ont particulièrement souffert d'incidents cyber. D'une part, la maison-mère était naturellement très exposée par sa filiale médicale, à au moins deux titres : il s'agissait d'un acteur financier, le type de cible visé en priorité par les groupes cyber-criminels, mais également désormais bien identifié par les acteurs de marché comme des actifs sensibles aux cyber-attaques (voir par exemple le bureau de crédit Equifax, coté lui, et qui a perdu jusqu'à un tiers de sa valeur en 2017 suite à une cyber-attaque) ; d'autre part, la filiale médicale gérait de la donnée médicale en lien avec des traitements de particuliers – une donnée extrêmement sensible, pour laquelle il y a déjà de la règlementation aux États-Unis. La filiale médicale constituait donc déjà en termes de gestion de risques un actif extrêmement sensible. En outre, l'entreprise semble avoir pris du temps pour reconnaître la gravité de la situation, puisqu'une première situation d'incident avait émergé 9 mois plus tôt, dès l'été 2018. La crise est souvent un moment de « révélation », en particulier les forces et les faiblesses de l'organisation. Ici, la révélation donne l'apparence de négligence continue qui ne permet pas le rétablissement de la confiance auprès des clients. Enfin, la réduction drastique des accès informatiques et l'impression de difficultés de communication exponentielles au sein du groupe donne la sensation que le groupe ne s'était jamais préparé à ce type d'incident et a donc été pris au dépourvu. L'ensemble de ces manquements qui sont très essentiellement du domaine de la gestion de crise a été fatal à l'entreprise.

CAS #2

ETI, fabricant d'acier laminé dans le Sud des États-Unis.

Ce deuxième cas présente un autre exemple d'une société qui semble avoir été très durement touchée par une cyber-attaque de type rançongiciel. L'impact a bloqué la production pendant au moins une semaine, avec quelques échos dans la presse locale, évoquant un montant de rançon élevé sans que l'entreprise ait pu par la suite confirmer ou infirmer. Les impacts économiques semblent avoir été importants, car l'entreprise finit par voir un quasi doublement de son risque de défaillance (9 % à 17 %), la plaçant dans une situation extrêmement délicate en termes de risques. Son appartenance à un groupe industriel lui a peut-être permis d'éviter les difficultés graves rencontrées dans le Cas #1.

CAS #3

PME Française, distributeur de pièces de rechange.

À contrario, dans ce troisième cas, la PME, un distributeur de pièces de rechange au centre de la France, ne pourra pas bénéficier de cette « protection » suite à une attaque par rançongiciel. Celle-ci survient à l'automne 2017. Rapidement, c'est l'ensemble des informations les plus sensibles - stock, commandes, listing clients, au total plusieurs dizaines de milliers de fichiers qui passent entièrement sous le contrôle exclusif du rançongiciel. La PME n'avait pas de systèmes redondants pour retrouver rapidement l'ensemble de ces informations. Hors le coût de la demande de rançon (minime – moins de 5.000 Euros, mais qui doublait tous les jours), le fait de ne pas payer la rançon, peut-être sous les conseils des autorités, a néanmoins forcé l'entreprise à finir par déposer le bilan.

ANALYSE

Contrepoint par la taille et l'industrie au cas #1, le cas #3 « PME Française » est là encore illustratif de plusieurs points importants. D'abord, que même une entreprise « traditionnelle », s'occupant d'un secteur de services dans les produits bruns, peut disparaître en raison d'une cyber-attaque. Ce n'est pas uniquement pour Equifax ou pour le Cas #1 « Entreprise financière aux US » (et son réseau de laboratoires partenaires) que les données numérisées sont critiques, mais également désormais pour tout type d'entreprise – y compris donc un distributeur de pièces d'électroménager dans le centre de la France. En outre, là encore, l'absence de préparation au choc – en particulier le fait qu'aucun système de sauvegarde protégé de l'information n'ait été envisagé en amont – a pu être fatal à l'entreprise. À nouveau, la question de l'investissement dans la résilience cyber pour le tissu de PME et d'ETI se pose de manière importante.

Dans les faits : ... Le plus souvent, une dégradation de l'activité

Même si c'est le plus spectaculaire, le défaut n'est évidemment pas le cas le plus fréquent. Une dégradation forte et plus ou moins temporaire de l'activité semble constituer le cas commun. Deux exemples illustrent ces situations de fragilisation plus ou moins bien maîtrisées.

CAS #4

ETI informatique américaine.

La victime ici est un fournisseur cloud aux États-Unis de services et logiciels comptables dédiés aux experts comptables. L'entreprise s'est retrouvée victime à l'été 2019 d'une cyber-attaque de type rançongiciel qui a bloqué l'accès à toutes les données de comptabilité de ses clients pen-dant plus de 3 jours. La réputation de l'entreprise a pu être entachée d'autant que la société a laissé longtemps dans l'ignorance ses clients de la date éventuelle de rétablissement des accès en ligne. La colère de certains clients a été perceptible jusque sur Twitter et sur Facebook. En réponse, la société s'est contentée de désactiver son compte Twitter et supprimer des commentaires négatifs de sa page Facebook. L'entreprise a fait l'expérience d'une dégradation significative de ses délais de paiement dans les mois qui ont immédiatement suivi la crise, passant à plus de 141 jours de retard, mais partant d'un niveau qui était déjà très élevé. La société a par la suite été rachetée en fin d'année 2019 par une autre ETI informatique américaine pour un prix non dévoilé, sans que l'on puisse établir si ce rachat a été précipité ou non par la crise liée au rançongiciel.

ANALYSE

Ce cas montre à nouveau qu'au-delà des problèmes techniques, une mauvaise gestion de crise peut potentiellement abimer l'un des plus grands actifs que possède une entreprise : la confiance de ses clients. La situation est ici d'autant plus délicate, qu'elle concerne un autre type de données critiques : la comptabilité des entreprises (d'autant que les cyber-criminels peuvent non seulement opérer un chantage sur l'accès aux données, mais également en profiter pour identifier des données commerciales sensibles et masquer par la suite l'attaque en « simple rançongiciel »). Au-delà, une mauvaise communication de crise comme c'est le cas ici - agissant parfois dans une sorte de déni ou de volonté de suppression de l'information - peut au contraire avoir des effets adverses graves, à commencer par l'expression de la colère sur les réseaux sociaux. Qu'il s'agisse d'ailleurs de marchés B2C, semi-pro, ou B2B, les réseaux sociaux recouvrent une réalité désormais absolument incontournable. Ils imposent une dose de transparence et surtout d'honnêteté nécessaire dans la communication de crise.

LE CAS #5 D'UNE ETI,

Société d'ingénierie française travaillant pour un constructeur aéronautique illustre un autre point important : la responsabilité de chacun dans le cadre des relations clients-fournisseurs. Cette société d'ingénierie est d'ailleurs initialement victime d'une attaque via sa propre filiale hors France. L'attaque, très sophistiquée, aurait néanmoins démarré en 2018 en passant par le VPN du grand constructeur. Les objectifs ont pu être multiples – tels que, d'une part, utiliser le fournisseur pour arriver à voler des informations sur son grand client comme de la propriété intellectuelle (par exemple motorisation ou informatique embarquée), des éléments sur les certifications en cours ou bien encore des données personnelles sur les employés, ce qui peut permettre de préparer par la suite des attaques de social engineering (connaissance de l'utilisateur qui permet d'inférer des mots de passe, des pratiques, etc...). Au final, les informations de score de défaillance indiquent une augmentation significative de la probabilité de défaillance, sans pour autant atteindre des seuils de dangers élevés. Il s'agit peut-être là de l'expression d'un dialogue commercial client-fournisseur plus tendu suite aux attaques.

ANALYSE

Cet exemple illustre le fait qu'une entreprise se retrouve très souvent au cœur d'un écosystème (d'ailleurs parfois dominé par un grand acteur) ; mais que l'entreprise elle-même déploie aussi parfois son propre écosystème, dans une logique un peu fractale. Or, tous ces éléments et ces liens sont en jeu dans la cadre de la cyber-sécurité. Cela d'autant plus que les attaques peuvent avoir en fait pour objet d'affaiblir durement le grand constructeur en identifiant le sous-traitant qui développe des pièces ou des expertises uniques : en le ciblant, on ralentit le système productif du grand constructeur. Les logiques d'écosystèmes, et de protection non pas de chaque entreprise face aux autres, mais de l'ensemble des entreprises toutes ensembles face à la menace, imposent une évolution profonde des liens clients-fournisseurs. On le voit dans certaines évolutions méthodologiques, comme par exemple des approches de cartographies de risques par écosystèmes développées en Israël par l'INCD, l'équivalent local de l'ANSSI ; ou bien encore par des logiques d'entraide qui apparaissent entre gros clients et fournisseurs en cas de crise, en particulier justement dans les écosystèmes aéronautiques. Cette entraide doit non seulement inclure la coopération technique face à la menace cyber, mais peut-être aussi certaines dimensions de fragilité économique – en tout cas, éviter de faire trop peser des menaces juridiques ou des demandes de renégociations commerciales à des entreprises temporairement affaiblies par un incident cyber. Ce serait en réalité prendre le risque d'affaiblir l'ensemble de l'écosystème et donc soi-même.

Dans certains cas, le cyber-incident permet de faire la démonstration de la résilience de l'entreprise

Les données récupérées permettent d'observer que certaines entreprises ont réussi à bien résister à la crise et même parfois améliorer leurs positions – en tout cas, éviter une dégradation de leur score de défaillance.

ETI INDUSTRIELLE FRANÇAISE, FILIALE D'UN GRAND GROUPE INTERNATIONAL

Ce cas constitue un exemple de communication de crise en situation d'attaque cyber déclenchée à nouveau par un rançongiciel. La crise démarre sur le réseau du grand groupe industriel, ainsi que dans la filiale française au printemps 2019, celle-ci étant spécialisée dans certains produits B2B2C. La filiale française, site entièrement intégré dont tous les outils sont pilotés par l'informatique, se retrouve entièrement paralysée.

La cartographie du stock où sont recensées plusieurs milliers de références s'est retrouvée inutilisable et le magasin automatique, inopérant. Mais l'entreprise, en prenant peut-être pour modèle la maison-mère, prend le pari vertueux de la transparence en même temps que les équipes repassent en mode manuel alors que les services IT se mettent en mode crise 24/7 et relancent l'infrastructure.

Ainsi, à la différence d'autres entreprises françaises victimes du même rançongiciel et qui ont été beaucoup plus discrètes, la filiale française et le groupe font le pari d'une communication fréquente et qui se veut la plus transparente possible. Dès le lendemain de l'attaque, une page web dédiée est créée par le groupe et une web-conférence de presse est immédiatement organisée. Le retour aux procédures manuelles est également clairement affiché.

À environ J+15, alors que le retour à la normale est bien enclenché, le Groupe crée une chaîne Youtube où les employés peuvent raconter ce qu'ils ont vécu. L'objectif est peut-être de laisser parler les employés afin simplement de « parler » - la crise peut être vécue comme un moment traumatisant – mais donc également d'aider les équipes à rester soudées tout en se montrant à leur écoute[16] . Le groupe annonce également assez vite, à J+45 quelle est son estimation du dommage en termes à la fois des coûts directs et de chiffres d'affaires non réalisés.

Le cours de bourse retrouve rapidement son niveau avant l'annonce de l'incident. Au niveau de la filiale française, sa situation

en termes de score de défaillance s'améliore légèrement durant la période. Il ne semble pas y avoir eu de déstabilisation profonde de l'activité.

ANALYSE

Ce cas souligne l'importance de points déjà vus plus haut, à savoir à la fois la réalité de postes de travail et de processus d'informations clients ou stocks qui sont déjà passés en très large partie dans la sphère numérique et qui sont donc désormais fortement susceptibles de vulnérabilités cyber ; mais aussi la qualité de la politique de résilience (et peut-être donc des plans de réponse à incident / plans de continuité de l'activité) au-delà même des solutions technologiques mises en œuvre. Une communication transparente et détaillée, incluant une certaine franchise sur le fait que l'on va passer en mode dégradé (ex. du passage à des fonctions manuelles) est en réalité nécessaire et critique pour rétablir à nouveau l'actif intangible le plus important pour l'entreprise : la confiance de ses clients et partant de là, la confiance de ses actionnaires. Cet exemple fait écho à l'actualité de la crise Covid-19 où là encore, l'importance de la confiance entre gouvernants et gouvernés, et donc d'une communication la plus transparente possible, y compris en reconnaissant erreurs et manquements, est au cœur de la gestion de crise. Les exemples à travers le monde, échecs ou réussites, abondent désormais en ce sens. Ils s'appliquent tout autant à la gestion de la crise cyber. Bien exécutés, ils permettent d'éviter l'amplification du risque de défaut et de préserver la valeur patrimoniale de l'entreprise.

Conclusions intermédiaires...

Cette étude, même si limitée par un échantillon encore relativement étroit, obtient des résultats généraux suffisamment significatifs pour renforcer l'hypothèse, déjà émergente pour les entreprises cotées, d'un impact significatif des cyber-incidents sur la stabilité économique et la valorisation de l'entreprise non cotée.

- L'étude renforce l'hypothèse qu'un incident cyber peut constituer un évènement critique pour une PME ou une ETI, même si les premiers impacts ici évalués ne sont pas aussi dramatiques que ceux évoqués dans d'autres publications (telle que la disparition d'une PME française sur quatre suite à une cyber-attaque[17], voire même aux Etats-Unis trois PME sur cinq dans les 6-12 mois suivant l'attaque[18]). Une augmentation du risque de défaut d'un facteur compris entre +40 % et +80 % constitue néanmoins un impact très significatif.
- L'analyse comparative entre entreprises cotées et non cotées réduit proportionnellement l'impact lié aux questions de réputation externes, très importantes pour les entreprises non cotées, mais pas exactement à la même magnitude que pour les grandes entreprises cotées[19]. Cependant, le risque opérationnel de l'entreprise non cotée, structurellement plus élevé que celui de l'entreprise cotée, contrebalance ces effets.
- Les ordres de grandeurs évoqués, quand évalués dans le sens d'une dégradation correspondante de la valorisation de l'entreprise, semblent alignés en termes de magnitude, avec les impacts estimés par les études Comparitech et PwC/GP Goldstein.

...Vers la Cyber-résilience

Au final l'étude met en avant le gain d'une cyber-résilience réussie : celui d'éviter l'augmentation du risque de défaillance pour l'entreprise et potentiellement une baisse qui pourrait se traduire, dans les cas étudiés, par une réduction moyenne d'environ 8 à 10 % de la valeur de l'entreprise. Voilà l'enjeu.

Mais l'analyse des cas permet également de souligner les éléments clés qui permettent d'obtenir ce qui est au cœur d'un concept venant du latin *resiliare* : à savoir rebondir, après avoir chuté. Cette dynamique peut se décomposer en trois éléments clés :

1. la préparation à la réaction au choc, bien avant que le choc ne soit là ;
2. l'absorption du choc initial ;
3. l'agilité et l'ouverture dans la réponse.

Voilà, à traits grossis, la méthode, illustrée par certains des exemples tirés du panel.

1. La préparation à la réaction au choc, venant avant le choc, constitue le dernier élément clé. À nouveau, les exemples issus montre des extrêmes presque caricaturaux – entre l'ETI industrielle, filiale d'un grand groupe, qui s'était déjà préparée et a exécuté son plan de réponses à incident avec la souplesse nécessaire pour toujours réadapter le plan aux imprévus et d'un autre coté, la PME française du centre de la France, qui s'est retrouvée absolument dépourvue en termes de plan de réaction. Est-ce là un cas isolé ? Malheureusement non – bien au contraire. Une récente étude a montré qu'en France, 80 % des entreprises n'avaient pas de plans de réponses robustes à incident face aux cyber-risques[20], pourtant désormais l'un des trois plus grands risques de l'entreprise. Que dire alors quand bien-même d'ailleurs le plan ne suffit pas - mais qu'en plus du plan, il faut absolument le tester, idéalement sur la plupart des niveaux hiérarchiques de l'entreprise, comme le recommande par exemple la Banque d'Israël depuis 2015, qui demande à ce que les structures dirigeantes jouent à des simulations de crise ?

...S'agit-il d'un idéal ? On peut se poser la question, tant tous ces éléments montrent une évidence. Comme pour la crise Covid-19, certes il faut une réponse technique, mais en réalité, même sans « vaccins anti-virus » ou sans « thérapies informatiques » claires, il y a des moyens pour réduire considérablement le choc. Ils

consistent en quelques règles et méthodes simples. Comme le masque face au virus, il ne s'agit pas de « formules magiques », et ce ne sont pas des solutions qui coûtent chères. Mais comme les masques, on omet de les appliquer. Le résultat de cette omission peut être grave et sévère.

2. L'absorption du choc initial permet à l'organisation de ne pas se retrouver prise à la gorge et de gagner du temps pour comprendre et être capable de réagir de manière adaptée à la crise. Mais pour cela, il faut des capacités redondantes. Le cas de la PME française, distributeur de pièces de rechange, qui se retrouve dépourvue car elle n'a précisément aucune copie, sur d'autres capacités protégées, de l'ensemble de ses stocks, listings clients et commandes, est un exemple cruel d'un manque de redondance qui bloque tout rebond. À un niveau plus financier, l'accès à des facilités de crédit permet de mieux tenir le choc. Or, c'est précisément l'un des désavantages de l'entreprise non cotée par rapport à son homologue cotée (voir plus haut). Son temps d'adaptation et d'absorption du choc initial est donc réduit.

3. L'agilité et l'ouverture dans la réponse correspondent à la phase de réaction et d'adaptation en tant que telle. On pourrait citer différentes composantes essentielles à une bonne exécution de cette phase par l'organisation : le fait d'avoir une vision de sortie de crise correctement exprimée par le leadership ; la nécessité d'avoir une action décentralisée et autonomisée afin que la prise de décision ne soit pas limitée à un centre, ou une « tête », qui va rapidement être débordée par la masse des décisions de crise nouvelles à prendre en plus de la gestion des autres opérations courantes ; enfin, la nécessité d'avoir une bonne communication entre toutes ces unités décentralisées et autonomes afin de partager une même vision d'ensemble – l'ensemble de ces points ayant été illustré d'une manière tragique lors de la crise Covid-19 entre la réaction centralisée de la France et décentralisée de l'Allemagne, qui trouve peut-être son origine dans la différence entre le modèle d'un coté napoléonien et de l'autre l'Autragstaktik de Helmut von Moltke, qui a par la suite inspiré la doctrine du Mission Command dans les forces occidentales. Cette opposition illustre d'ailleurs le facteur clé de succès lors de la crise, qu'elle soit militaire, ou cyber, ou sanitaire : aller plus vite que la menace. Parmi tous les éléments qui composent cette réaction, la communication interne ou externe constitue un des points clés. Elle est particulièrement bien illustrée dans le cadre de l'ETI industrielle française, filiale d'un groupe étranger, qui va faire preuve d'une grande transparence et déployer de nombreux outils de communication interne et externe. Il y a là la compréhension de l'une des choses les plus importantes en jeu lors de la crise : protéger la confiance des clients et des collaborateurs. C'est l'élément intangible au cœur de la création de valeurs de l'entreprise. *A contrario*, l'exemple de l'ETI informatique américaine, qui va censurer sa communication en ligne et les réponses de ses clients, va précisément à l'encontre de cette reconstruction de la confiance. À cette aune, elle devient un actif déprécié qui aura besoin de l'ombrelle d'une autre marque pour survivre. C'est peut-être ce qui lui est arrivé lors d'un rachat rapide quelques mois plus tard.

PARTIE 02

L'enjeu de la réputation face à une crise cyber ?

02

Regard

de Laurent Porta

« Cyber-risques : tous menacés et pourtant encore peu préparés à faire face ! »

Laurent Porta

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

« Parce qu'il touche directement à la réputation, l'actif immatériel le plus précieux, ce risque doit faire l'objet d'un process de gestion et de communication ad hoc. »

Nul besoin de posséder des données qui valent de l'or pour voir fondre sur soi les attaques cyber. Ces dernières visent aujourd'hui tout type de structure. Le risque cyber fait partie intégrante de toute cartographie des risques au même titre que le risque environnemental, juridique, financier ou social. Parce qu'il touche directement à la réputation, l'actif immatériel le plus précieux, il doit faire l'objet d'un process de gestion et de communication ad hoc.

Quel est le point commun entre l'assureur MMA, la mairie de Mitry-Mory (77), le Tribunal Judiciaire de Paris et l'entreprise Clermont Pièces (63) ? Tous ont été victimes, dans les douze derniers mois, d'un piratage avec demande de rançon.

Contrairement aux *a priori*, les premières victimes de cyber-attaques ne sont pas les multinationales ou les petites entreprises, mais bien les ETI, dont le nombre de victimes avait augmenté de 36 % à 63 % en 2019. Sous l'effet de la crise Covid-19, la généralisation bien souvent « à la hâte » du télétravail a renforcé la vulnérabilité des entreprises face aux attaques cyber et il y a donc fort à parier que ces chiffres seront de nouveau en hausse cette année. Il n'est donc pas étonnant que la crise cyber soit devenue en l'espace de 3 ans la principale crainte des entreprises.

Dès lors pour les entreprises, quels que soient leur taille, leur chiffre d'affaires, leurs produits ou leur emplacement géographique, la question n'est plus de savoir si elles vont être victimes d'une attaque cyber, mais plutôt de savoir quand et comment elles le seront !

La croissance exponentielle des sources et modes d'attaque doit conduire les entreprises à s'organiser pour les affronter. Même les plus aguerries à la gestion de crise doivent intégrer ce nouveau risque et adapter en conséquence leurs organisations, process et moyens de gestion et de communication.

Cette adaptation est vitale car toutes les entreprises ne survivent pas aux cyber-attaques, ces dernières pouvant provoquer la faillite d'une entreprise. En effet, les crises cyber ont un impact majeur sur la réputation des entreprises qui en sont victimes. Elles détruisent de la valeur et peuvent être mortelles pour les entités : perte de confiance des clients, des salariés, des partenaires, des investisseurs, etc. En 2015, le site de rencontres extraconjugales canadien Ashley Madison a fait l'objet d'une grande attention lorsque des pirates ont publié en ligne l'identité de millions d'inscrits, provoquant le départ de son PDG Noel Biderman tandis que l'entreprise a dû verser 11,2 millions de dollars aux victimes du piratage.

Dès lors, une fois l'attaque lancée et identifiée, les entreprises doivent accepter de mener la bataille de la communication que ce soit en externe, mais aussi en interne. En ayant toujours en-tête deux règles d'or qui sont des constantes en communication de crise :

1. Le refus d'admettre (ou, pire, le mensonge) aggrave les crises ;
2. Une forte exposition médiatique marque les mémoires durablement.

En matière de communication de crise, la cyber-attaque répond à des spécificités qu'il faut avoir en tête pour bien l'appréhender :

- Le paradoxe du temps long : l'informatique se pilote sur un temps long, la découverte de l'intrusion, la remédiation et l'assainissement des infrastructures prend du temps. Or, en temps de crise, on doit pouvoir rapidement prendre la parole au risque de laisser le champ libre à ses détracteurs et perdre la maîtrise du temps. La cellule de crise doit donc composer avec ce paramètre pour adapter sa composition et son temps de réponse.
- L'ampleur médiatique qui n'est pas forcément liée à la gravité réelle de la crise, mais qui se nourrit d'une double fascination : le facteur « David contre Goliath » (une personne seule arrive à s'infiltrer dans un gros système IT), auquel s'ajoute l'admiration de l'opinion public pour le « Pirate », notamment si l'action réalisée est techniquement complexe. L'entreprise doit alors s'interroger sur la nature même de sa communication : quel(s) message(s), quelle(s) forme(s) et quel(s) interlocuteur(s) ?

Dès lors, se pose pour l'entreprise, la question de réussir sa communication. Pour cela 3 grands principes se doivent d'être respectés :

1. La nécessité de partager rapidement des éléments techniques vérifiés : ce principe répond à la demande de l'opinion publique de transparence et de responsabilité de la part des entreprises. Or, une attaque cyber est rarement simple et ses retombées pas immédiatement identifiables. Mais pour garder la confiance de ses parties prenantes, l'entreprise doit faire preuve d'une grande pédagogie. Elle doit être en mesure d'expliquer, dans un langage simple, ce qu'il s'est passé et quelles actions sont menées pour revenir à un état sûr.

Ainsi lorsque l'entreprise américaine Garmin, spécialiste des bracelets connectés et des services de navigation par GPS, met plusieurs jours à admettre qu'elle est victime d'une cyber-attaque et non d'une panne informatique, qui paralyse pendant près d'une semaine l'ensemble de ses services, elle génère frustration, inquiétude et finalement perte de confiance chez ses clients utilisateurs. D'autant plus que les médias spécialisés et les réseaux sociaux faisaient état d'une cyber-attaque alors même que Garmin déclarait que ses serveurs étaient « en cours de maintenance ».

2. La maîtrise de ses vecteurs de diffusion : dans l'idéal il faut choisir un porte-parole unique, bilingue IT/grand public (ayant une bonne compréhension des dommages causés par l'attaque et des enjeux de l'entreprise) et le media de communication le mieux adapté : réseaux sociaux, site internet, presse spécialisée, etc. Enfin, il faut savoir utiliser les communautés d'alliés (cercles, leaders d'opinion) ayant une influence sur son activité.

3. Le souci de l'interne. Les salariés doivent être la première préoccupation de l'entreprise en cas de crise cyber, car ils peuvent se trouver en position d'être :

- Acteurs de la gestion de crise : pour coordonner l'ensemble des acteurs mobilisés dans la gestion de la crise (ex : équipes de supports, équipes techniques, équipes juridiques, etc.), il est primordial de communiquer en interne. Il convient donc de donner à chacun les informations dont il a besoin pour assumer ses activités mais également maintenir son engagement et investissement dans la gestion de l'évènement. Il faut néanmoins veiller à trouver le bon dosage dans le partage d'informations et préférer une communication ciblée, pour limiter les impacts négatifs en cas de fuites ;
- Premiers impactés : les salariés d'une entité sont souvent sollicités par leur entourage en cas de crise avérée dans leur entreprise. Ils doivent donc recevoir de leur hiérarchie une information claire, validée et stabilisée pour qu'ils puissent, chacun à leur niveau, relayer les messages.

Enfin, parce que les salariés peuvent aussi être à la source de la crise, il est important d'informer et former en amont sur les risques cyber pour inculquer les bons réflexes et comportements. En effet, l'étude mondiale Trend Micro « Head in the Clouds » portant notamment sur le comportement des salariés en télétravail a démontré que 39 % des collaborateurs avaient eu des comportements à risques, en utilisant par exemple un appareil personnel (smartphone ou ordinateur privé) pour accéder aux données et services de l'entreprise. Par ailleurs, en France, 41 % reconnaissent ne pas disposer d'un premier niveau de protection par mot de passe sur leurs appareils personnels !

La cyber-attaque est donc un risque aux enjeux et conséquences parfois dramatiques (pertes financières, poursuites juridiques en cas de fuite de données, impact sur l'image et la réputation de l'entreprise, etc.). Comme le met en exergue l'étude Bessé, la cyber-attaque peut entraîner une augmentation 40 % du risque de défaillance dans les 6 mois qui suivent l'attaque pour les entreprises victimes, et une baisse de -8 % à -10 % de la valorisation de l'entreprise. Ce risque ne doit donc pas être traité comme les autres et ne peut plus être sous-estimé. Il est essentiel qu'au niveau le plus élevé de l'entreprise, il soit identifié, défini et que des plans d'actions soient mis en œuvre pour le couvrir. Il doit faire l'objet d'un plan de prévention et de formation des collaborateurs qui auront à le gérer.

PARTIE 03

Révolution technologique et défis de la cyber-sécurité : l'exemple de la 5G

03

Regard
de François Barrault

François Barrault

François est Président fondateur de FDB Partners SPRL, société d'investissement et de conseils dans le secteur Technologies Médias & Télécommunications (TMT) et l'Edition depuis 2009 et Président d'IDATE DigiWorld depuis 2011.

« On vit une époque formidable !! ... »

Pendant des années les innovations technologiques ont été rythmées et cadrées par les fameuses « Lois de Moore » à savoir on double la puissance informatique des processeurs tous les 18 mois. Cette référence admise par tous les professionnels a permis de mieux cranter le développement des systèmes et leur financement. Mais les choses changent : on parle d'un facteur d'un Million pour les 8-10 prochaines années. Nous sommes à l'aube d'une révolution industrielle sans précédent qui va bouleverser le monde moderne déjà fortement ébranlé depuis 7 mois par le Covid 19. La 5G en est un des piliers, mais pas le seul.

Tout d'abord la nouvelle « Loi de Moore 2.0 » va s'appliquer à toute la chaine de création et traitement des données : « sensors », caméras, 'edge computing' ou informatique embarquée, stockage infini et gratuit et enfin processeur quantique. Bien sur chaque maillon se verra enrichi par de l'IA, Intelligence Augmentée et non artificielle qui traitera un nombre croissant d'opérations sans avoir à faire appel à des ressources décentralisées.

Les objets de la vie courante ou nos environnements personnels ou professionnels seront des machines à collecter des données, à les traiter, les comparer et à priori à nous fournir une meilleure qualité de vie, une sécurité renforcée.

La deuxième révolution sont les données et leur traitement : 'Data is the new Gold' !. Le premier pilier va créer des trillions de données tous les jours et pour qu'elles soient vivantes et exploitables, il faut les rendre pertinentes, intelligentes et surtout prédictives.

Enfin le lien essentiel entre la technologie et les données, la 5G dont les enchères de la première allocation de fréquences en 3,5 et 3,71 Ghz viennent d'être attribuées aux 4 opérateurs français. Il était temps car la 5G est déjà opérationnelle dans 35 pays chez 52 operateurs depuis 2018 !

Ce lancement qui devrait arriver avant la fin de l'année de manière sporadique sur notre territoire suscite beaucoup de questions anxiogènes.

A la 5G sont reprochés des impacts environnementaux, sanitaires et comportementaux. Si on exclut la théorie conspirationniste qui affirme que la 5G diffuse le covid-19, quatre thématiques sont au cœur des débats, en plus de celui de la souveraineté nationale.

1. Exposition aux ondes électromagnétiques (comme avec la 3G ou la 4G) plus importante avec l'utilisation des bandes millimétriques et une multitude d'objets connectés
2. Consommation énergétique (objets, capacité de stockage et de transmission)
3. Obsolescence prématurée de milliards de terminaux 4G
4. La cyber-sécurité liée à la souveraineté nationale est aussi une question centrale.

En France, des auditions ont eu lieu à l'Assemblée nationale et au Sénat ces dernières semaines. La Convention citoyenne pour le climat, réunie fin septembre pour voter sur les différentes propositions à soumettre au gouvernement, a d'ailleurs jugé ce passage de la 4G à la 5G « sans réelle utilité ».
M. Olivier Véran (Ministre de la santé) et Mme Elisabeth Borne (Ministre de l'environnement) ont écrit à M. Edouard Philippe alors Premier Ministre pour lui demander de temporiser avant d'obtenir l'avis de l'ANSES et notamment de reculer les enchères prévues initialement en avril et reportées fin septembre 2020.

Sur le terrain, des pylônes sont ainsi attaqués, souvent brûlés et détruits dans plusieurs pays mobiles avancés par des associations du type STOP5G (et ses déclinaisons nationales STOP5GBE, STOP5GNL...).

C'est un mouvement qui naît en Europe (avec plusieurs antennes détruites en France) et semble s'étendre dans les Amériques.

La conséquence de ces annonces perturbent fortement les citoyens et nos élus : il faut faire preuve de beaucoup de prudence et surtout

de pédagogie plutôt que de livrer à des joutes verbales stériles sur les plateaux TV : 'tough with fact, nice with people'

Concernant l'aspect sanitaire et pendant les 3 prochaines années, les fréquences utilisées sont très proches des existantes (3G,4G, Wifi) voire au-delà (Wifi 2,4 Ghz, 5 Ghz) à la maison. Donc pas de panique pour le moment. Il nous reste 5 ans pour étudier l'impact des très hautes fréquences déjà en opérations dans certains pays.

Sur le terrain très glissant de la consommation énergétique, de nombreux efforts ont été demandés aux constructeurs, équipementiers et opérateurs pour réduire de manière très significative (facteur 100 à débit égal). Le fait notamment d'apporter de l'Intelligence Augmentée (IA !) à chaque niveau de la chaîne de valeur, la miniaturisation des éléments vont contribuer à ces économies vertigineuses. Les constructeurs de mobiles travaillent aussi d'arrache-pied sur l'obsolescence prématurée et programmée des milliards de terminaux 4G et 3G notamment sur leur recyclage ou les mises à jour des terminaux.

Enfin, la Commission européenne et l'Agence européenne pour la cyber-sécurité (ENISA) ont publié en 2019 un rapport évaluant les défis de la cyber-sécurité dans les réseaux 5G. Le rapport souligne que les changements technologiques augmentent la surface d'attaque globale et le nombre de points d'entrée potentiels pour les acteurs de la menace.

Quelques scénarios possibles pourraient s'avérer difficiles à gérer avec la 5G. Cela s'explique en partie par le fait que les réseaux ont une architecture moins centralisée et par l'utilisation accrue de logiciels dans les équipements 5G.

En 2020, la Commission Européenne a publié une boite à outils « cyber-sécurité » : son objectif est de définir une approche européenne coordonnée fondée sur un ensemble commun de mesures visant à atténuer les principaux risques en matière de cyber-sécurité des réseaux 5G qui ont été recensés dans le rapport sur l'évaluation coordonnée des risques dans l'UE.

Elle vise également à donner des orientations pour la sélection et la hiérarchisation des mesures qui devraient faire partie des plans d'atténuation des risques tant au niveau national qu'à l'échelon de l'UE. Le but ultime est de créer un cadre solide et objectif de mesures de sécurité qui garantira un niveau adéquat de cyber-sécurité des réseaux 5G dans toute l'UE, dans le cadre d'approches coordonnées efficaces entre les États membres. L'approche adoptée est fondée sur les risques et uniquement motivée par des raisons de sécurité. Cette approche est pleinement conforme à l'ouverture du marché intérieur de l'UE tant que les exigences de l'UE en matière de sécurité sont respectées.

La cyber-sécurité doit aussi être prévue dès la conception des objets connectés qui coexisteront par millions/milliards et encadrée pour assurer la sécurité des réseaux. La France a répondu aux inquiétudes par une loi (« la loi Huawei ») qui prévoit que toute personne qui veut mettre en place un réseau 5G devra obtenir une certification validée par l'ANSSI. Un nouveau dispositif de contrôle des équipements télécoms a été mis en place, conduit par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Ce dispositif s'applique quel que soit l'équipementier et son pays d'origine.

La fusée a 3 étages est partie et nous allons être les témoins vivants d'une révolution technologique et industrielle sans précédents… 'Stay tuned ' !!

Jean-Philippe Pagès

PARTIE 04

Résilience d'entreprise : un avantage concurrentiel face à la crise cyber

04

Regard de Bessé

Jean-Philippe Pagès
Directeur Bessé Industrie & Services

« Cyber-résilience : du risque à l'opportunité ! »

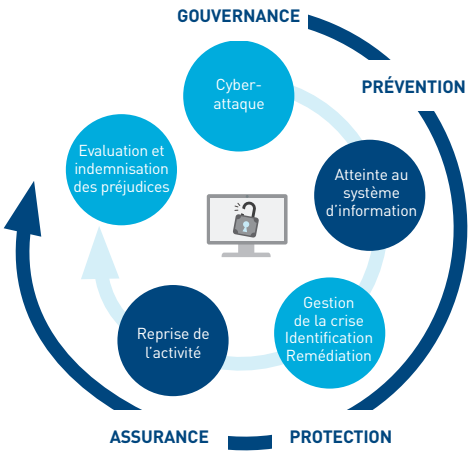
Crises pandémiques, risques technologiques, épuisement des matières premières, dérèglement climatique, instabilité géopolitique, catastrophes naturelles, mouvements sociaux, vulnérabilité des chaines d'approvisionnement ... La liste des risques menaçant la solvabilité des entreprises de toute taille et de tout secteur n'a jamais été aussi longue. L'analyse détaillée des défaillances reposant sur l'évaluation des impacts financiers (pertes d'exploitation, frais additionnels, pertes matérielles, etc.) à partir de scénarios d'interruption des activités a longtemps permis aux risk managers d'optimiser les ressources nécessaires à la gestion des risques de leur entreprise et d'évaluer les besoins en assurance. Ce modèle doit désormais être adapté face à la complexité, l'intensité et la fréquence des risques cyber.

La valeur patrimoniale des entreprises est en risque

Les conclusions de cette première étude réalisée par Guy-Philippe Goldstein traitant de l'impact des menaces cyber sur les entreprises non cotées sont sans appel : les enjeux stratégiques sont considérables puisqu'ils aggravent le risque de défaillance des entreprises et s'attaquent à leur valeur patrimoniale. Dans la plupart des cas, la médiatisation des évènements cyber provoque une dégradation immédiate de la notoriété des sociétés ciblées, même lorsque celles-ci ne subissent pas de détérioration prolongée de leur capacité d'exploitation. Les conséquences sont quasi-irrémédiables : perte de confiance des investisseurs, détérioration des parts de marché et du potentiel de croissance. L'ensemble de ces facteurs menacent non seulement la survie des entreprises touchées mais aussi celle du tissu économique connecté.

La résilience au cœur de la gouvernance des entreprises

Face à cette menace cyber croissante, le concept de résilience organisationnelle est devenu un modèle stratégique de gouvernance indispensable à la pérennité de nombreux acteurs économiques. C'est aussi un avantage concurrentiel indéniable dans un contexte de plus en plus incertain. Le principe de la résilience est simple : garantir en situation de crise un niveau d'exploitation répondant aux attentes des clients et autres partenaires commerciaux, maintenir un climat de sécurité pour l'ensemble des collaborateurs et anticiper les besoins en ressources financières, technologiques, opérationnelles et humaines nécessaires au déploiement d'une gestion de crise efficace.



Quelles sont les principales caractéristiques d'une entreprise résiliente face au risque cyber ? Quelles sont les solutions à mettre en place ? Comment maintenir un niveau de résilience efficace ? Quelle est la valeur que peut apporter l'assurance dans le traitement du risque résiduel ? Pour répondre à ces questions, le rôle de l'équipe dirigeante, la culture d'entreprise, les axes stratégiques dictant la mise en place d'une gestion des risques pertinente, la nécessité d'impliquer l'ensemble des fonctions clés de l'entreprise sont des aspects essentiels à aborder.

Le rôle moteur de l'équipe dirigeante

La prise de conscience du comité de direction de la menace cyber est indispensable au développement d'un modèle d'activité résilient. Afin de mener leur mission à bien, les risk managers qui, dans la plupart des cas sont responsables du développement, de l'amélioration et de la mise à jour des solutions de gestion de crise dépendent fortement de l'implication des membres du Comex.

Les équipes dirigeantes ayant déjà été confrontées à des situations de crise grave n'hésiteront d'ailleurs pas à user de leur influence pour accélérer la mise en place et le maintien des ressources nécessaires au niveau de résilience requis. On s'aperçoit alors que la gestion des risques devient un élément incontournable de la gouvernance d'entreprise où les décisions stratégiques (investissements opérationnels et technologiques, développement commercial, projet de fusion acquisition, etc.) sont prises en parfaite connaissance de l'évolution des risques encourus.

Les risques cyber concernent l'ensemble des fonctions de l'entreprise.

Contrairement à certaines idées reçues, la menace cyber n'est pas que l'affaire des responsables informatiques. Investir dans des solutions de gestion du risque inadaptées à la réalité économique et commerciale de l'entreprise reviendrait à ne pas agir contre cette menace. C'est pour cette raison que les fonctions essentielles de l'entreprise doivent aussi pleinement participer à la gestion du risque cyber. L'implication des responsables opérationnels, du management financier, des ressources humaines, de la supply chain ou du développement commercial est indispensable à la définition d'objectifs de continuité et de résilience en phase avec la stratégie de l'entreprise.

La culture du risque inscrite dans l'ADN de l'entreprise

La résilience d'une entreprise ne dépend pas seulement de la volonté de l'équipe dirigeante et de la mise en œuvre d'un mode de gouvernance transverse. Le turnover impactant tous les niveaux hiérarchiques de la plupart des entreprises fragilise l'efficacité des programmes de gestion des risques en place. Pourtant, certaines entreprises parviennent à maintenir une culture du risque forte malgré les changements fréquents de direction ou de personnel clé.

Dans certains cas, la nature des activités de l'entreprise justifie une maîtrise sans faille des risques. Certains industriels de la chimie ou de la pharmaceutique par exemple sont exposés à des risques industriels, environnementaux ou biologiques conséquents. La maitrise de ces risques fait donc partie intégrante de leur expertise et de leur culture d'entreprise.

Dans les secteurs à fort contenu technologique, la résilience est devenue tout aussi primordiale puisqu'elle apporte un avantage compétitif différenciant. C'est le cas de groupes spécialistes de la transformation digitale et du numérique, ainsi que du milieu de la finance qui, tout en faisant face aux risques cyber et autres indisponibilités informatiques, garantissent malgré tout à leurs clients un accès permanent aux produits et services qu'ils commercialisent.

La mise en place de solutions parfaitement appropriées à la stratégie définie.

Les solutions améliorant la résilience d'entreprise face aux risques cyber sont multiples : prévention et amélioration physique et numérique des risques, gestion de la continuité des activités et de reprise d'exploitation, maîtrise de l'élément humain, reconfiguration opérationnelle et transformation digitale, transfert du risque résiduel vers l'assurance. Il est avant tout essentiel de définir une stratégie à adopter et des objectifs commerciaux, financiers ou opérationnels à atteindre en situation de crise. Cette étape critique et trop souvent négligée permet d'identifier les mesures les plus appropriées qui doivent être implantées conjointement et de façon à optimiser les chances de survie en situation de crise.

La valeur de l'assurance comme outil de traitement du risque résiduel

La multiplicité et la gravité des attaques cyber ne cessent de croître et vont continuer à croître proportionnellement à la digitalisation de nos économies, de nos entreprises et de leurs écosystèmes.

5G, objets connectés, intelligence artificielle, demain ordinateur quantique seront les prochains facteurs de progrès accélérant cette transformation inhérente à nos sociétés et à nos usages.

Dans ce contexte d'évolution et donc d'aggravation permanente du risque cyber, le risque zéro, celui pour une entreprise de ne jamais être victime d'un attaquant ayant réussi à contourner toutes ses défenses, y compris toutes celles au meilleur état de l'art, de fait n'existe pas et, n'a jamais existé.

Sur un marché naissant de l'assurance dont les challenges existentiels sont nombreux, évaluation et quantification du risque mais surtout management de son caractère systémique, l'assureur ne pourra jouer pleinement son rôle et financer efficacement dans la durée le risque résiduel que l'entreprise souhaite lui transférer que si celle-ci contribue à l'analyse en profondeur de celui-ci.

L'entreprise, de ce point de vue aussi, s'inscrira dans le cadre de sa stratégie de cyber-résilience.

A ce titre, par exemple, au-delà de la mise en œuvre de prévention et de protection adaptées, elle cherchera au titre de sa cartographie des risques à quantifier finement les conséquences financières d'une attaque cyber, frais de gestion de crise, pertes d'exploitation sans dommage, tous autres frais supplémentaires, et l'impact potentiel sur son bilan de façon à transférer à l'assureur le risque le plus précisément dimensionné.

Avec le même objectif, elle pourra également intégrer cette recherche constante de la mesure des impacts financiers lors des exercices de simulation de crise cyber régulièrement réalisés.

C'est ainsi que l'entreprise bénéficiera de toute la valeur de son transfert de risques à la faveur de l'indemnisation obtenue lors du sinistre qui favorisera la vitesse et l'efficacité de son rebond une fois la crise maîtrisée.

Risque cyber : du risque à l'opportunité

L'étude de Guy-Philippe Goldstein démontre qu'une entreprise ayant un modèle d'activité résilient parvient à stabiliser plus facilement ses flux de trésorerie et sa valeur patrimoniale face à la menace cyber. La résilience est devenue un vecteur important de bonne santé financière qui assurera un retour sur investissement à un moment ou à un autre si elle fait partie intégrante de la cuture de l'entreprise.

La gestion des risques cyber n'échappe pas à cette règle : la prise de conscience du comité de direction, la définition d'une stratégie de résilience précise basée sur un constat réaliste de la menace, le déploiement homogène de solutions préventives et de gestion de crise, une politique de maintenance et de mise à jour des programmes de gestion des risques et des assurances permettront à de nombreuses entreprises de se préserver des risques cyber.

Comme souvent, ce sont les mieux armées qui, non seulement parviendront à rebondir à l'issue de la crise mais en tireront un avantage concurrentiel fort et durable, gage de pérennité rentable de leurs activités.

EN CONCLUSION

Agissons ensemble pour la cyber-résilience des entreprises et créons de la valeur.

En mars 2018, avec PwC, nous produisions « Les dirigeants d'ETI face à la menace Cyber ». De cette étude ressortait un paradoxe majeur : souvent conscients de la réalité de ce risque de nouvelle génération, très peu y consacraient les moyens permettant d'identifier leurs vulnérabilités et de se préparer à la crise.

18 mois plus tard, en novembre 2019, nous publions une nouvelle enquête réalisée pour notre compte par l'IFOP. Elle montrait une perception plus forte du caractère stratégique de risque cyber chez les dirigeants mais toujours une large sous-estimation de leur exposition.

Nous concluions dans les deux cas à la nécessité d'organiser la cyber-résilience des ETI et Bessé appelait au partage d'expérience par la création de Cercles d'échanges.

Aidée par les témoignages des victimes d'attaques cyber dont la fréquence et l'intensité augmentent de jour en jour, la prise de conscience enfin est aujourd'hui réelle. **Les dirigeants savent désormais et veulent agir.**

Novembre 2020 : cette troisième étude est ainsi naturellement ciblée vers l'action, en commençant par le diagnostic des conséquences financières de la crise. Elle met en évidence l'accroissement du risque de défaillance créé par l'attaque cyber et son effet sur la valeur patrimoniale de l'entreprise.

Elle pose la question de l'évaluation des pertes financières directes consécutives à la crise mais aussi celles des pertes indirectes plus difficilement mesurables : image, réputation, expérience client, attractivité, climat interne, rétention et recrutement. Il est en effet généralement admis que les pertes indirectes peuvent être bien supérieures aux pertes directes avec des effets à long terme potentiellement beaucoup plus déstructurants.

Les regards portés par les personnalités sur les résultats de l'étude sont reliés les uns aux autres par un fil rouge : la recherche de la résilience de l'entreprise et le rôle clé des dirigeants pour la mener.

Caroline Ruellan nous donne un éclairage précieux : la première réponse à la crise cyber est **le discernement du dirigeant.**

Laurent Porta propose aux dirigeants **les axes concrets de leur préparation** pour réussir leur gestion et leur communication de crise cyber.

Enfin, François Barrault en projetant dans un avenir très proche la nouvelle révolution numérique, la 5G, nous montre **l'extension exponentielle de la menace** et du champ d'action des cyber-attaquants.

La question n'est donc plus de savoir si l'entreprise sera touchée, ni même quand, mais comment elle saura réagir efficacement à la crise lorsqu'elle surviendra !

Alors la cyber-résilience organisée et démontrée deviendra un atout concurrentiel créateur de valeur pour l'entreprise au sein de son écosystème.

Pierre Bessé
Président de Bessé

#ÉPIGRAPHE

1 Le questionnaire semestriel de la Banque d'Angleterre auprès de représentants des institutions financières de la City de Londres citait ainsi les cyber-risques comme le 2ème risque le plus important après le risque politique propre au Royaume-Uni pour les firmes représentées lors de l'évaluation du 2ième semestre 2019, évoquée presque la moitié du temps. Dans la première moitié de la décennie, le risque cyber n'avait jamais dépassé le 13ième rang (Voir Bank of England, Systemic Risk Survey, 2019 H2, disponible à https://www.bankofengland.co.uk/systemic-risk-survey/2019/2019-h2). De même, dans le Global Risk Survey du World Economic Forum publié en janvier 2020, sur les risques pour les affaires, les cyber-attaques arrivaient en première position aux Etats-Unis, mais également au Royaume-Uni et aussi en France (voir http://reports.weforum.org/global-risks-report-2020/survey-results/global-risks-of-highest-concern-for-doing-business-2020/#country/FRA). La question est devenue critique.

2 Voir Financial Times https://www.ft.com/content/13bed6c2-dd89-4c22-a86a-d9a584dd2b06

3 Voir http://www.leparisien.fr/high-tech/hausse-des-cyberattaques-pendant-la-crise-du-covid-19-comment-proteger-ses-donnees-27-05-2020-8324358.php et https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/

4 Voir https://www.helpnetsecurity.com/2020/05/28/external-attacks-on-cloud-accounts/

5 Par exemple : intervention technique de remédiation, frais de communication, frais juridiques, pertes nettes en termes de chiffres d'affaires non récupérables, augmentation temporaire de la structure de coût dans la période de travail dégradé, etc...

6 CGI et Oxford Economics au Royaume-Uni observent que les cours de bourses baissent de manière structurelle de 1.8 % après une cyber-attaque. Pour une entreprise cotée du FTSE100, cela équivaudrait à une perte de GBP 120 millions. L'étude observe également que les impacts boursiers sont plus forts au fur et à mesure des années : la baisse observée entre l'annonce de l'incident et le vendredi qui suit n'est que de -0.2 % en 2013, mais -1.5 % en 2014 et -2.7 % en 2015/2016 (voir https://www.cgi.com/sites/default/files/2018-08/cybervalueconnection_full_report_final_lr.pdf p. 4 et p.10). L'étude Comparitech de 2019 sur 33 incidents montre une sous performance par rapport au NASDAQ de -4.2 % dans les 14 premiers jours en moyenne, puis -6.5 % en moyenne sur les 12 premiers mois et même -13.3 % sur 2 ans (Voir https://www.zdnet.com/article/this-is-how-a-data-breach-at-your-company-can-hit-share-prices/)

7 https://www.hbrfrance.fr/chroniques-experts/2018/05/20164-valeur-de-lentreprise-a-lepreuve-cyber-attaques/

8 Certaines études sur les entreprises cotées aux Etats-Unis et au Royaume-Uni ont montré que la réputation contribue à hauteur de 30 à 40 % de la valorisation pour respectivement les entreprises du FTSE100 et les 250 entreprises les plus importantes du S&P500. Cependant, cette contribution de la réputation à la valorisation de l'entreprise varie énormément en fonction de la taille de l'entreprise. Elle redescend à 12 % de la valeur pour les 250 entreprises les plus petites du S&P500 (Voir Reputation Dividend Reports, 2012-2018) , mais peut monter jusqu'à autour de 55 % de la valeur pour des très larges capitalisations mondiales telles que Shell ou Unilever (Voir https://www.echoresearch.com/images/uploads/media/UK_Reputation_Dividend_Report_Feb_2018.pdf). On peut donc considérer que pour des ETI cotées, ces effets réputationnels restent à contrario relativement modérés, et donc que l'augmentation de volatilité par rapport à des ETI non cotées demeure limitée.

9 Une étude du World Economic Forum montre en effet que pour les entreprises non cotées au niveau mondial, une croissance de la taille d'un écart-type est associée avec une croissance de l'endettement de 24 %, mais en réalité une croissance de 37 % de la dette court terme et 19 % de la dette long terme soit la moitié de la dette court terme (Voir WEF https://www.weforum.org/agenda/2019/02/differences-in-the-borrowing-behavior-of-public-and-private-firms/; et également https://www.nber.org/papers/w25226). On notera qu'au contraire, les entreprises cotées sont capables de mieux augmenter la part en capital au détriment de la dette court terme dans un premier temps de croissance ; puis avec une taille plus grande d'augmenter en réalité la part de la dette long terme – l'ensemble offrant une structure moins risquée.

10 https://rodneywhitecenter.wharton.upenn.edu/wp-content/uploads/2014/04/24.14.Gilje_.pdf. On notera, en outre, que les entreprises produisant de manière régulière de l'information financière sur leurs situations arrivent à plus facilement obtenir des facilités de crédit court et moyen terme – et c'est évidemment le cas des entreprises cotées par rapport aux entreprises non cotées (Voir https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1264730&rec=1&srcabs=1931164&pos=7)

11 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1931164

12 http://faculty.haas.berkeley.edu/manso/fms.pdf

13 de 3 à 5 par entreprise « victime » de cyber-attaques, sélectionnées par Altarès / Dun & Bradstreet

14 Une étude de modélisation, reprenant des valeurs types pour une entreprise américaine, a identifié que dans cet exemple « standard », une augmentation de 1 % de la probabilité de défaut pouvait réduire la valeur des dettes long terme de 17 % et également réduire de 21 % la valeur du capital de l'entreprise de 21 % (Voir Jennergren, L. Peter. «Firm Valuation with Bankruptcy Risk.» Journal of Business Valuation and Economic Loss Analysis 8.1 , 2013) . D'autres approches de valorisation plus simples en fonction d'un modèle de croissance ont montré que selon l'incrément en termes de risque de défaut (de 0 % à 5 %) et selon le taux de croissance continu de l'entreprise (de 0 % à 8 % par an), la réduction de la valeur de l'entreprise suite à une augmentation de 1 % de la probabilité de défaut pouvait aller de -8 % à -36 % (voir Kenth Skogsvik, "Probabilistic Business Failure Prediction in Discounted Cash Flow Bond and Equity Valuation", SSE/EFI Working Paper Series in Business Administration 2006:5, May 2006) . La magnitude des impacts est conservée. Ces ensembles de valeurs permettent d'établir une évaluation conservative de la perte en termes de valorisation liée à une augmentation de la probabilité de défaut.

15 On pourra d'ailleurs noter que dans les scores Altarès / Dun & Bradstreet, ces valeurs correspondent assez bien aux seuils entre « risque faible à modéré » et « risque modéré à élevé », la majorité des scores de défaillance (11 sur 20) se situant justement entre la probabilité 0 % et 1.7 %.

16 https://www.zdnet.fr/blogs/green-si/la-communication-virale-de-norsk-hydro-

39883119.htm

17 https://www.ouest-france.fr/bretagne/finistere/une-charte-contre-la-cyber-criminalite-5355415

18 https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

19 En ce sens, l'analyse rejoint certaines conclusions de l'étude IRT SystemX sur 60 entreprises françaises (essentiellement des PME de moins de 50 personnes et des TPE) qui dans les coûts indirects relativise l'impact des coûts de réputation et revalorise l'impact sur l'organisation elle-même, y compris dans les aspects intangibles de confiance dans l'organisation collective de l'entreprise.

20 https://www.informatiquenews.fr/80-des-entreprises-francaises-nont-pas-de-plan-de-reponse-aux-incidents-de-cybersecurite-71584

CB.IARD (commercialement dénommée « Bessé Industrie & Services ») Ecrire à : 46 bis rue des Hauts Pavés – BP 80205 - 44002 Nantes Cedex 1
SAS au capital de 253 545 € - Siège social : 135 Boulevard Haussmann 75008 Paris - RCS Paris 873 800 023
Conseil et courtier en assurances (exerçant conformément à l'article L521-2-1°b) du Code des assurances)
N° Orias 07 022 453 – www.orias.fr Soumis au contrôle de l'ACPR – 4 place de Budapest 75009 Paris
Liste des fournisseurs actifs disponible sur www.besse.fr
Toute réclamation ou demande sur les procédures de médiation peut être adressée par écrit au Service Réclamation Bessé Industrie & Services 46 bis rue des Hauts Pavés – BP 80205 - 44002 Nantes Cedex 1.
Vous recevrez un accusé de réception sous 10 jours maximum et une réponse dans un délai maximum de 2 mois.

Desing / studio.annabelleb.com - Impression / Alliance Partenaires Graphiques, Reims