RÉSULTATS DE L'ENQUÊTE
BESSÉ - PwC

MARS 2018

LES DIRIGEANTS D'ETI FACE À LA MENACE CYBER

BESSÉ
CONSEIL EN ASSURANCES

pwc

de **M. FRÉDÉRIC SANCHEZ**
Président du Groupe FIVES
Président du MEDEF International

Je tiens ici à saluer cette étude réalisée conjointement par BESSÉ et PwC sur les risques Cyber. Je les remercie sincèrement de cette initiative sur un sujet qui nous concerne tous : les ETI bien sûr, mais aussi tous les acteurs économiques, sans distinction.

Digitalisation, Big Data, Intelligence Artificielle vont façonner notre futur. A l'heure où le monde se transforme à la vitesse « V », sous l'effet de cette révolution digitale, le champ des possibles ne cesse de s'étendre en même temps que la taille des défis à relever s'accroît. Le risque Cyber en est un, et non des moindres, au vu des menaces qui pèsent sur l'intégrité de nos systèmes d'information, la sécurité de nos flux financiers et la protection de nos données.

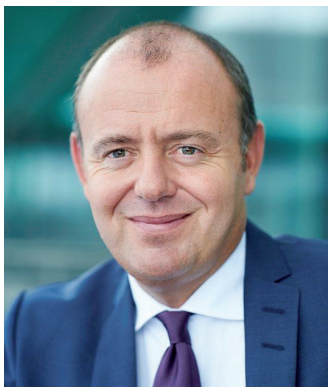
Les vulnérabilités numériques rendent nos entreprises fragiles. Les risques Cyber sont nouveaux, inédits et de nature à fragiliser gravement nos entreprises et nos organisations. Dans ce contexte, cette étude est riche d'enseignements. En tant que Dirigeant, elle ne peut que nous amener à agir pour sinon éliminer, du moins fortement réduire ces risques.

Certes, la menace est invisible, le risque diffus, poreux, le sujet parfois technique. Nous devons le prendre en compte dans toutes ses dimensions ; dimension interne d'abord, en adaptant à ces nouveaux enjeux la gouvernance de nos entreprises et les programmes de formation et de sensibilisation de nos collaborateurs à ces nouveaux risques ; dimension externe ensuite au travers des relations avec nos partenaires, prestataires et clients.
A défaut d'identifier clairement ce que nos entreprises ont à craindre, les moyens mis en œuvre pour gérer les risques Cyber ont toutes les chances d'être inadaptés et sous-dimensionnés.

Face à la singularité de cette nouvelle génération de risques, parfaitement mise en lumière par BESSÉ et PwC, les ETI, et plus largement toutes les entreprises, peuvent-elles agir seules ? La question est légitime car la tâche n'est pas simple d'autant que les compétences à rassembler sont multiples. Les bonnes pratiques en matière de Cybersécurité et les retours d'expériences face aux incidents constatés se doivent aussi d'être partagés. Les enjeux sont collectifs. Je ne peux qu'encourager l'initiative d'une collaboration inter-entreprises appelée de ses vœux par BESSÉ et PwC. Elle a d'ores et déjà tout mon soutien ! J'encourage les Dirigeants d'ETI à les rejoindre ; à s'investir pour que cette belle initiative prenne vie.

PIERRE BESSÉ ET PHILIPPE TROUCHAUD

PIERRE BESSÉ
Président de BESSÉ



PHILIPPE TROUCHAUD
Associé PwC - Spécialiste en Cybersécurité

Voici la première étude sur les Entreprises de Taille Intermédiaire face à la menace Cyber.

Chacun dans notre métier de conseil, nous connaissons bien les ETI, et nous tenons à les accompagner dans ce vaste mouvement incessant du changement.

Nous le savons tous, les ETI sont les forces vives de l'industrie et des services de notre pays. Avec elles, *"France is back"* parce qu'elles investissent et rayonnent sur toute la planète. Ces ETI embauchent, forment et préparent les métiers de demain. Elles ne sont pas toujours connues ou reconnues alors qu'elles développent des savoir-faire, un vrai sens de l'anticipation et une approche réaliste et volontariste de la révolution 4.0.

Comme l'ensemble du monde industriel et des services, ces ETI sont face aux défis de la digitalisation. C'est un changement fondamental qui demande des adaptations humaines et technologiques, crée une disruption majeure avec les habitudes, les savoir-faire, les normes de production de service des ETI. Ce choc de la digitalisation nécessite un changement de paradigme et nous avons voulu le révéler, le concrétiser en écoutant leurs dirigeants.

Nous avons été étonnés par un paradoxe majeur.

Les dirigeants que nous avons interrogés sont tous conscients de la réalité du risque Cyber. Ils le perçoivent comme inquiétant, très inquiétant même. Probablement, parce qu'ils n'ont pas encore aujourd'hui toutes les références, tous les appuis nécessaires pour piloter le développement de la digitalisation, et parallèlement prévenir le risque Cyber qui en résulte.

Cette inquiétude nouvelle est très médiatisée. Elle s'infiltre dans les entreprises sournoisement, sans prévenir, sans qu'un mode d'alerte puisse être réellement mis au point. Les dirigeants et les comités de direction se posent des questions : quelles sont les références ? Qui a déjà été confronté à pareil risque ? Quelles sont les conséquences humaines, commerciales, financières… ?

Se préparer, anticiper et réagir en cas de crise, oui mais comment ? Qui sont les appuis techniques mais aussi juridiques et assurantiels ? Autant de questions que se posent ces dirigeants, autant de réponses partielles, d'inquiétudes réelles, de désarroi parfois, voire même d'attentismes mais aussi des prises de conscience, avec la mise en œuvre de moyens comme les délégations internes ou externes, des investissements pas tous organisés et cohérents, et des groupes de réflexion.

Il faut aller plus loin : connaître, comprendre, organiser la défense contre cette menace. C'est important pour les entreprises et pour leurs équipes. C'est essentiel pour l'avenir économique de nombreuses filières mais aussi de notre pays.

Cette étude n'est qu'une pierre à l'édifice à construire : celui de la Cybersécurité, celui de la Cyber résilience, celui de la sérénité des dirigeants des ETI.

BESSÉ et PwC se sont lancés conjointement dans cette étude parce que notre proximité avec les dirigeants nous a alertés sur le fait que la prise en compte de la menace Cyber par les ETI s'avérait beaucoup plus contrastée que pour les grands groupes, en particulier les sociétés cotées qui ont dans leur ensemble engagé des mesures concrètes. Nous écoutons, nous échangeons et nous ressentons ce besoin de comprendre, d'être rassurés tout en n'imaginant pas toujours que le risque concerne chacun.

Nous avons mobilisé nos forces vives et nos équipes pour échanger en profondeur et recueillir l'expression réelle des dirigeants. Cette écoute est complétée par une étude quantitative et le commentaire de spécialistes. Vous avez ainsi les grandes orientations du sujet, un cadre chiffré et précis pour aborder cette question du risque Cyber.

Nous souhaitons aussi agir, réagir, accompagner les dirigeants. C'est notre métier, celui du conseil avec des champs d'activités complémentaires : la Cybersécurité et les solutions assurantielles. C'est aussi notre engagement, notre devoir. Conseiller, c'est prévoir et rassurer. Aujourd'hui, il y a urgence.

EN SYNTHÈSE, CE QU'IL FAUT RETENIR EN **10 POINTS CLÉS**

1

Les dirigeants d'ETI sont informés et sensibilisés au risque Cyber : 76% des sondés déclarent avoir subi au moins un incident Cyber en 2017.
La forte médiatisation du sujet est également pour eux une source essentielle d'information.

2

Ils ont la vision d'un risque majeur extrêmement complexe dont ils cernent mal les contours précis.
Avec une appréhension réelle, ils sont conscients des menaces.

3

Leur perception du risque et de son étendue est néanmoins relative pour leurs propres entreprises.
En dépit des attaques, ils ne se sentent pas toujours directement exposés.
Ils identifient principalement la menace externe, Cybercriminalité, mais sous-estiment celle des concurrents, ainsi que leurs vulnérabilités internes.

4

Les dirigeants d'ETI ont conscience qu'ils n'ont pas pris en compte toute la dimension stratégique du risque.
Ils ont la vision d'un risque très technique dont ils délèguent souvent la gestion et la prévention à leurs seules équipes informatiques et leurs sous-traitants.
Ils favorisent rarement les postures d'alertes internes.

5

Ils reconnaissent qu'ils sont insuffisamment préparés pour affronter une crise Cyber.

6

Ils reconnaissent aussi qu'ils n'ont pas de vision précise des conséquences financières potentielles d'un événement Cyber.

7

Ils ne perçoivent pas non plus l'assurance Cyber comme un outil prioritaire de traitement efficace du risque faute de l'avoir précisément identifié.

8

La posture rationnelle, voire parfois attentiste des dirigeants d'ETI est compréhensible. Mais elle ne peut être une réponse efficace face à ce risque d'une nouvelle génération dont les spécifictités singulières font qu'il serait vain de rechercher à en acquérir la pleine maîtrise avant d'agir.

9

L'objectif devrait plutôt être d'**organiser la Cyber résilience** des ETI face à cette menace d'une extraordinaire complèxité.
Pour cela, il faut agir, dès à présent, aller plus loin, plus concrètement, pour ensemble favoriser le partage d'expériences, des bonnes pratiques, et **pourquoi ne pas créer un forum d'échanges, voire un cluster Cyber résilience dédié aux ETI** ?

10

Les dirigeants d'ETI sont conscients de ce **besoin de Cyber résilience, créateur de valeur pour leurs entreprises**.

BESSÉ et PwC sont à leur écoute et prêts à les accompagner.

Parlons-en ensemble !

Enquête réalisée en 2017 sur la base d'un échantillon de 432 entreprises interrogées en France et de 50 témoignages de dirigeants d'ETI, Présidents, Directeurs Généraux ou membres des Comités de Direction.

PARTIE 01

Résultats de l'enquête

Témoignages de dirigeants et chiffres clés

01

#1

Les dirigeants d'ETI sont informés et sensibilisés au risque Cyber

Au total, selon l'analyse PwC, plus de 76% des ETI en France déclarent avoir subi au moins un incident Cyber en 2017.

La forte médiatisation du risque Cyber est le principal levier d'information et de sensibilisation des Dirigeants d'ETI.

Les Dirigeants sont désormais très réceptifs en raison des attaques Cyber qui affectent leurs organisations.

Pour l'échantillon de dirigeants que nous avons interrogés, les attaques sont régulières, voire permanentes. Certains parlent de dizaines d'incidents qu'ils sont parvenus à déjouer.

Mais certains ne l'ont pas été !

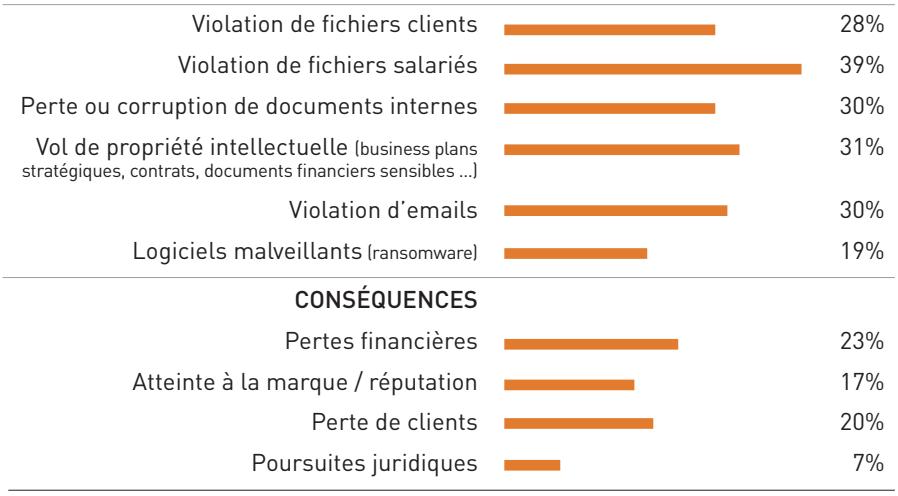
Des dirigeants relatent des faits très concrets : vol de données sur un serveur R&D, virus sur une filiale en Asie avec demande de rançon,... *« Nous avons eu sept attaques signifcatives depuis 2014, des virus ou des tentatives pour pénétrer nos systèmes »*, témoigne l'un d'entre eux.

Sont cités aussi régulièrement les appels pour obtenir des virements, ainsi que les tentatives de fraude bancaires et de chantage au président.

Les attaques laissent des souvenirs très précis et les dirigeants racontent en détail : *« Nous avons, par exemple, observé dans notre base de données comptable le changement de RIB d'un fournisseur : le nouveau RIB était sur une banque polonaise…»*

Types d'incidents subis par les ETI en France :

France



Source : PwC Source : PwC, Enquête Global State of Information Security Survey (GSISS) 2017.
Un répondant peut cumuler plusieurs nature d'incidents.

#2

Les dirigeants d'ETI ont la perception d'un risque extrêmement complexe

D'une manière générale, les dirigeants interrogés ne sont pas parvenus à donner une définition précise à la notion de risques Cyber. Un temps de latence a été régulièrement enregistré entre la question *« Comment définiriez-vous les risques Cyber pour l'entreprise ? »* et la réponse lors des entretiens.

COMPLEXITÉ EXPONENTIELLE DU CYBERESPACE

Les usages numériques évoluent de manière exponentielle depuis les années 2000.

Depuis 2000 les équipements utilisés par les employés de l'entreprise augmentent en nombre. Chaque employé peut aujourd'hui disposer d'un mobile, d'une tablette et de plusieurs ordinateurs, outils d'efficacité opérationnelle qui ouvrent le système d'information de l'entreprise au monde extérieur.

L'innovation des entreprises qui produira de nouveaux objets connectés sur Internet fera, au cours des prochaines années, augmenter de manière exponentielle l'exposition des entreprises sur Internet et donc son risque Cyber.

Par ailleurs, la complexification des systèmes augmente la probabilité de vulnérabilités. A titre d'exemple, le nombre de lignes de code source d'un cœur de système d'exploitation « *Linux* » a été multiplié par 10 pour atteindre plus de 20 millions de lignes. Comment maîtriser cette complexité à l'échelle humaine ?

Ce point étonne puisque les dirigeants sont directs et précis lorsqu'ils abordent les autres risques bien appréhendés que sont les risques sociaux, opérationnels, commerciaux ou financiers.

Pour la plupart, le risque Cyber est assimilé à la fraude, en particulier au cas d'ingenierie sociale dit de *« Fraude au Président »*.

Au travers de nos échanges, les interlocuteurs constatent cependant que ces risques Cyber sont de diverses natures.

Certains ont conscience d'une origine plus clairement identifiée avec la digitalisation des processus de leurs entreprises, qui crée une vulnérabilité potentielle. Plus l'entreprise est dématérialisée, plus elle est exposée. Et plus elle progresse, plus elle sera dématérialisée, digitalisée, ... et donc exposée à des risques de grande ampleur. C'est un constat qui ne se fait pas de façon naturelle.

En résumé, ce qui semble le plus significatif est *« la conscience d'une action criminelle ou frauduleuse liée aux SI pour créer un dysfonctionnement ou tenter de soutirer des rançons »*.

La transformation digitale est donc très clairement perçue comme un facteur d'aggravation du risque. Les dirigeants d'ETI ont le sentiment de subir cette situation. Ils ont conscience de la complexité exponentielle du Cyberespace, et qu'il en résulte des menaces qui ne vont cesser de s'amplifier.

#3

Les dirigeants d'ETI ont une perception relative du risque pour leurs entreprises.

ORIGINES DES MENACES

INTERNES	France
Employés	**30%**
Fournisseurs de services / consultants / contractants	**32%**
Partenaires	**18%**
Clients	**12 %**

EXTERNES	France
Hackers	**25%**
Crime organisé	**17%**
Activistes	**25%**
Concurrents	**34%**

Source : PwC, Enquête Global State of Information Security Survey (GSISS) 2017. Un répondant peut citer plusieurs sources d'incidents.

Cela n'arrive que chez les autres !

Malgré le grand nombre de dirigeants d'ETI qui signale avoir subi une Cyber attaque, on constate que les dirigeants interrogés ne se rendent pas compte spontanément que leur propre entreprise est concernée par ces risques.

Certains n'y croient pas : *« Cela arrive aux autres, le sabotage est impossible chez nous. »* (rires)

D'autres enfin se justifient par leur activité B to B : *« Nous sommes une entreprise en B to B qui n'est pas connue du grand public et certaines activités sont très certainement bien plus exposées que nous, notamment le secteur banque assurance ou la grande distribution - compte tenu de la nature et de la quantité de données que ces secteurs sont amenés à gérer. »*

Rares sont les dirigeants qui identifient de manière globale la nature exacte des risques qui pèsent sur leurs activités au regard des atteintes pouvant potentiellement affecter leurs systèmes d'informations et les données qu'ils contiennent. La vision est le plus souvent parcellaire et limitée à ce qui est facilement identifiable ou visible.

La grande majorité des dirigeants perçoit la menace Cyber comme une menace essentiellement externe, d'origine criminelle, motivée par des objectifs financiers

Dans les faits, cette perception est contredite par notre étude puisque, en France, les incidents Cyber imputables à des sources externes ne sont que de 25% pour les hackers et de 17% pour les réseaux de criminalité organisés.

Cette perception est probablement dûe à l'assimilation que nous avons constatée du risque Cyber aux cas de fraude très fréquemment cités, même lorsque ceux-ci ne relèvent pas toujours de risques Cyber en tant que tels.

D'une manière frappante : la menace interne est largement sous-évaluée par les dirigeants

En ce qui concerne les employés, tous les dirigeants peinent à croire

qu'ils puissent être impliqués dans les attaques. On se réfère aux valeurs, à l'éthique de l'entreprise, à la confiance... Il est difficile d'admettre que cela pourrait venir des personnels. On se réfère aussi aux règles mises en œuvre : *« Non, nous avons bien sûr des règles stipulées dans les contrats de travail, des procédures particulières qui permettent de tracer les actions de ceux qui entrent sur nos serveurs. ».*

Lorsqu'on leur pose la question, moins d'un dirigeant interviewé sur deux estime que le risque d'un incident Cyber est susceptible de provenir de l'interne. Cela se traduit par une politique interne de sensibilisation et de prévention souvent insuffisante.

Dans les faits, on note tout de même que 30% des sociétés françaises sondées témoignent que ces attaques proviennent d'employés actuels et 24% d'anciens employés. La menace interne est majeure et ne doit donc pas être sous-estimée.

Cette donnée statistique mérite cependant d'être nuancée dans la mesure où les employés ne sont pas véritablement les auteurs d'une attaque Cyber mais en sont avant tout les vecteurs, en favorisant par exemple, la propagation de malware après avoir négligemment cliqué sur une pièce jointe à un mail. Ces attaques Cyber par email font partie des types d'attaques les plus répandus.

A la question *« Vous sentez-vous concerné au niveau de votre entreprise ? »* la réponse est claire : *« Oui, c'est un vrai sujet. Nous sommes défaillants, je pense que nos systèmes ne sont pas assez protégés. »*. Cette réponse est largement partagée et complétée : *« Nous ne sommes pas entrés dans une phase très active pour nous protéger. »*

Leur perception des risques potentiels, dont les concurrents ou les partenaires pourraient être la source, est limitée.

On touche là à une certaine culpabilité mêlée d'intérêt.

Dans les faits, les sources d'attaques dont sont victimes les entreprises sont multiples. Elles seraient imputables :

DANS

32%

des cas aux interconnections avec leurs fournisseurs de services, consultants et contractants passés.

DANS

34%

des cas à leurs concurrents

SEULEMENT DANS

17%

des cas à la Cyber criminalité organisée.

Les incidents imputables à l'externe (hackers ou conccurrents) ont décliné entre 2016 et 2017, alors que ceux imputables à l'interne (employés, fournisseurs de services, consultants...) ont stagné voire même augmenté !

#4

Les dirigeants d'ETI ont conscience qu'ils n'ont pas encore intégré toute la dimension stratégique du risque Cyber et que leurs entreprises ne sont pas structurées en conséquence

L'enquête démontre que les dirigeants d'ETI considèrent le risque Cyber plutôt comme un risque technique que stratégique.

Ils n'ont pas encore tous structuré leurs entreprises en conséquence et souvent ne s'en inquiètent pas outre mesure, car beaucoup ne se perçoivent pas encore comme des cibles potentielles.

Certains adoptent une attitude plutôt résignée en constatant que même les plus grandes organisations étatiques se font pirater.

Pour d'autres, les très grands groupes et les acteurs en B to C sont en premier lieu concernés.

Cela se traduit par les trois principaux constats suivants :

1 Les dirigeants n'ont pas encore tous défini une stratégie de Cybersécurité et organisé une gouvernance du risque structurée et transversale au sein de leurs entreprises

Seules 49% des sondées déclarent avoir mis en place une stratégie de Cybersécurité.

De plus, ces chiffres paraissent élevés en comparaison des propos recueillis en entretiens : au même titre que les dirigeants ne formulent pas une définition précise du risque Cyber, ils appréhendent encore mal le concept de stratégie de Cybersécurité qui revêt pour eux des contenus variables, allant du système le plus sophistiqué de détection et gestion des incidents, jusqu'à une simple charte de sécurité affichée sur le mur d'un bureau. Ceci révèle que beaucoup ont peut-être le sentiment d'être protégés contre les éventuelles attaques, alors que ce n'est pas le cas. On touche alors à un effet relativement pervers : l'illusion d'être protégé sans que ce ne soit réellement le cas accroît alors la vulnérabilité de l'entreprise.

Seules 39% des ETI sondées déclarent avoir mis en place une organisation transversale associant les fonctions Finance, Juridique, Ressources Humaines, Opérationnelles, SI et RSSI pour piloter le risque Cyber au sein de leurs entreprises.

D'un point de vue plus opérationnel, les ETI ne sont plus que 32% à déclarer avoir mis en place une procédure de gestion des incidents de sécurité impliquant la Direction Générale.

La manière d'identifier les menaces est symptomatique de ce manque de structuration, de stratégie et de gouvernance.

Pour les dirigeants interviewés qui signalent avoir été victimes d'attaques, à la question : *« comment avez-vous identifié ces attaques ? »*, les réponses ont souvent mentionné que l'identification est aléatoire. Manifestement, les incidents réguliers ne remontent pas à la direction générale et il n'y a pas de procédure précise et écrite d'identification et d'analyse des alertes.

L'origine de l'information des managers est incertaine et non codifiée :

- Quand l'incident est important : rançon, blocage,... Le manager est informé, généralement via la DSI ou la direction financière. L'information est remontée à la Direction générale, mais sans organisation précise.
- Pour certains, cela vient des prestataires : *« nous externalisons chez notre prestataire d'e-cloud et c'est lui qui a identifié l'attaque »*, nous confie un dirigeant.

Nous constatons en règle générale que les alertes ne sont pas remontées, elles sont réglées par la DSI, dont on estime que *« c'est le boulot »*.

En synthèse, on constate un manque de méthode d'alerte, et une absence de partage par les équipes de direction.

2 Très peu d'ETI disposent d'une cartographie spécifique de leurs vulnérabilités d'origines externes et internes

Des entreprises interviewées, très peu ont véritablement établi une cartographie précise de leurs expositions face aux risques Cyber. Ce constat n'est pas surprenant. L'exercice est en effet complexe, d'autant plus que les menaces sont mouvantes et que l'organisation des SI est en perpétuelle évolution.

En allant plus précisément au fond de la question, on s'aperçoit que la cartographie des risques est une notion relativement vague. Elle reprend un ensemble de risques variables selon les entreprises et les risques Cyber ne sont pas toujours clairement identifiés.

Les dirigeants témoignent que leurs entreprises ne savent pas toujours comment utiliser cette cartographie et notamment faire le lien avec un plan d'action.

La cartographie reste très incertaine quant à sa réalisation, le champ d'investigation, le positionnement des risques Cyber, la fréquence, l'actualisation et l'utilisation pour mettre un place un plan d'action. Nous sommes dans un flou assez général, sauf pour les entreprises qui ont une activité B to C, lesquelles sont plus armées dans la mesure où nous avons vu qu'elles étaient perçues (et se percevaient elles-mêmes) comme des cibles plus vulnérables aux Cyber attaques.

3 Le risque Cyber n'est donc pas encore perçu comme stratégique mais comme technique par les Dirigeants qui s'en remettent à leur DSI

Beaucoup de dirigeants considèrent que la Cybersécurité est essentiellement l'affaire du DSI ou du Responsable de la Sécurité Informatique.

Seuls 30% des DSI des ETI rapportent directement aux DG, d'un point de vue hiérarchique et fonctionnel.

Dans les différents entretiens, nous constatons une excellente inclusion de la DSI dans les groupes ou entreprises comme un service transverse indispensable, reconnu et compétent.

Cette très grande délégation de confiance fait que 56% des dirigeants d'ETI sondés témoignent qu'ils ne s'investissent pas dans la Cybersécurité de l'entreprise.

Dans l'esprit des dirigeants, cette même DSI a donc la responsabilité de gérer les risques Cyber perçus avant tout comme des risques technologiques.

En règle générale, la Direction Financière, hormis sur les questions de budgets, et les Directions métiers sont très rarement impliquées. La DRH l'est par contre indirectement dans les entreprises pour lesquelles la prévention des salariés est mise en place.

#5

Les dirigeants sont conscients qu'ils sont insuffisamment préparés en cas de crise

L'enquête constate que les dirigeants sont conscients de leur réelle impréparation à pouvoir gérer un incident Cyber significatif dans toutes ses composantes :

SEULS
37%

des répondants disent être prêts à gérer un incident de Cybersécurité et disposer des processus qui leur permettraient de le faire efficacement.

SEULS
39%

des répondants affirment que leur entreprise sensibilise leurs collaborateurs en matière de Cybersécurité.

SEULS
42%

ont décliné leurs besoins de Cybersécurité vers leurs partenaires et leurs fournisseurs.

ET
19%

déclarent ne pas avoir mis du tout en place de stratégie de protection de l'information.

En cas de crise, l'urgence :

RÉTABLISSEMENT DE LA DISPONIBILITÉ, DE L'INTÉGRITÉ ET DE LA CONFIDENTIALITÉ DES DONNÉES, PLAN DE CONTINUITÉ OU DE REPRISE D'ACTIVITÉ, GESTION DE CRISE, COMMUNICATION CLIENTS, FOURNISSEURS ET PARTENAIRES

La plupart des répondants témoignent de plus que les processus clés pour la conduite des activités de leurs sociétés ne font l'objet d'aucune surveillance Cyber spécifique. Seule la moitié des répondants s'attache à vérifier leurs bases de données d'incidents.

A la question *« Avez-vous fait réaliser une étude d'évaluation du niveau de sécurité de vos systèmes d'information ? »*, **seules 35% des réponses sont positives** et elles sont très contrastées en faisant part de limites importantes :

- Les études ne concernent pas nécessairement tout le spectre des systèmes d'informations de l'entreprise. Le mot partiellement est cité régulièrement.
- La régularité est aléatoire. Pour certains, elles sont anciennes.

Elles sont en général réalisées par les *« prestataires habituels »* à qui l'on fait confiance pour, à la fois, mener l'étude et, en amont, contribuer à la définition du cahier des charges de l'étude.

Les dirigeants s'interrogent aussi sur la suite réservée à ces études une fois qu'elles ont été menées. Dans certains cas, ils reconnaissent que ces études n'amènent aucun élément correctif par manque de compréhension des enjeux, ou des actions correctives limitées compte tenu des coûts générés.

Très peu d'ETI ont des Plans de Continuité ou de Reprise d'Activité, ainsi que des Plans Gestion de Crise spécifiques au risque Cyber, a fortiori régulièrement testés dans la très grande majorité des cas :

« Sur les risques Cyber, nous manquons de formalisation et nous ne sommes pas exhaustifs. »

Enfin certains dirigeants n'hésitent pas à dire : *« Nous sommes dépassés, nous allons devoir agir »*.

Cela témoigne d'une vraie prise de conscience de la nécessité d'agir ou parfois d'une forme de culpabilité assez générale que confirment les chiffres de l'enquête constatant des améliorations sensibles en matière de prévention :

- **45% des ETI ont augmenté leurs investissements en 2017** dans la gouvernance du risque Cyber et la mise en conformité.
- **29% font appel à des entreprises externes**, tout particulièrement en ce qui concerne les prestations Cloud.

UN RECOURS ACCRU AUX PRESTATATIONS CLOUD

Les solutions Cloud représentent en 2017 près de 50% des services informatiques apportés aux entreprises. Parmi ces services, beaucoup d'ETI préfèrent déléguer aux prestataires de clouds la sécurisation de leurs infrastructures informatiques. Ces solutions cloud sont alors identifiées comme un moyen de renforcer la protection des données même si la concentration d'entreprises au sein d'un même hébergeur augmente le risque systémique de nature à les impacter en cas de défaillance du prestataire. Il est également très complexe pour ces ETI de vérifier que les prestataires remplissent leurs engagements en matière de Cybersécurité, les plaçant dans une posture délicate d'un *« rapport de force »* déséquilibré. L'externalisation implique donc, dans une certaine mesure, un manque de maîtrise, avec une visibilité amoindrie du niveau de sécurité des systèmes informatiques et une capacité relative des ETI à pouvoir vérifier l'adaptation des solutions à leurs propres enjeux.

#6

Les dirigeants reconnaissent qu'ils n'ont pas de vision précise des conséquences financières potentielles d'un incident Cyber.

APPRÉCIER ET QUANTIFIER LES IMPACTS FINANCIERS D'UN INCIDENT CYBER POTENTIEL EST LONG ET COMPLEXE. IL EST PRIORITAIRE D'ORGANISER LA CYBER RÉSILIENCE DE L'ENTREPRISE ET DE PRÉVOIR LES FINANCEMENT APPROPRIÉS

Si les dirigeants identifient de possibles impacts au niveau opérationnel et un risque d'atteinte à leur image, aucune des entreprises consultées n'a de vision précise sur l'ampleur et la durée possibles d'une crise Cyber et n'est en mesure de présenter un diagnostic précis de ses conséquences financières aux actionnaires. Elles concernent principalement :

- La non disponibilité des données pour une durée indéterminée
- la perte immédiate de chiffre d'affaires
- le blocage de l'activité, total ou partiel.

Ce constat n'est pas surprenant dès lors que les scénarii de risques sont multiples. L'absence de référentiel et de retours d'expériences ne facilitent pas l'exercice. Les impacts de Not Petya et de Wanna Cry, qui ont notamment touché de grandes entreprises telles que Saint Gobain ou Maersk, interpellent de par l'ampleur des préjudices révélés.

Le degré de préparation de l'entreprise joue aussi fortement sur l'ampleur et la durée et de la crise.

Le non chiffrage est justifié par l'étendue des attaques possibles, leur nature, les activités concernées (tout le groupe ou une partie) et donc un risque très large et peu précis. Il est possible de préparer des scenarii, pas de définir un risque comme une perte d'exploitation ou un incendie d'équipement. Dans les conversations, et de façon plus intuitive que rationnelle, on ressent un certain regret ou même une certaine culpabilité à ne pas avoir chiffré ces conséquences.

Cette question du chiffrage est révélatrice de deux points majeurs :

- Une non préparation à la crise Cyber de façon générale. La prévention du risque Cyber n'est pas une action privilégiée ; elle n'est pas incluse dans les plans d'action et de développement.
- Une certaine gêne à avouer qu'il existe un risque majeur et non contingenté.

A la question *« Comment évaluez-vous l'impact financier supportable par l'entreprise ? »* On nous a répondu *« Pas d'idée, pas évalué ». « Je touche du bois ».*

On a l'impression que cette question gêne tant elle apparaît comme normale et tant les réponses sont aléatoires et faibles.

Pour certains, le risque est lié au temps :

- *« Plus on redémarre la vie normale de l'entreprise, moins le coût sera élevé. C'est une question de timing. »*
- Deux jours d'indisponibilité seraient supportables, pas au-delà.

Certains chiffres sont avancés :

- Quelques dizaines de milliers d'euros et au-delà, il faudrait trouver une solution assurantielle. C'est manifestement faible par rapport aux échos de grandes catastrophes.
- Maximum **15 %** de la marge brute

Les entreprises ne devraient pas avoir pour seul objectif de chercher à maîtriser ce risque, mais celui prioritaire d'organiser, par tous les moyens, la résilience de l'entreprise. A ce titre, l'assurance peut tenir une place importante. Elle renforce en effet la politique de Cybersécurité en favorisant la mise en place de services d'accompagnement et de leurs financements ainsi que la prise en charge en tout ou partie des pertes constatées.

#7

L'assurance n'est pas encore perçue comme un outil qui participe au traitement efficace du risque Cyber.

FACE À UN RISQUE AUSSI COMPLEXE, L'ASSURANCE EST UN FACTEUR DE CYBER RÉSILIENCE DE L'ENTREPRISE.

Si les dirigeants ont connaissance de l'existence de solutions d'assurance, ils ne perçoivent pas encore l'assurance comme un élément de traitement pertinent de leurs risques.

La plupart des Dirigeants interviewés axent prioritairement leurs réflexions sur la prévention et souvent repoussent l'étude de solutions d'assurance au préalable d'une vision précise de leurs expositions (probabilité et fréquence d'occurrence) et des conséquences en cas de sinistre.

« Avant de prendre une assurance, l'important est de comprendre et évaluer ce que l'on craint », a précisé un dirigeant interviewé.

Mais si l'objectif recherché est pertinent, la question est de savoir en fait s'il est atteignable face à un risque aussi complexe et évolutif.

Face à cette situation, intégrer l'assurance comme un facteur de résilience constitue une approche novatrice. La question n'est plus simplement de chercher à maîtriser un risque, puis de transférer à l'assurance le risque résiduel, mais bien de concevoir l'assurance aussi comme un investissement en matière de Cyber sécurité.

PARTIE 02

Analyse des résultats de l'enquête

02

Regard croisé de deux spécialistes de la prise de décision et de la transformation au sein des entreprises

JACQUES FRADIN

Docteur en médecine, spécialiste en psychologie cognitive, prise de décision en situation complexe ou à risque, prévention et gestion du stress, auteur ou co-auteur de nombreux articles et livres dont *« L'intelligence du stress » et « Crises et facteur humain : Les nouvelles frontières mentales des crises »*.

BRUNO LUIRARD

Consultant indépendant,
Associé fondateur et Président de
« La Voix des Hommes »

Analyse de
JACQUES FRADIN

« Face à cette menace d'une extrême complexité, l'attitude des dirigeants d'Entreprises de Taille Intermédiaire est plus prévisible, compréhensible et même pertinente qu'il n'y paraît »

L'attitude quelque peu attentiste, immobiliste, circonspecte des dirigeants d'ETI pourrait finalement être plus rationnelle qu'il n'y paraît en l'état de la complexité, voire de l'imprévisibilité de tels risques virtuels, de la lourdeur et du coût direct et indirect de mise en œuvre des stratégies de prévention et de traitement.

Cette anticipation conjointe de la complexité et de la gravité entraîne un sentiment classique d'impuissance et/ou d'attentisme vis-à-vis de :

- Ce que l'on ne connaît pas
- Ce que l'on ne maîtrise pas
- Ce qui semble tout à la fois dangereux mais incertain et/ou hors de portée de nos capacités de prévention et d'action.

Par ailleurs, la dramatisation médiatique et celle des organismes de prévention (assureurs, institutions…) ajoute paradoxalement une couche à cette difficulté : autant l'agitation d'un risque connu, mesurable et maîtrisable produit ordinairement de la mobilisation, autant vis-à-vis d'un risque incernable dans sa forme comme dans sa cible, cela produit plutôt un repli.

En effet, pour explorer de nouvelles démarches, il faut adopter une attitude de curiosité, ce qui se fait dans un contexte pédagogique et bienveillant : progressivité des difficultés, droit à l'erreur comme dans le brainstorming, simulation ou exposition initiale à de faibles enjeux… La dramatisation entraîne un évitement qui soulage et nous permet de repartir dans la gestion du quotidien !

Les approches assurantielles classiques alimentent trop souvent des peurs aussi floues qu'inquiétantes, proposent des réponses et ressources (celles des grands Groupes) perçues intuitivement comme à la fois approximatives et surdimensionnées. Elles ont donc peu de chances de convaincre et de mobiliser massivement.

De ce qui précède, on comprend que l'anxiété d'anticipation est la résultante de deux types de facteurs :

1. Des stresseurs externes (liés à la *« gravité x probabilité »* des enjeux)
2. Une stressabilité interne du décideur ou du collectif, avant tout liée à un manque de cohérence entre les résultats/livrables attendus et les moyens accessibles/mis en œuvre pour les obtenir, à un manque d'anticipation, de prise en compte du réel, des signaux faibles….

Pour aller plus loin dans la compréhension des ressorts internes de la stressabilité, il faut considérer quelques aspects du fonctionnement du cerveau lui-même : il se met ainsi par défaut et le plus souvent en mode automatique (ce que l'appréhension ou la peur accentue). Or cet état atténue la perception du risque virtuel au profit du souci quotidien, plus concret et tout à fait certain, l'inconnu au profit du connu, le rassurant au profit de l'inquiétant !

D'autres mécanismes permettent d'affiner l'analyse : ainsi, le risque subi est-il souvent plus facile à gérer que le risque pris, ce qui peut pousser à la non-décision ! Ceci est d'autant plus marqué que le décideur éprouve un vécu de *« soumission »*, notamment en situation sociale sous pression (tendance à l'anticipation négative, à la culpabilité avec comportements compulsifs de vérification, syndrome de l'imposteur…). A l'inverse, ceux qui ont tendance à la dominance sont plus sujets à surestimer leur capacité à bien gérer les situations critiques en *« live »*… !

En fait, ces deux tendances (construites tout au long de notre histoire personnelle et de nos succès ou échecs dans les rapports de force sociaux, réels ou symboliques) distordent notre perception de la réalité et donc des risques (biais cognitifs), le sujet *« soumis »* étant plus à

même de surprotéger l'entreprise, privilégiant les processus de sécurité, au risque d'en freiner le développement, les initiatives ou l'innovation… A l'inverse, la dominance engendre des prises de risque plus importantes, voire inconsidérées, une surestimation de sa capacité à faire face… et même une confiance irrationnelle dans sa *« bonne étoile »* ! Ce qui peut là aussi entraîner un déni, pour des raisons diamétralement opposées !

Quelles que soient les causes de l'anxiété d'anticipation et/ou de la mauvaise évaluation des risques, le dirigeant ou le collectif gagnera à mobiliser son Mode Mental Adaptatif (mode curieux, global et agile, en miroir du Mode Automatique), facilitant ainsi ses capacités d'analyse rationnelle mais aussi et surtout une capacité décisionnelle plus globale et probabiliste, pertinente en situation complexe ou incertaine. Cette attitude est par ailleurs contagieuse auprès des équipes et se révèle plus apaisante qu'un management directif et *« protecteur »* !

Parmi les actions possibles pour accompagner les dirigeants d'ETI en de telles situations à risque ou de crise, on peut imaginer, en amont, pendant et en aval de situations de crises, du conseil, des formations au management du risque, des coachings (voire coachings cognitifs) préparant à une meilleure (neuro)connaissance de soi et des autres en situations difficiles.

On peut s'inspirer des interventions proposées par exemple aux cellules de crise, aux pilotes de chasse, aux sportifs de l'extrême, aux personnels hospitaliers exposés, etc., inviter des intervenants ayant ce type de maîtrise, construire des réseaux de coopération.

EN SYNTHÈSE :

« le risque Cyber n'est sans doute pas un risque qui peut être (seulement) traité comme les autres »

1. Chercher à le décrire et à le mesurer précisément est illusoire (sinon pour décrire ce qui s'est déjà passé) : *« c'est (largement) un leurre » ;*
2. Une des réponses pertinentes et plus immédiatement facile à mettre en œuvre dans le contexte actuel, serait plutôt d'organiser et d'accompagner d'abord la résilience des ETI face au risque et à ses conséquences pour l'entreprise sans (trop rapidement) alimenter les peurs (l'action calme, l'attente angoisse) ;
3. Comme en médecine, où l'on a d'abord pris en charge la crise (le symptôme ou la maladie) avant de proposer de la prévention, l'objectif premier sur un risque nouveau est sûrement d'identifier ce qu'il est utile de faire face au risque (de façon générique, en matière de préparation à la gestion de crise) pour mieux gérer la crise lorsqu'elle surviendra. Cela passe notamment par du conseil et de la prévention en amont et par la mise en place de mesures d'accompagnement et d'indemnisation. C'est à partir de ce premier pas comportemental que le sentiment initial d'impuissance/de sidération peut se dissoudre et ouvrir la voie à une prévention complémentaire (partielle, probabiliste et agile) des risques eux-mêmes.

Analyse de
BRUNO LUIRARD

Comment appréhender ces résultats de manière dynamique, voire prospective ? Comment apprécier justement l'attitude et les choix des dirigeants d'ETI au regard de cette enquête ?

D'abord rappelons-nous que nous sommes bien plus les enfants de notre époque, que les héritiers de nos parents !

En nous lançant dans une telle observation de ces observations, veillons à prendre en compte ce futur qui est déjà là, et qui conditionne le présent autant que le fait le passé : 5G, IA, IOT, VR, RA, Userx, Nowgen…

Nous devrons garder à l'esprit l'injonction faite aux dirigeants *« Que les ventes continuent pendant les travaux, et que la sécurité n'obère pas trop notre développement ! »* Nous ne pourrons comprendre toute la pertinence des choix actuels sans intégrer la pression de la mondialisation, de la digitalisation et de la vitesse d'exécution.

L'empathie pour nos chers dirigeants devra nous servir de point d'appui pour les inviter à briser un certain nombre de paradigmes limitants et peut être plus mortifères que jamais.

Quels sont les principaux constats issus de l'étude, qu'une écoute allocentrée nous permet de confirmer ou de préciser au quotidien ?

1. Face aux flux médiatiques, à l'omniprésence des attaques (100% des entreprises sont attaquées), à la multiplication des crises sectorielles, nationales, et mondiales, il n'est plus possible d'ignorer les risques Cyber. Cependant, prendre en compte l'occurrence de Cyber-risques, ne veut pas dire les connaître, encore moins les dimensionner.

2. Quelle que soit la taille des réponses technico-organisationnelles, le ROI dépend immédiatement de leur utilisation en mode Vigipirate. Or ce mode coopératif, solidaire et responsable réclame un niveau d'investissement dans l'éducation de tous les acteurs et dans l'anticipation des crises que les dirigeants savent ne pas avoir engagés à cette heure !

3. Les risques Cyber sont aussi complexes, que l'est l'évaluation des niveaux de dommages *« potentiels »*. Seules quelques entreprises sont aujourd'hui capables d'organiser des réponses en suite de dommages dépassant les capacités de résistance immédiates de l'entreprise. La très grande majorité se mobilise sur les Risques Maximums Tolérables, travaille à protéger leur organisation contre des intrusions relativement banales, aux conséquences désastreuses. Et ce n'est pas parce que les méthodes utilisées sont régulièrement la transposition de méthodes déjà connues par les hackers que l'action n'est pas essentielle.

Quelles observations complémentaires viennent étayer cette évaluation des postures actuelles des dirigeants face aux risques Cyber ?

1. Depuis les années 2010, de plus en plus de dirigeants osent confier dans le cadre de dialogues singuliers ou dans l'anonymat d'études mondiales comme celle IBM Institute for Business Value, qu'ils se sentent dépassés par la combinaison, complexité / accélération continue. Si comme le dit Montaigne : *« la vraie science est une ignorance qui se sait »*, alors ce sont près de 25% des dirigeants qui sont devenus *« scientifiques »* de ce point de vue ! Et c'est une excellente nouvelle. Il est plus facile de surpasser une difficulté si elle est visible. En la nommant, les dirigeants la rendent visible. Merci à eux.

2. La plupart des modèles économiques sont incapables de supporter immédiatement le niveau d'investissement nécessaire en matière de protection face à la Cybercriminalité. Par exemple, dans le domaine de la santé, et particulièrement celui des mutuelles :

- Comment garantir simultanément à des fonctionnaires de police la protection totale de leurs données personnelles face à tous types d'intrusions, même terroristes, et ce dans un business model aspiré par une compétition des prix à outrance ?
- Comment les mouvements de secours solidaires pouvaient-ils imaginer qu'un jour, les protections des datas pourraient potentiellement représenter 25% à 30% de leurs budgets de fonctionnement ? Où trouver ces ressources quand la pression marchande interdit de reporter ces nouveaux coûts sur les cotisations ?

3. Les dirigeants qui arrivent à exprimer *« à cet instant, je ne sais pas répondre de manière satisfaisante aux Cyber risques »* reconnaissent en ressentir un soulagement intense.

En cas de crise, seule une infime minorité d'entreprises accepte de s'appuyer sur les compétences institutionnelles nationales ou de partager leurs données pour fabriquer ensemble les meilleures parades.

Les Cyber risques sont aussi nés de l'économie du partage, si nous gardons nos réflexes issus des économies de stock, alors nous irons au-devant de grandes difficultés, de désillusions encore plus grandes.

Au total, quelle est la bonne nouvelle ?

L'action des dirigeants est intelligente :

- Si les dispositifs déployés ne sont pas suffisants, ils n'en sont pas moins nécessaires ;
- L'hésitation relative à passer la vitesse supérieure, permet de ne pas céder à la précipitation dans des solutions trop technico-centrées et donc très facilement contournables via le facteur humain.

- Exprimer son ignorance partielle est certainement la première condition exemplaire, pour libérer l'intelligence cachée et la créativité dans l'analyse des erreurs, dans le partage fructueux de toutes les dimensions de l'expérience.
- Les dirigeants commencent à exprimer leur intuition ou leur conscience diffuse que le Risk Cyber est d'un niveau de complexité qui va nous astreindre à poser le problème plus radicalement que d'habitude.

Quels sont les défis nichés dans les plis de ces différents constats ?

1. Pour les risques comportant des conséquences dépassant le seuil maximal tolérable, quel nouveau paradigme penser ? Que faire une fois la catastrophe passée et l'entreprise à terre ?

2. Face à des communautés d'agresseurs organisés en réseaux, comment réagir avec la puissance du collectif ? Comment partager la défense de ce que l'on ne veut pas voir partager ?

3. Si de l'éducation des peuples dépend le destin des nations, comment éduquer efficacement tous les membres de l'écosystème aux postures et aux pratiques qui conjuguent le mieux performance opérationnelle, protection de la valeur et exploitation optimale des crises ?

4. Face à de nouvelles générations de risques aussi complexes et porteuses de conséquences dévastatrices, que voudra dire à présent le terme de « *maîtrise* » ? Que pourrons-nous attendre que nous n'imaginons pas encore des systèmes d'assurance et de réassurance ?

Il n'est pas inutile, en cette période, de se rappeler que : pour vivre, il faut maintenir toutes ses fonctions vitales, pour mourir, il suffit d'en détruire une seule ! Le rapport entre la vie et la mort est asymétrique et pourtant, les humains ne cessent de prolonger l'espérance de vie en bonne santé !

Le progrès semble reposer sur la capacité de l'homo sapiens à coopérer et à commérer (cf. livre « *Sapiens* » de HARARI)

PARLONS-EN ENSEMBLE.

Regard
DE PwC

Nous intervenons régulièrement en France et à l'étranger pour évaluer et accompagner les ETI à se préparer, se protéger, détecter et réagir face aux menaces Cyber. C'est ainsi au travers de cette expérience que nous avons souhaité porter un regard sur les enseignements de cette étude.

Les ETI françaises, quel que soit le secteur dans lequel elles sont engagées : finance, industrie, services, font face aux mêmes challenges en matière de Cybersécurité que les entreprises de grande taille. Par construction, les moyens qu'elles sont en mesure de déployer pour faire face à la menace sont plus limités et les possibilités de synergies plus faibles. De ce fait, elles sont tout autant, voire plus, exposées aux risques Cyber et devraient se mettre en recherche du même *« Graal »* : maîtriser de manière efficace ce risque qui sera à l'avenir un élément clé de la confiance des clients.

Le paradigme de la Cybersécurité va au-delà de la discipline de sécurité de l'information. Ce paradigme intègre l'apparition de menaces sophistiquées, mettant en œuvre des stratégies conçues pour atteindre des objectifs précis qui peuvent intéresser des attaquants de type *« crime organisé »* ou encore *« état nation »*. De tels attaquants disposent de moyens techniques et financiers considérables et disposent de l'avantage de la surprise. Ils opèrent sans être connus, observent et ont l'avantage de maîtriser le temps dans lequel ils opèrent. Ils peuvent attaquer le jour, la nuit, les jours fériés ou encore pendant que les personnes en charge de la protection de l'entreprise sont en vacances. Ils disposent toujours d'une longueur d'avance sur les entreprises qui sont ainsi toujours en position de défense et de réaction. Dans un domaine où la maturité ne permet pas de se protéger de manière absolue contre la menace, la première étape est d'assurer un niveau de protection suffisant tout en mettant en place des mécanismes robustes permettant la réponse et la résilience de l'entreprise en cas d'attaque.

La médiatisation des incidents de Cybersécurité contribue à sensibiliser les dirigeants d'entreprises et en particulier les dirigeants d'ETI. Cette médiatisation montre des incidents dont l'impact est toujours plus important et spectaculaire. Le monde a récemment observé de nombreux incidents à même d'avoir un impact sur l'ensemble des entreprises. En effet, au-delà d'impacter une entreprise, ces incidents contribuent à renseigner, former et améliorer les capacités des attaquants.

QUELQUES EXEMPLES :

AVRIL 2014

« Shadow Broker »

Le groupe d'attaquants connu sous le nom de *« Shadow Brokers »* dévoile au grand public le vol d'outils d'espionnage et d'attaque utilisés par la NSA, offrant ainsi au monde des Cyberattaquants une connaissance à même de leur servir de *« source d'inspiration »*. A fortiori, certains outils partagés permettaient l'exploitation de vulnérabilités alors non connues par le marché.

MAI 2017

« WannaCry »

Plusieurs souches d'un logiciel malveillant désignées sous le nom de ransomware *« WannaCry »* se sont répandues dans le monde entier, faisant ainsi sombrer des centaines de milliers de cibles y compris des services publics et de grandes entreprises telles que Renault en France. Cette attaque a exploité l'une des vulnérabilités divulguées par le groupe *« Shadow Brokers »* (vulnérabilité dite *« EternalBlue »* développée par la NSA). Les Cyberattaquants apprennent... Et a priori plus vite que les entreprises... Bien que Microsoft ait publié un correctif pour cette vulnérabilité dès mars 2017, les entreprises n'avaient pas

encore toutes appliqué ce correctif permettant d'éviter la propagation de l'attaque. Cela n'aurait pas eu pour effet d'être complètement prémuni contre l'infection mais aurait pu limiter les conséquences en rendant les entreprises plus résilientes…

JUIN 2017

« NotPetya »

Les entreprises apprennent définitivement moins vite que les attaquants. Au travers d'une attaque différente, la vulnérabilité *« EternalBlue »* est de nouveau exploitée et crée des dégâts considérables. Certaines entreprises françaises sont de nouveau touchées telles que Saint-Gobain. Le groupe français a vu certaines de ses filiales (Lapeyre, Point P) paralysées. Le groupe a estimé à 220 millions d'euros sa perte en revenus sur les six premiers mois de l'année, soit 1,1 % de son chiffre d'affaires. Le résultat d'exploitation est quant à lui amputé à hauteur de 65 millions d'euros (soit 4,4 % du total).

D'autres exemples ayant eu des impacts différents comme par exemple la mise hors service partielle ou totale d'infrastructures informatiques ont également été médiatisés. En septembre 2017, OVH, hébergeur de données français a subi une attaque dite par *« déni de service »*.

Et il ne s'agit là que de quelques exemples qui ont été très médiatisés… Nous découvrons ainsi tous les jours de nouvelles menaces chez nos clients, parfois présentes depuis plusieurs mois / années…

Compte-tenu de cette médiatisation, il est donc naturel que les dirigeants d'ETI soient conscients de cette réalité et la craignent. Nous confirmons cependant aux travers de nos diverses expériences le constat d'ETI non armées pour faire face à cette menace ; nous constatons globalement :

- Un manque de compétence (tout le marché en souffre) accompagné d'un marché de la Cybersécurité parfois déceptif (promesse de valeur exagérée compte tenu de la réalité de la menace). Nous entendons encore beaucoup d'entreprises se pensant protégées en ayant acheté le *« dernier outil à la mode »*…
- Un manque d'implication des dirigeants dans la compréhension du risque Cyber résultant en des prises de décisions non éclairées en la matière.

Ces facteurs induisent un immobilisme assumé des entreprises ne sachant pas comment mieux traiter le problème. Comme commenté par nos experts Jacques Fradin et Bruno Luirard, cet immobilisme est une première réaction cohérente et intelligente compte-tenu des facteurs sociaux et humains qu'ils observent régulièrement en entreprise. Cette réaction a probablement des fondements profonds liés à la manière dont l'humain est construit. La prochaine étape intelligente est probablement de s'armer face à cette menace que seule une ETI ne pourrait résoudre…

Les entreprises les plus lucides recherchent du conseil pour évaluer leur capacité à répondre à la menace et tenter de revoir leur posture ou encore à souscrire à des solutions assurantielles. Ces approches sont souvent des démonstrations de bonnes intentions sans pour autant être suffisantes pour construire une approche efficace. De notre expérience, l'efficacité des dispositifs est avant tout une affaire de compromis :

- Protection v/s Atteinte des objectifs métiers : Comment équilibrer les investissements ?
- Protection v/s Surveillance, détection et réponse aux attaques : Partant du principe que la protection absolue n'existe

pas, comment mettre en place une détection efficace qui nous permettra d'être résilient en cas d'attaque.

Ces équilibres sont, de notre expérience, encore que trop rarement atteints :

- Trop d'entreprises survivent encore avec une dette technologique qu'elles n'ont pas traitée.
- Des dispositifs de détection en place pour permettre de révéler les comportements malicieux mais largement insuffisants pour détecter les signaux, faibles indicateurs d'une attaque avancée et sans précédent.
- Un bénéfice de la Cybersécurité pour les métiers pas encore suffisamment promu pour permettre une adhésion complète à la démarche de Cybersécurité de l'entreprise.

Même si de nombreuses entreprises françaises indiquent avoir une stratégie de Cybersécurité, le fait est que nous avons souvent été déçus par le manque de pertinence et de contenu de celles-ci…

Bien que les dirigeants interrogés dans le cadre de cette étude confirment que les attaques sont régulières voire permanentes, nous avons été surpris par l'excès de confiance que ceux-ci pouvaient avoir dans leur capacité à déjouer les attaques et plus globalement sur le fait d'être totalement protégés contre les Cyber attaques. Dans le cadre de cette étude, les dirigeants d'ETI ont davantage mis en avant le traitement des menaces connues (incidents détectés) que leur capacité ou incapacité à traiter les menaces non connues (incidents non détectés mais potentiellement présents). Dans les cas de réponse à incident que nous avons pu traiter, la menace était présente dans l'environnement depuis plusieurs mois et parfois plusieurs années.

La discipline de Cybersécurité est censée également se concentrer sur le traitement de menaces non connues :

- Exploitation de vulnérabilités non connues : les attaquants exploitent de plus en plus des *« O-days »*, vulnérabilités non connues et parfois revenues sur le marché noir.
- Attaques spécialisées selon l'objectif de l'attaque et le secteur de l'entreprise : les attaquants développent des spécialités et associent des compétences métiers (compréhension des processus financiers d'une entreprise) à des compétences techniques (connaissance technique des systèmes et des technologies).

Les dirigeants d'ETI ne sont pas une exception en la matière : bien que le niveau de sensibilisation augmente dans la population des dirigeants d'entreprises, la définition du risque Cyber est parfois floue et mal appréhendée des Comités de Direction.

Par ailleurs, l'absence d'un cadre permettant de gérer ce risque Cyber et de le suivre, a pour probable conséquence que les entreprises n'ont aucune idée des types d'attaques qu'elles seraient en mesure de contrer, détecter et répondre. Comment couvrir un risque que l'on ne connaît pas ?

Les usages numériques évoluent de manière exponentielle depuis les années 2000. Depuis 2000, les équipements utilisés par les employés de l'entreprise augmentent en nombre. Chaque employé peut aujourd'hui disposer d'un mobile, d'une tablette et parfois plusieurs ordinateurs. L'innovation des entreprises qui produira de nouveaux objets connectés sur Internet fera, au cours des prochaines années, augmenter de manière exponentielle l'exposition des entreprises sur Internet et donc son risque Cyber. Par ailleurs, la complexification des systèmes augmente la probabilité de vulnérabilités. A titre d'exemple, le nombre de lignes de code source d'un cœur de système d'exploitation *« Linux »* a été multiplié par 10 pour atteindre plus de 20 millions de lignes.

Le risque d'inconnu augmente ainsi de manière exponentielle… Comment maîtriser cette complexité à l'échelle humaine ? L'un des éléments de réponses issu de nos échanges avec nos clients des plus matures aux moins matures est la coopération. L'échange

d'informations s'avère un élément clé pour apporter une réponse à la menace.

L'origine des menaces Cyber identifiées par les ETI étant très diverses : employés internes, acteurs externes tels que partenaires ou encore concurrents, il est en réalité souvent très difficile de l'identifier de manière certaine ; une attaque peut :

- Provenir du poste de travail d'un employé sans pour autant qu'il en soit à l'origine ;
- Provenir du réseau d'un partenaire ou d'un concurrent suite à la compromission de son système d'informations ;
- Utiliser des outils dont l'origine pourrait laisser penser que les attaquants ont une certaine provenance, là où il ne s'agirait que de camouflage pour cacher l'origine réelle de l'attaque.

Comme évoqué précédemment, le domaine de la Cybersécurité est un domaine où l'on ne peut avoir confiance qu'en très peu de choses et où la remise en question constante est un facteur clé de succès.

La maîtrise de la Cybersécurité constituera désormais une clé de la confiance qu'un client pourra porter dans une entreprise. Le client sera désormais soucieux de la pérennité de l'entreprise mais surtout de sa capacité à gérer des données qui le concerne directement, personnellement. Par ailleurs, la réglementation opère pour protéger les clients. Un règlement européen, le RGPD - Règlement Général sur la Protection des Données - impose aux entreprises des mesures pour protéger les données personnelles. Ce règlement rentre en application en mai 2018.

L'évolution des ETI montre qu'elles sont le moteur de l'innovation française. En effet, leur compétitivité passe souvent par une stratégie centrée sur l'innovation technologique et une forte capacité de transformation digitale. Ces caractéristiques sont des facteurs d'augmentation du risque Cyber mais représentent aussi des opportunités pour les ETI de gérer efficacement leur risque Cyber. La gestion du risque Cyber nécessite des comportements agiles et une maîtrise de la technologie.

A titre d'exemple, le Cloud constitue une solution de plus en plus privilégiée par les ETI. Cette transition aux services Cloud constitue une opportunité permettant aux ETI de bénéficier des dispositifs de sécurité mutualisés dans lesquels elles ne seraient pas en mesure d'investir pour sécuriser leurs infrastructures propres. Cependant, comment garantir que les prestataires de Cloud remplissent leurs engagements en matière de Cybersécurité ? Comment s'assurer que ces moyens répondent aux enjeux des ETI ? Les ETI ont-elles les compétences pour challenger ces prestataires de Cloud ? Le rapport de force est-il équitable ? Le challenge pour les ETI est de comprendre les enjeux de la Cybersécurité tout en étant en mesure de les challenger sur les plans techniques, juridiques, ...

QUI MIEUX QUE DES PAIRS DE CONFIANCE POUR STRUCTURER LA RÉPONSE À LA MENACE CYBER TOUT EN ORGANISANT LA RÉSILIENCE DES ENTREPRISES FACE AUX CYBER ATTAQUES ?

Regard
DE BESSÉ

Tous les dirigeants d'ETI et leurs équipes anticipent et gèrent au quotidien l'ensemble des menaces qui pèsent sur leurs entreprises, notamment celles qui relèvent du risque industriel. Le risque Cyber, lui, est singulier.

Il appartient à une nouvelle génération de risques dont la complexité est extrême et les caractéristiques diamétralement opposées à celles du risque industriel.

Pour le traiter efficacement, il est indispensable d'innover en créant des solutions nouvelles et des services adaptés, tant du point de vue de la prévention, de l'assurance, de la gestion de crise et du règlement des sinistres.

ALORS QUE LE RISQUE INDUSTRIEL EST PRINCIPALEMENT D'ORIGINE ACCIDENTELLE, LE RISQUE CYBER EST PRINCIPALEMENT D'ORIGINE « MALVEILLANTE »

Le risque Cyber trouve ses causes principales dans la malveillance externe ou interne et non dans un événement aléatoire.

Les atteintes portées ainsi à l'entreprise exploitent des vulnérabilités inhérentes à :

- La multiplication des outils digitaux individuels et les échanges de données avec des partenaires externes
- Et/ou la confiance naturelle des collaborateurs dans le système d'information de l'entreprise.

Face à cette menace permanente et multiforme que constitue la malveillance, ni la protection technologique, ni les meilleurs règles internes en mode *« Vigipirate »* ne sont suffisantes, lorsque l'on sait à quelle vitesse les Cyber assaillants développent des outils de plus en plus sophistiqués et les rendent accessibles gratuitement au plus grand nombre en libre service sur le web. Comment être certain de parer ces pratiques dénommées *«Ransomware as a Service »* ou *«Raas »* d'une *« criminalité 4.0 »* organisée en mode collaboratif ?

LE RISQUE CYBER EST « ÉVOLUTIF », ALORS QUE LE RISQUE INDUSTRIEL EST « STABLE »

L'événement propre au risque Industriel est intrinsèquement stable par nature : un incendie reste un incendie, une explosion reste une explosion, un bris de machine reste un bris de machine, une tempête reste une tempête, une erreur de conception reste une erreur de conception…

A l'inverse, le risque Cyber est évolutif par nature. Nous ne pouvons pas anticiper ce que seront demain ni ses origines, ni ses conséquences.

Il évolue sans cesse depuis le développement du numérique. Aux risques informatiques des années 80/90 et la crainte du virus se sont substitués les risques digitaux et les menaces Cyber.

Tentaculaire, le numérique a infiltré progressivement tous les secteurs d'activité. Il interconnecte tous les acteurs de l'économie et les rend de fait interdépendants. L'évolution permanente du secteur numérique est telle qu'il est impossible de se projeter à plus de 10 ans. Dans quel monde vivrons-nous avec le déploiement de l'Intelligence Artificielle, les Smart City, les transports autonomes ?

Évolutif, le risque Cyber est aussi mouvant, multiple et multiforme. Il en est de même au niveau des menaces, crimes organisés, concurrents, états, pirates informatiques ; comme au niveau des motivations, financières, espionnage ou simple volonté de nuire. Il est pour l'essentiel attaché à la malveillance aux motivations très diverses. Comment, dans ces conditions, pouvoir prétendre maîtriser ce risque ? La maîtrise ne peut être qu'éphémère, car mise à mal par l'évolution permanente des organisations, des systèmes d'informations et la mise en lumière de nouvelles vulnérabilités révélées du fait de moyens d'attaques de plus en plus puissants.

LE RISQUE CYBER EST « SYSTÉMIQUE » ALORS QUE LE RISQUE INDUSTRIEL EST « CANTONNÉ ».

Alors que les risques Industriels ont un impact géographique limité, les risques Cyber sont, à l'inverse, potentiellement planétaires. Ce sont de fait et contrairement à un événement de nature catastrophique tel un incendie majeur ou un ouragan, les seuls risques à pouvoir affecter, en une seule occurrence, la totalité du bilan d'un Groupe (une entreprise et ses filiales en plusieurs points du monde).

A titre d'exemple, une attaque Cyber sur le système SAP d'un groupe industriel international peut bloquer l'ensemble de ses chaînes logistiques au plan mondial.

Ils génèrent également des risques latéraux inédits. Une attaque sur un fournisseur stratégique suffit à impacter l'ensemble de la supply chain avec des conséquences financières certaines pour l'ensemble des entreprises touchées directement et indirectement. Ils sont aussi capables de se propager dans l'entreprise en s'infiltrant par le biais d'un acteur de confiance.

Ces caractéristiques confèrent aux risques Cyber une dimension diffuse, cumulative et systémique. De fait, elles rendent impossible la mesure certaine de ces effets, tant sur les entreprises affectées, que sur l'ensemble de leur écosystème.

LE RISQUES CYBER EST « INQUANTIFIABLE » ALORS QUE LE RISQUE INDUSTRIEL EST « QUANTIFIABLE ».

Le risque est en effet difficilement quantifiable. On ne peut effectivement préjuger de l'étendue réaliste des conséquences d'un événement Cyber.

En plus, s'agissant d'un risque systémique, on identifie mal l'effet cumulatif de ce type de risques.

Ces caractéristiques singulières posent des questions de fond sur l'approche de la gestion de ce risque singulier : il est extrêmement compliqué, pour un industriel ou une autorité, de dimensionner les ressources et les moyens à allouer face aux menaces Cyber. Le marché de la Cybersécurité n'en connaît pas moins un développement spectaculaire. Il est clair que plus les moyens alloués à la défense seront importants, plus les attaques pourront être contrées.

En matière de Risk Management et au niveau des Dirigeants, la problématique posée est de déterminer comment gérer au mieux ce risque Cyber et se prémunir de conséquences potentiellement désastreuses. Ces caractéristiques, opposées à celles d'un risque Industriel, supposent aussi de mettre au point des réponses globalisées comme par exemple la création de référentiels en matière Cybersécurité.

Mais face à un risque Cyber aussi particulier et évolutif, est-il réaliste voire légitime de parler de normes, de référentiels ou de contrôle ? Quel référentiel construire dans la durée dans un domaine où les évolutions technologiques sont permanentes ?

Sur le terrain des responsabilités, la question s'avère également complexe. Est-il recevable de mettre en cause un industriel pour une faute de conception sur un matériel, au motif d'une vulnérabilité rendue possible bien des années plus tard du fait des évolutions technologiques ?

LES ZONES D'INCERTITUDES FACE AU RISQUE CYBER SONT DONC NOMBREUSES. QUELLE APPROCHE TENIR DANS CES CONDITIONS POUR CONTENIR LE RISQUE ET SURTOUT SES CONSÉQUENCES ?

Deux axes sont à prendre en considération.

LE PREMIER concerne la gestion en amont des risques liés à l'organisation des systèmes d'informations de l'entreprise et à la protection des données. A titre d'illustration, quelques pistes de réflexions au travers des interrogations suivantes :

- La centralisation des ressources et des moyens informatiques dans l'entreprise ne génère-t-elle pas une sur-concentration de risques en particulier quand les applications clés desservent en central l'ensemble d'un groupe et de ses filiales ?
- Ne faudrait-il pas au contraire repenser les architectures informatiques au profit d'un ensemble de cellules autonomes afin de décloisonner les risques ?
- A l'inverse, les solutions Cloud sont–elles suffisamment contrôlées ? L'externalisation à l'excès ne crée-t-elle pas un risque de dépendance extrême ?

L'évolution en cours de la réglementation favorise bien sûr une meilleure appréhension et gestion du risque.

Les législateurs soucieux de la préservation et de la sauvegarde des intérêts de tous les acteurs installent de nouveaux cadres, que ce soit par exemple avec le nouveau Règlement Général sur la Protection des Données personnelles (RGPD), que la Directive NIS, récemment transposée en droit français et qui impose désormais aux OSE (Opérateurs de

Services Essentiels) soit plusieurs centaines d'entreprises, de renforcer leur niveau de sécurité informatique.

Mais ne faudra-t-il pas aller encore plus loin à très court terme?

LE DEUXIÈME axe consiste à traiter efficacement et le plus largement possible les conséquences financières pour l'entreprise, quelle qu'en soit la nature, préjudices matériels ou immatériels, y compris préjudice d'image et de réputation, par voie de transfert au marché de l'assurance.

Les assureurs sont nombreux sur le marché et devraient pouvoir mutualiser ces risques moyennant un engagement unitaire adapté et le contrôle de leur cumul de pertes sur un même événement Cyber. Mais sur ce marché naissant de l'assurance Cyber, aucun assureur n'est aujourd'hui en situation d'estimer précisément le cumul de ces engagements, ce qui de facto limite ses capacités de souscription sur les risques les plus exposés.

L'assurance Cyber représente ainsi une source d'innovation majeure. Elle ne saurait se limiter à la souscription d'une police Cyber spécifique sans l'avoir coordonnée avec les risques qui relèvent des branches classiques de l'assurance ; Dommages aux Biens, Responsabilité Civile, Automobiles, Maritime, Transport, Aviation...

Les marchés d'assurance et les polices d'assurance telles qu'elles sont construites aujourd'hui devront continuer à évoluer afin d'intégrer ces problématiques clés et toutes celles nouvelles induites par l'évolution des usages liés au digital.

La question est posée également en matière de valorisation des données, en particulier lors de l'indemnisation des conséquences d'une perte, d'un vol ou d'une copie de données sensibles ayant trait aux secrets commerciaux ou de fabrication de l'entreprise. En assurance Dommages aux Biens, les données ne devront-elles pas être considérées comme un bien assuré à part entière ?

Le sujet est déjà posé en automobile avec le développement de la conduite autonome et des interactions entre le véhicule et son environnement, en matière de signalétique par exemple, ou pour l'intervention des secours en cas d'accident. Comment seront traitées les questions de responsabilités en fonction du niveau de défaillance digitale ?

Sur le champ des responsabilités, comment traiter des conséquences d'une vulnérabilité numérique d'un produit si aucune faute ou négligence n'est imputable à son fabricant ?

Nous le voyons bien, les questions sont nombreuses. Des réponses existent déjà, d'autres sont à construire. Cela nécessite des approches sur mesure, de l'écoute et du conseil.

Dans tous les cas, il nous semble que l'objectif visé par les ETI ne devrait pas être de chercher à maîtriser parfaitement ces risques Cyber avant d'agir, car l'état de l'art ne nous le permet pas aujourd'hui.

Il s'agit plutôt, en combinant l'ensemble des moyens utiles à tous les niveaux de la chaîne de valeur, de la prévention à la conception de solutions assurantielles robustes soutenues par une gestion sinistre adaptée et des services de gestion de crise, de contribuer par nos actions coordonnées à rendre les ETI, ainsi que toutes les entreprises exposées, résilientes à celui-ci, c'est-à-dire en situation d'en limiter les impacts quelle qu'en soit la nature, le jour où le risque se réalisera.

Les dirigeants d'ETI sont conscients de ce besoin de Cyber résilience, créateur de valeur pour leurs entreprises.

Les enjeux sont collectifs :

AGISSONS ENSEMBLE !

EN CONCLUSION, ORGANISONS LA CYBER RÉSILIENCE DES ETI !

En allant ensemble plus loin, plus concrètement… en favorisant le partage d'expériences, des bonnes pratiques… et pourquoi pas en créant un forum d'échanges, voire un cluster Cyber résilience dédié aux ETI ?

Cette étude nous donne une étonnante photographie des ETI face aux enjeux de la Cybersécurité, et l'on pourrait extrapoler pour se poser la question plus large de la capacité à aborder la transition digitale. Certes, chacun peut imaginer que les dirigeants, leurs équipes et leurs partenaires sont en route et abordent ce sujet avec le professionnalisme qui les caractérise. Mais restons dans notre sujet, celui qui consiste à se prémunir de cet incroyable *"banditisme des temps actuels"* qui peut si soudainement fragiliser une entreprise.

Comment accélérer la prévention ? Comment faire les bons choix, les investissements appropriés ? Comment former les équipes, maintenir un niveau de vigilance constant et évolutif au rythme de la créativité extravagante des pirates et hackers ?

Quelles assurances prendre ou ne pas prendre et comment être bien conseillé ?

D'autres questions se posent : que font les entreprises de même taille ? Quelles sont les politiques réussies de certains, et les accidents riches d'enseignements des autres ? Quelle résilience a été possible, et comment les ETI attaquées ont-elles rebondi ?

Toutes ces questions sont légitimes et d'autant plus que, d'année en année, elles sont plus nombreuses et plus floues, plus complexes avec des conséquences potentielles encore plus angoissantes.

Cette étude de l'opinion face aux dangers des Cyber attaques, ne peut rester sur une étagère comme c'est le cas de beaucoup d'études. Nous constatons un phénomène croissant, et rien ne laisse supposer qu'il cesse prochainement. Alors voici trois conditions pour réagir.

La première

Ne pas rester seul. Quelles que soient les compétences du dirigeant et de son Comité de Direction, l'implication des DSI et de leurs équipes, la solitude est risquée. Le partage d'expériences avec des consultants, des conseils spécialisés, ou avec d'autres industriels ou prestataires de services sera enrichissant et constructif.

La deuxième

Dans le cadre de ces échanges, maintenir un niveau de confidentialité approprié.

La troisième

Anticiper. Nous le savons tous, du fait de la sophistication des systèmes et de l'essor du digital, la fragilité des entreprises au risque Cyber risque d'augmenter. Prévoir, prévenir, imaginer et construire les réponses aux éventuelles attaques devient une tâche à part entière.

Echange, confidentialité et anticipation : voilà qui pourrait être la conclusion pratique de l'étude menée par BESSÉ et PwC en favorisant dans ce cadre le partage d'information et la collaboration entre les entreprises, ce qui pourrait idéalement aboutir à la création d'un forum d'échanges voire d'un cluster Cybersécurité dédié aux ETI, si leurs dirigeants l'appelaient de leurs vœux.

S'il est trop tôt pour en définir les contours, la rencontre de dirigeants mobilisés entre eux d'abord, puis ouverts aux experts et conseils qui chaque jour réfléchissent, innovent, réagissent, sera fructueuse. Le travail en commun n'évitera pas le risque : il permettra de prévoir, de créer des solidités et des solidarités.

Le risque Cyber est encore mal connu et appréhendé avec les moyens et les méthodes traditionnelles. Ensemble, avec l'appui d'une organisation adaptée, participative, garante de la confidentialité et permettant d'anticiper, il sera abordé aussi pleinement que possible.

Artwork / studio.annabelleb@orange.fr - Impression / Alliance Partenaires Graphiques, Reims

www.besse.fr
www.pwc.fr