Sommaire

Introduction

Pierre Bessé
Président de Bessé……1

Crise cyber : quel impact sur la valorisation des entreprises ?

Guy-Philippe Goldstein,
Enseignant-chercheur à l'École de Guerre Économique, Advisor pour PwC……..3

Quelle prise de conscience de la part des dirigeants d'entreprises ?

Jean-Philippe Pagès
Directeur Industrie & Services de Bessé……5

DÉBATS ……7

Conclusion

Jean-Philippe Pagès
Directeur Industrie & Services de Bessé……10

Introduction

Pierre Bessé

***Hugo Ronsin**, Boury, Tallon & Associés*
Bienvenue à cette rencontre live sur la Cyber résilience organisée à l'initiative de Bessé. Elle a lieu dans le contexte de l'explosion du risque cyber : alors que le nombre d'attaques a quadruplé en France cette année, il est urgent de renforcer la cyber résilience. Cette rencontre tournera autour de deux axes : l'impact d'une éventuelle crise cyber sur la valorisation de nos entreprises, et les solutions assurantielles pour renforcer la cyber résilience. Je laisse Pierre Bessé, président de Bessé, ouvrir cette rencontre.

"Ce monde est « sur-affolant », avec l'omniprésence de ce péril du cyber."

PIERRE BESSE

Merci, bonjour à toutes et à tous. Nous nous étions interrogés sur l'opportunité de cette rencontre, mais c'est l'actualité qui nous a montré à quel point elle est nécessaire : chaque jour, des laboratoires pharmaceutiques, des armateurs maritimes ou des sites Internet d'hôpitaux sont attaqués. Ce monde est "sur-affolant", avec l'omniprésence de ce péril du cyber. De plus, l'on on ne cesse "d'ajouter du numérique au numérique", comme le montre la récente introduction en bourse, pour une valorisation folle, de Coinbase, une plateforme virtuelle d'échange de cryptomonnaies totalement dématérialisées. L'omniprésence de ce monde virtuel et du risque qui y est attaché nous contraint à trouver les moyens de vivre avec, comme nous devons le faire pour le risque sanitaire.

Nous travaillons sur le sujet du risque cyber depuis plus de 6 ans, nous avons publié trois études, nous nous sommes associés aux meilleurs experts – l'Anssi, le FIC, etc. – et j'aimerais pouvoir dire, aujourd'hui, que la prise de conscience est réelle et qu'elle nous permet d'élaborer ensemble des solutions propres à traiter ce péril. Ceci étant, bien que le président de la République ait lancé un plan doté d'un budget de 1 milliard d'euros pour investir dans le domaine, c'est très peu au regard des 430 milliards d'euros dépensés dans la lutte contre la crise sanitaire, et cette somme est largement insuffisante face au péril que représente le cyber. Certes, la création d'un campus à Paris est une très bonne nouvelle, tout comme les multiples initiatives privées – dans lesquelles nous nous inscrivons – qui prennent corps, avec les contributions de l'Institut Montaigne et d'autres organisations de premier plan. De même, j'ai été particulièrement ébahi en apprenant que Jérôme Powell, le président de la Réserve fédérale américaine, considérait que le cyber est le principal risque pesant sur l'économie mondiale, avec des conséquences potentiellement plus lourdes que celles de la crise de 2008, notamment dans l'hypothèse d'une attaque contre les moyens de paiement et les transactions financières. J'espère que l'on me croira, comme l'on aurait dû croire Bill Gates lorsqu'il affirmait

“Il nous revient de travailler très en amont, car l’assurance ne sera qu’une brique d’un ensemble beaucoup plus vaste intégrant l’identification des risques et l’organisation de la réponse.”

PIERRE BESSE

en 2015 qu’une pandémie pourrait bientôt bouleverser le monde, et j’espère que l’on va développer les moyens de trouver des réponses qui sont indispensables. Les entreprises ont-elles pris conscience de cette urgence ? Je dirais que c’est le cas, car elles se sentent davantage concernées, mais beaucoup reste à faire.

Dans ce contexte, il nous incombe de faire des propositions de valeur qui ne se limitent pas à l’assurance, car le monde des produits sur étagère – avec des polices dont on ne sait pas exactement ce qu’elles couvrent – n’existe plus, les entreprises doivent gagner en robustesse, tant au niveau des technologies numériques, des RH ou du management opérationnel, car le monde de l’assurance a pris conscience de l’importance grandissante de ce risque. Il nous revient de travailler très en amont, car l’assurance ne sera qu’une brique d’un ensemble beaucoup plus vaste intégrant l’identification des risques et l’organisation de la réponse. L’analyse des éventuelles conséquences financières est elle aussi primordiale : auparavant, certains considéraient qu’une cyber attaque impacterait leur activité pendant deux à trois semaines, mais en réalité c’est beaucoup plus long. Notre proposition de valeur aidera les entreprises privées à mieux se préparer.

Crise cyber : quel impact sur la valorisation des entreprises ?

Guy-Philippe Goldstein

Hugo Ronsin
Guy-Philippe Goldstein, quels sont les grands enseignements de vos travaux relatifs à l'impact d'une crise cyber sur la valorisation des entreprises ?

"Le nombre d'attaques a été multiplié par 4, les attaques de rançongiciels sur les grandes entreprises ont été multipliées par 2,5 selon l'ANSSI, et au niveau mondial le nombre des attaques contre des hôpitaux a été multiplié 5, selon PwC."

GUY-PHILIPPE GOLDSTEIN

Bonjour, merci pour ce rappel du contexte, qui est très dur : le nombre d'attaques a été multiplié par 4, les attaques de rançongiciels sur les grandes entreprises ont été multipliées par 2,5 selon l'ANSSI, et au niveau mondial le nombre des attaques contre des hôpitaux a été multiplié 5, selon PwC. Ceci étant, avant même la crise du covid, de nombreux décideurs économiques avaient pris conscience que ce risque était devenu l'un des principaux auxquels sont exposés les entreprises, comme le montrent le Global Risk Survey du Worl Economic Forum de Davos ou les analyses de la Banque d'Angleterre effectuées auprès des cadres de la City de Londres.

L'étude que j'avais effectuée à la fin des années 2010 pour PWC montrait que, dans deux tiers des cas, pour les entreprises cotées, la baisse moyenne des cours consécutive à une attaque s'élevait à 9 % après 21 jours de cotation. Dans 40 % des cas, il s'avérait que l'entreprise n'était pas résiliente et subissaient une baisse de 20 % de sa cotation au bout d'un an, et dans 23 % des cas le rebond des entreprises les plus résilientes était de 6 %.

Pour Bessé, nous nous sommes intéressés aux PME et aux ETI, qui forment le socle du tissu économique national, et nous nous sommes demandé si l'impact d'une crise cyber serait égal ou plus fort que ce que subissaient les entreprises cotées. En l'absence de données publiques, nous avons sollicité certains fournisseurs de données pour connaître des indicateurs comme le nombre de jours de retard de paiement ou la probabilité qu'une entreprise recoure à une procédure collective, dans le cadre d'une liquidation ou d'un redressement. Sur un panel réduit de 30 entreprises étudiées (15 internationales et 15 françaises), il s'avère que le risque de défaillance augmente de 50 %. L'étude du panel d'entreprises françaises montre que l'impact est plus rapide (le pic de la crise est atteint dès le 2e mois contre le 3e mois pour les entreprises internationales) et que le délai de paiement augmente de 50 % à partir du 4e mois. En comparaison avec des entreprises équivalentes (taille et secteur identiques), le score de défaillance est beaucoup plus fort pour les entreprises victimes d'un cyber incident. Si ces panels ont une taille réduite, il est indéniable que, sur un plan qualitatif, les effets constatés sont significatifs. Précisons que passer la barre des 1 % de probabilité de défaillante (avec des scores pouvant atteindre 1,6 ou 1,7 % après 6 mois)

“Le cyber implique de nouveaux standards de qualité industrielle dont les entreprises pourront se prévaloir comme argument de vente.”

GUY-PHILIPPE GOLDSTEIN

entraîne pour ces entreprises victimes de cyber attaques une incidence forte sur leur valeur patrimoniale, de l’ordre de 8 à 10 %. Cet ordre de grandeur est assez comparable à l’évolution des cours de bourse des sociétés cotées.

Après une attaque, les conséquences sont variables, elles vont de la faillite (comme ce fut le cas pour une entreprise de recouvrement de créance ou une PME de B2B2C) à des difficultés, cas le plus fréquent, et peuvent même dans certains cas conduire à la démonstration d’une capacité de rebond, vis-à-vis des clients comme des employés. La résilience suppose les qualités suivantes :

- Agilité et ouverture dans la réponse.
- Capacité d’absorption du choc.
- La préparation au choc.

In fine, sans résilience l’entreprise subit une dégradation de la perception des clients et fait preuve d’une dégradation de sa qualité industrielle. Le cyber implique de nouveaux standards de qualité industrielle dont les entreprises pourront se prévaloir comme argument de vente.

Quelle prise de conscience de la part des dirigeants d'entreprises ?

Jean-Philippe Pagès

Hugo Ronsin
Jean-Philippe Pagès, est-ce que les dirigeants d'entreprises ont conscience de l'impact potentiel d'une crise cyber ?

"Pour notre part, le risque cyber est actuellement le sujet qui concentre la plus grande part de nos travaux avec les dirigeants d'entreprise."

JEAN-PHILIPPE PAGES

Bonjour et à tous, merci pour cette question. L'indicateur du degré de prise de conscience du risque par les dirigeants est en effet essentiel, il est à la base de l'action. Nous suivons cet indicateur depuis 2016 et lors de la publication de notre première étude, en 2018, cette perception était très faible. Aujourd'hui, le caractère stratégique de ce risque a très fortement progressé et aucun dirigeant n'ignore la menace. Plusieurs facteurs expliquent cette évolution :

- La multiplication du nombre de cas.
- La communication dans les médias par les victimes, qui alertent sur le fait que toute entreprise peut être touchée.
- La crise sanitaire, car le recours massif au digital a pu révéler ça et là les failles de sécurité des entreprises.

Toutefois, les dirigeants reconnaissent qu'ils n'ont pas tous analysé finement leur exposition au risque, qu'ils n'ont pas évalué précisément leur niveau de maturité en cyber sécurité et, élément décisif, qu'ils n'ont pas encore quantifié les conséquences financières d'une attaque cyber sur leur entreprise. Pourtant, un chef d'entreprise doit valoriser un risque, d'autant plus lorsqu'il fait peser la menace de millions d'euros de perte par jour d'inactivité consécutive à l'arrêt des systèmes d'information. Connaître ce chiffre permet au dirigeant de calibrer son action, de dimensionner sa dépense et d'en mesurer le retour sur investissement.

Compte tenu de la nature systémique et évolutive du risque, de la diversité des préjudices qu'il peut causer à l'entreprise (matériel, image de marque, confiance des clients, part de marché), l'analyse est bien plus complexe que celle réalisée habituellement pour les risques "classiques". Pour notre part, le risque cyber est actuellement le sujet qui concentre la plus grande part de nos travaux avec les dirigeants d'entreprises.

HUGO RONSIN
Concrètement, qu'est-ce que la cyber résilience ?

JEAN-PHILIPPE PAGÈS
Nous avons lancé dès 2018 un appel à renforcer la résilience des entreprises car la question n'est plus de savoir si une entreprise va être victime d'une attaque, ni même quand ou comment : il faut considérer que cette attaque est

"Toute entreprise doit reconnaître qu'elle sera inévitablement attaquée un jour : 100 % des tentatives de pénétration opérées par des spécialistes réussissent."

JEAN-PHILIPPE PAGES

certaine. Toute entreprise doit reconnaître qu'elle sera inévitablement attaquée un jour : 100 % des tentatives de pénétration opérées par des spécialistes réussissent. Par conséquent, manager un risque certain implique un management différent du schéma habituel (fondé sur une cartographie des risques qui probabilise survenance et coût), et c'est ici qu'intervient le principe de résilience, qui suppose avant tout d'anticiper la crise et de s'y préparer le plus régulièrement possible, avec des exercices de crise fréquents associant les parties prenantes concernées. Ainsi, un de nos clients, dirigeant d'ETI, a constaté qu'il n'avait pas organisé la mobilisation des experts dont il aurait absolument besoin pour remettre en activité ses systèmes d'information en cas de besoin. Ajoutons que si un grand nombre d'entreprises était touché simultanément sur le territoire national, la course aux experts qualifiés serait féroce et la remise en place rapide des réseaux s'en trouverait compromise. Une fois que l'entreprise a quantifié le risque et s'y est préparée, elle sera en capacité de rebondir, de revenir à un niveau d'activité nominal et d'assurer un niveau minimum à ses fonctions essentielles ou vitales. C'est de cette manière que la cyber résilience deviendra un avantage concurrentiel évident.

HUGO RONSIN
Quelle valeur une cyber assurance peut-elle apporter à une entreprise ?

JEAN-PHILIPPE PAGÈS
L'assurance n'aura une valeur forte que si l'entreprise peut manager son risque cyber et se préparer à affronter la crise. L'assurance n'est qu'un maillon de la chaîne de valeur de la cybersécurité de l'entreprise, celui du traitement du risque résiduel, après que toutes les défenses ont été transpercées par les agresseurs. Il s'agit alors d'indemniser les préjudices subis, principalement la perte financière ou les conséquences en termes de violation des données et la prise en charge des frais d'experts mobilisés.

Ce marché est naissant : l'encaissement des assureurs opérant en France est de l'ordre de 250 millions d'euros de prime (105 millions d'euros en 2019), soit 1 % du volume total engagé par les entreprises en France, et 5 % au niveau mondial. Les assureurs ont pris conscience de cette menace et sont donc devenus beaucoup plus prudents, ils professionnalisent leurs analyses et augmentent fortement leurs exigences en matière de prévention. L'assurance sera donc réservée aux entreprises capables de démontrer un niveau suffisant de maturité en cyber sécurité et l'existence d'un plan de cyber résilience robuste. Pour notre part, nous ne présentons jamais au marché de l'assurance le risque cyber d'un client sans l'avoir accompagné dans l'analyse et l'évaluation du risque, et sans avoir coconstruit avec lui un dossier extrêmement solide. Sans ces éléments, le marché de l'assurance n'est déjà plus en mesure d'offrir des solutions performantes face à ce risque. Cela signifie que, demain, l'accès au marché de l'assurance sera un avantage concurrentiel très fort pour les entreprises.

Débats

"Il faut faire de la cyber sécurité un élément de culture de l'entreprise, en se concentrant en priorité sur le facteur humain, car souvent, le déclencheur de la crise provient du clic malvenu d'un salarié."

JEAN-PHILIPPE PAGES

Hugo RONSIN
Guy-Philippe Goldstein, avez-vous repéré des bonnes pratiques et des pistes de solutions propres à renforcer la cyber résilience des entreprises, à l'échelle européenne et au-delà ?

Guy-Philippe GOLDSTEIN
La résilience englobe non seulement la préparation mais aussi la réponse à la crise, à travers laquelle l'entreprise peut démontrer à ses clients et à ses employés que la leçon a bien été apprise et qu'un palier a été franchi.

Un groupe industriel basé dans un pays nordique et disposant d'une filiale en France qui avait été particulièrement touchée a montré ses bonnes pratiques. Les principales sont les suivantes :

- En cas de crise, communiquer de la façon la plus fréquente et la plus transparente auprès des partenaires ; avoir une communication spécialisée et fournir de premières estimations de l'impact financier probable ; communiquer auprès des employés, par exemple à travers une chaîne YouTube pour leur permettre de faire part de leurs difficultés.
- Soigner la sauvegarde, car elle évite de devoir payer une éventuelle rançon.
- Effectuer un exercice de crise au moins une fois par an au niveau de la tête de l'entreprise, comme le recommande la Banque d'Israël.

Jean-Philippe PAGÈS
Nous constatons à travers toutes nos études que les entreprises les plus cyber résilientes sont celles qui ont bâti un système de gouvernance du risque transverse associant toutes les parties prenantes : DSI, RSSI, DRH, fonctions opérationnelles, etc. Il faut faire de la cyber sécurité un élément de culture de l'entreprise, en se concentrant en priorité sur le facteur humain, car souvent, le déclencheur de la crise provient du clic malvenu d'un salarié. Lors de la gestion de crise, si les équipes et les parties prenantes de l'entreprise sont préparées et prêtes à assumer la crise, elles seront également prêtes à contribuer au rebond.

Philippe de BRISOULT
Où en est la cyber sécurité dans le secteur public ?

Guy-Philippe GOLDSTEIN
Dans le domaine de la lutte informatique offensive, l'État français est performant, mais en matière de protection des opérateurs de services essentiels, des administrations nationales et des collectivités territoriales, la protection affiche un niveau moyen à dégradé. La gestion du risque se pose au monde public et je ne sais pas si les outils pour penser ce risque sont bien présents. À travers les attaques contre les hôpitaux et les mairies, nous constatons que des pans entiers du pays ne sont pas suffisamment protégés. Cela peut provenir d'un manque de prise de conscience.

“Nous avons créé un écosystème de prestataires à disposition de nos clients afin qu’ils obtiennent les réponses techniques qui leur manquent.”

JEAN-PHILIPPE PAGES

Hugo RONSIN
Pierre pose la question suivante : “Ne devrions-nous pas réfléchir à des solutions d’assurance mixant privé et public ?”

Jean-Philippe PAGÈS
C’est une piste. Il existe des solutions d’assurance mixant public et privé, notamment en matière de catastrophes naturelles et de risque terroriste. Nous y viendrons certainement, mais quel que soit le schéma retenu, il est certain que nous n’aurons pas de système d’assurance pérenne sans atteindre le niveau de maturité suffisant pour assurer le bon fonctionnement de la cyber sécurité. Selon nous, il importe d’interpeler sur les moyens à mettre en œuvre pour développer la prise de conscience et tendre vers les niveaux de cyber sécurité les plus élevés possible.

Pierrik CHAIGNAUD, sales Manager Business development d’Anozrway
Il est indispensable en effet que la cyber sécurité figure dans l’ADN et la culture de l’entreprise. En tant qu’assureur, recommandez-vous des bonnes pratiques à vos clients ?

Jean-Philippe PAGÈS
Tout à fait, car notre offre de valeur ne peut se limiter à la brique résiduelle de l’assurance dans la chaîne de valeur de la cyber sécurité. Les briques principales sont indispensables à la mise en place d’un contrat d’assurance. Nous avons créé un écosystème de prestataires à disposition de nos clients afin qu’ils obtiennent les réponses techniques qui leur manquent. Ainsi, notre partenariat avec Almond portant sur le scoring de la maturité en cyber sécurité peut susciter la prise de conscience du dirigeant.

Pierrik CHAIGNAUD
Je vous invite à consulter l’offre d’Anozrway, notamment en matière d’empreinte numérique humaine. Grâce à ce service, les entreprises prennent connaissance de ce que d’éventuels agresseurs verraient d’elles en termes de couverture humaine (emails connus, mots de passe ayant éventuellement fuité, capacité à être ciblé par des tentatives d’usurpation d’identité, etc.).

Marc WATIN-AUGOUARD, fondateur du FIC
Le thème de la résilience est passionnant car il nous amène à concevoir la cyber sécurité de manière collective. Nous devons absolument faire partager par le personnel de l’entreprise et de l’administration une culture cyber qui ne soit ni catastrophiste ni angélique. En effet, chacun a sa part responsabilité et la résilience dépend de cette somme de comportements individuels qui permettront à l’entreprise de résister.

Par ailleurs, il convient de d’assurer que la cyber sécurité monte bien jusqu’au comité exécutif de l’entreprise et qu’elle redescend jusqu’à la première personne qui pénètre dans l’entreprise le matin. L’organisation transversale et la capacité de réaction grâce à une organisation structurée, proche de celle d’un état-major militaire, avec des grandes fonctions, est également un élément déterminant auquel il convient de penser en amont, avant que ne survienne une crise.

Un dialogue entre l’assurance et l’entreprise est nécessaire. Cette dernière se prépare à la cyber résilience, ce qui donne confiance aux assureurs, tant le cyber risque devient difficile à assurer. Au sujet des collectivités territoriales, il est évident que l’administration reste en deçà de ce qu’elle devrait faire, malgré les efforts accomplis. C’est la raison pour laquelle j’ai créé l’Institut

national pour la cyber résilience des territoires, afin de mettre à niveau l'ensemble des acteurs publics sur ces questions.

Hugo RONSIN
Grégoire Lundi, quelle est la vision de l'ANSSI sur l'apport de l'assurance en matière de cyber résilience ?

Grégoire LUNDI, coordinateur sectoriel à l'Agence nationale de la Sécurité des systèmes d'information (ANSSI)
J'aimerais insister sur le bénéfice à retirer des exercices de crise d'origine cyber. Les entreprises peuvent également s'appuyer sur les guides de l'ANSSI.

"Il est nécessaire de développer une qualité cyber qui démontre que les entreprises du tissu national seront potentiellement moins attaquées que dans d'autres pays. Cela réduira les coûts et renforcera l'image de qualité de la France."

GUY-PHILIPPE GOLDSTEIN

Jean-Philippe PAGÈS
Nous recommandons en permanence à nos clients de se rendre sur le site de l'ANSSI et de télécharger les livrables élaborés, notamment le guide d'hygiène informatique, le guide permettant de définir la structuration du risk management cyber et le guide d'exercice de crise. Nous saluons régulièrement toute l'action de l'ANSSI en la matière.

Guy-Philippe GOLDSTEIN
Je confirme que l'exercice de crise est fondamental et que la préparation doit concerner tous les niveaux de l'entreprise, car l'erreur humaine est en cause dans 90 % des cas. Il est évident qu'il est préférable de se préparer à la gestion de la crise avant qu'elle ne survienne. Les directions générales et les conseils d'administration doivent être englobés dans cette politique. Il importe que les administrateurs connaissent le coût réel d'une éventuelle attaque.

J'aimerais enfin attirer votre attention sur la déclaration extrafinancière des entreprises au niveau européen. L'inclusion du risque cyber dans cet exercice devrait être envisagée afin que l'ensemble du tissu industriel comprenne le coût d'une attaque éventuelle.

Philippe METTOUX, directeur juridique et de la conformité de la SNCF
Nous nous sommes engagés vers une couverture cyber et avons tenu cette réflexion interne avec la gouvernance de l'entreprise. Bien évidemment, une couverture assurantielle du risque cyber ne rembourserait jamais les dégâts causés par une éventuelle attaque. Toutefois, comme c'est le cas du risque d'incendie, notre assureur nous apporterait son regard extérieur en nous indiquant où porter nos efforts.

Jean-Philippe PAGÈS
En effet, aucun risque industriel sensible ne trouve une couverture incendie s'il ne démontre pas un niveau de prévention efficace. Ce modèle en devenir permettra au marché de l'assurance cyber de maintenir une offre et d'être cyber résilient.

David GUYENNE, président de la Chambre de Commerce et d'Industrie de la Nouvelle-Calédonie
Existe-t-il une prime pour les petites entreprises qui appartiennent à la France ? Comment quantifier l'avantage de faire partie de l'ensemble français ?

Guy-Philippe GOLDSTEIN
Une vaste campagne de rançongiciels frappe actuellement l'occident et, en France, l'ANSSI a évoqué une augmentation de 255 % de ce nombre d'attaques. En regard, en Israël, où un très fort écosystème d'entreprises de cybersécurité a été bâti, le nombre d'attaques recensées par l'INCD, l'équivalent israélien de l'ANSSI, a augmenté de seulement 50 % en 2020. Il est nécessaire de développer une qualité cyber

qui démontre que les entreprises du tissu national seront potentiellement moins attaquées que dans d'autres pays. Cela réduira les coûts et renforcera l'image de qualité de la France.

Conclusion

Jean-Philippe Pagès

J'aimerais en conclusion faire référence aux propos du général Marc Watin-Augouard : la cyber sécurité ne peut être que collective. Il faut absolument continuer à marteler ce message et nous inscrire dans un dialogue public-privé qui est indispensable à notre réussite et au succès de nos entreprises, quels que soient leur secteur d'activité et leur taille.

Continuons à travailler sur la prise de conscience de la menace et les fondamentaux qui y concourent :

- La valorisation du risque, car sans chiffre aucune action sérieuse n'est possible.
- La maturité de l'entreprise en termes de cyber sécurité : il est clair qu'à terme un standard en matière de cyber sécurité verra le jour, il conditionnera l'accès à certaines ressources, y compris à l'assurance.

Je tiens à remercier l'ensemble des participants de cette rencontre pour ces échanges fructueux, et j'espère vous revoir très bientôt pour les prolonger et travailler à cette indispensable cyber sécurité collective.

Hugo RONSIN
Merci à toutes et à tous.