COMMUNIQUÉ DE PRESSE

BESSÉ
CONSEIL EN ASSURANCES

Le risque de défaillance des ETI françaises augmente de 80% à la suite d'une attaque cyber

RÉSULTATS D'UNE ENQUETE BESSÉ SUR L'IMPACT D'UNE CRISE CYBER SUR LA VALORISATION DES ENTREPRISES NON COTÉES

Paris, le 2 décembre 2020

Le 4 novembre 2020, Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI), s'est inquiété de l'explosion de la grande criminalité dans le champ cyber, soulignant que le nombre d'attaques aux rançongiciels avait été multiplié par 3 ou 4 en un an (128 attaques répertoriées au 30 septembre 2020, contre 54 pour l'ensemble de l'année 2019). Ces actes malveillants augmentent à mesure que se développent les usages du numérique et cela, rappelle-t-il, ne devrait pas s'amoindrir, en raison des risques liés à la généralisation du télétravail dans ce contexte de crise sanitaire. Inhérente à la digitalisation des entreprises et de leur écosystème, la menace cyber figure désormais parmi les trois plus grands risques auxquels elles sont aujourd'hui confrontées. Pourtant, 80% d'entre elles, en France, n'ont toujours pas mis au point de plan de réponse leur permettant de faire face à un incident cyber robuste[1] ! Si ce risque était déjà prégnant hier, la crise COVID a accéléré l'imminence de la menace : de janvier à avril 2020, les attaques de rançongiciel ont d'ailleurs augmenté de 25%[2]... Le déploiement à venir de la 5G représente également un véritable défi à relever en termes de cybersécurité, puisqu'il risque de multiplier le nombre de points d'entrée potentiels pour les hackeurs... Face à l'urgence et soucieux d'accompagner au mieux les entreprises (plus particulièrement les ETI) dans la gestion de cette menace d'envergure, Bessé a réalisé au mois de novembre 2020, une étude permettant de mesurer l'impact réel d'une attaque cyber sur la valorisation et la réputation des entreprises non cotées. A la lumière des principaux enseignements tirés, cette étude revient également sur les comportements et solutions que les entreprises doivent adopter afin d'anticiper et maîtriser les conséquences d'une attaque cyber.

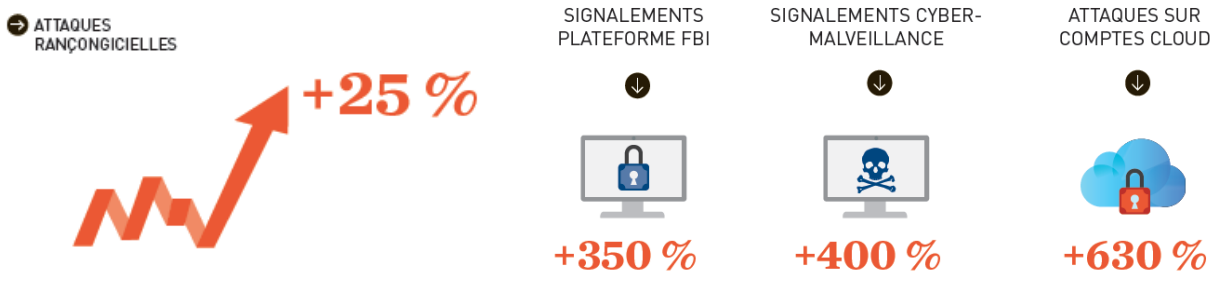
L'état de la menace cyber en quelques chiffres

- **76%** des dirigeants d'ETI déclarent avoir subi au moins une incidence cyber en 2019[3]
- **90%** des entreprises françaises ont été victimes de cyber-attaques en 1 an[4]
- **12%** des entreprises ont connu des attaques par rançongiciel[5]
- **80%** des entreprises françaises n'ont pas de plan de réponse aux incidents robustes[6]
- **86%** des entreprises sondées n'ont toujours pas souscrit de contrat cyber-assurance[7]
- **+ de 1 100** victimes d'attaques par rançongiciel en France depuis début 2020 (dont 26% de particuliers)[8]

[1] Source : IBM/Ponamon Institute
[2] Source : étude Bessé Novembre 2020
[3] Source : Étude Cyber Bessé – PwC 2017
[4] Source : étude Forrester 2020, commandée par Tenable et menée auprès de 800 RSSI dont 104 français
[5] Enquête CLUSIF 2020 Entreprise de plus de 100 salariés
[6] Source : IBM/Ponamon Institute
[7] Enquête CLUSIF 2020 Entreprise de plus de 100 salariés
[8] Source : www.cybermalveillance.gouv.fr

- **5 200 milliards de dollars : coût de la cybercriminalité, estimé par l'ONU, pour l'économie mondiale entre 2020 et 2025**[9]

Augmentation du risque cyber pendant la crise Covid-19[10]



Le dirigeant d'entreprise à la fois victime et coupable d'une attaque cyber

Dans la cartographie des risques des entreprises, le risque cyber occupe une place particulière. Il ne s'inscrit dans aucune grille de lecture et d'analyse traditionnels. Une cyber-attaque constitue une agression qui se rapproche plus du modus operandi militaire que d'une incursion économique ou boursière non désirée. Elle ne répond néanmoins à aucun des codes conventionnels de l'affrontement : difficulté majeure d'identifier l'adversaire et donc de concevoir une riposte, ce qui complique substantiellement la gestion d'une crise cyber…

> *« Ayant un impact à la fois stratégique, technique et financier, les attaques cyber ont des conséquences qui affectent véritablement la viabilité des entreprises. Dans ce contexte de crise sanitaire, l'impact d'une attaque cyber risque, par ailleurs, d'être d'autant plus important que les entreprises sont déjà fortement fragilisées. Si cette menace est complexe à appréhender, les dirigeants d'entreprise doivent donc urgemment se saisir de la question… »*, déclare **Pierre Bessé, Président de Bessé**.

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

Le rôle du dirigeant en amont de l'attaque est d'autant plus capital qu'il endosse le double rôle, quelque peu paradoxal, de victime et de coupable, à l'égard de l'agresseur et du client.

> « Il se révèle, en effet, extrêmement difficile pour l'entreprise et son dirigeant d'échapper au procès en négligence, *car la réussite d'une cyber-agression signe par essence l'échec plus ou moins important des dispositifs de défense. S'agissant d'une obligation de moyens et non de résultats, l'entreprise doit donc rapporter la preuve qu'elle avait mis tout en œuvre pour faire face à une agression de cette nature.* » ajoute **Caroline Ruellan**.

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

L'étude menée, en novembre 2020, par le courtier en assurances Bessé avec le **concours de Guy-Philippe Goldstein, enseignant-chercheur à l'École de Guerre Économique**, met en avant les points clés suivants :

1. **Le risque cyber est stratégique et vital pour l'entreprise.** Il est dès lors primordial d'évaluer, en amont, les coûts directs et indirects potentiellement générés par une

[9] Octobre 2020

[10] Sources précisées dans l'étude cyber de Bessé de novembre 2020

attaque cyber, afin de déterminer l'importance des investissements à accorder pour s'en prémunir ou en maîtriser les conséquences.

2. **Le choc économique est observable, pour les entreprises cotées, à travers l'évolution du cours de bourse.** Dans 63 % des incidents, **le cours de bourse baisse d'environ 9 % en moyenne au bout d'un mois**, comparé à son niveau avant l'annonce de l'incident. Deux destins se dessinent ensuite, sur ce même panel d'entreprises : 40% d'entre elles poursuivent un déclin de l'action en bourse jusqu'à -20% un an après, tandis que les 23% restants rebondissent après 3 mois de crise[11].

3. **Pour les entreprises non cotées, ce choc peut s'évaluer à l'analyse du score de défaillance de l'entreprise et du nombre de jours de retard de paiement.** Ces deux facteurs offrent en effet une vision globale de la stabilité économique de l'entreprise et de sa capacité à faire face à ses échéances. Ces indicateurs permettent de pallier le manque d'information de marché (à l'inverse des entreprises cotées) pour mesurer véritablement l'impact d'une crise cyber sur la valorisation des entreprises non cotées.

4. **En moyenne, le taux de défaillance de l'échantillon des entreprises internationales non cotées étudiées, augmente de 40% à 50% dans les trois mois** après l'annonce de l'incident cyber.

   « Quoiqu'il en soit, pour le panel combiné d'entreprises françaises et étrangères, un maximum de la crise cyber est atteint au 3ème mois, avec une élévation du risque de défaillance de +51% comparé à avant la crise », explicite **Guy-Philippe Goldstein, enseignant-chercheur à l'École de Guerre Économique**.

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

6. A la suite de l'augmentation du risque de défaillance des entreprises, **la dégradation de leur valeur patrimoniale peut être estimée à 8% à 10%**, après l'annonce de l'incident cyber.

7. Différentes études de cas démontrent que **les incidents cyber mènent, majoritairement, à une dégradation forte et plus ou moins temporaire de l'activité de l'entreprise** et, dans de rares situations, à une cessation d'activité. L'étude **confirme également que les entreprises non cotées les plus fragiles** sont celles qui n'ont **pas encore mis en place de politique de gestion des risques et de cyber-résilience**.

8. Ces premiers tests **renforcent l'hypothèse selon laquelle une attaque cyber constitue un événement critique pour une PME ou une ETI** et révèlent l'impact significatif d'un tel incident sur sa stabilité économique et la valorisation de l'entreprise non cotée : une **augmentation du risque de défaut de l'entreprise comprise entre 40% et 80%**, à la suite d'une attaque cyber.

9. **Le risque cyber, une fois annoncé, impacte directement la réputation d'une entreprise** (auprès de ses clients, fournisseurs et salariés). Ce risque doit donc **faire l'objet d'un processus de gestion et de communication parfaitement adapté**.

   « La réputation est l'actif immatériel le plus précieux dont dispose l'entreprise. Le risque cyber doit donc faire l'objet d'un process de gestion dédié. Dès lors, une fois l'attaque lancée et identifiée, les entreprises doivent accepter de mener la bataille de la communication en externe, comme en interne, en gardant en mémoire deux règles d'or : le refus d'admettre la crise ne peut que l'aggraver et une forte exposition médiatique marque

[11] Source : l'étude PwC France, réalisée avec G-P. Goldstein, sur 30 incidents.

durablement les mémoires. » précise **Laurent Porta, associé Vae Solis, spécialiste de la communication de crise et de la prévention des risques**.

10. **La cyber-résilience devient un atout concurrentiel, créateur de valeur pour l'entreprise, au sein de son écosystème**. Une dynamique qui peut se décomposer en trois éléments clés :
    - → **La préparation à la réaction au choc**, **bien avant que le choc ne se produise** : celle-ci induit la mise en place d'un plan de réponses adapté et souple afin de pouvoir le réadapter, en fonction de la situation. Or, à ce jour, 80% des entreprises françaises n'ont aucun plan de réponse leur permettant de faire face à un incident cyber robuste[12].
    - → **L'absorption du choc initial** qui permet à l'entreprise de gagner du temps pour réagir de manière appropriée. Cela nécessite, bien souvent, des capacités redondantes (copies de ses données) et l'accès à des facilités de crédit pour tenir davantage, face aux pertes financières générées par l'incident (ce que les entreprises non cotées obtiennent d'ailleurs moins aisément que les entreprises cotées. Si celles-ci sont donc plus agiles et réactives en cas de crise, elles sont également plus exposées sur un plan financier que les entreprises cotées, et donc plus fragiles…).
    - → **L'agilité et l'ouverture dans la réponse** passant par une vision de sortie de crise clairement exprimée par la direction, la mise en place d'actions décentralisées à tous les niveaux de l'entreprise et une bonne communication interne et externe afin de protéger la confiance de ses clients et de ses collaborateurs.

« Ainsi, comme pour la crise Covid-19, [...] même sans vaccins "anti-virus", il y a des moyens pour réduire le choc. [...] Mais, comme les masques, on omet de les appliquer. Le résultat de cette omission peut être grave et sévère… », constate **Guy-Philippe Goldstein**.

La cyber-résilience doit se trouver au cœur de la gouvernance des entreprises

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

« Une gestion maîtrisée du risque cyber induit notamment la prise de conscience du comité de direction, la définition d'une stratégie de résilience précise basée sur un constat réaliste de la menace, le déploiement homogène de solutions préventives et de gestion de crise, une politique de maintenance et de mise à jour des programmes de gestion des risques et des assurances. » ajoute **Jean-Philippe Pagès, Directeur Bessé Industrie & services**.

Révolution technologique et défis de la cybersécurité : le cas de la 5G

« La généralisation du télétravail engendrée par la crise sanitaire a renforcé d'évidence la porosité des entreprises au risque cyber, ouverture des systèmes d'information et management à distance en sont sans doute les deux principales causes. Une porosité qui risque de s'accroître véritablement avec le déploiement désormais acté de la 5G en France… Face à cette menace cyber croissante, le concept de résilience organisationnelle est devenu un modèle.

[12] Source : IBM/Ponamon Institute

Néanmoins, le défi de la cybersécurité ne pourra être relevé que grâce au développement de solutions et dispositifs publics-privés » déclare **Pierre Bessé**.

Selon le dernier rapport de la Commission européenne et l'Agence européenne pour la cybersécurité (ENISA), publié en 2019, sur les défis de la cybersécurité dans les réseaux 5G, les changements technologiques augmentent la surface d'attaque globale et le nombre de points d'entrée potentiels pour les acteurs de la menace.

« Afin de relever le défi, la France a répondu aux inquiétudes par une loi (« la loi Huawei ») qui prévoit que toute personne souhaitant mettre en place un réseau 5G devra obtenir une certification validée par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Un nouveau dispositif de contrôle des équipements télécoms a été mis au point, conduit par l'ANSSI. Ce dispositif s'applique quel que soit l'équipementier et son pays d'origine. Nous sommes véritablement à l'orée d'une révolution industrielle et technologique, sans précédents ! » souligne **François Barrault, président de l'IDATE Digiworld**.

BESSÉ
CONSEIL EN ASSURANCES

Les hommes et les femmes de Bessé sont des experts spécialisés dans le conseil et le service aux entreprises. Leur métier est centré sur le conseil sur-mesure en assurance, et l'accompagnement quotidien et durable de leurs clients en France et à l'international. Fort de ses 460 collaborateurs, Bessé est un acteur solide et incontournable du secteur. Fondé il y a près de 60 ans, il est aujourd'hui l'un des leaders français du conseil et du courtage en assurances pour les entreprises, et apporte plus de 900 Millions € de primes au marché de l'assurance.

CONTACTS PRESSE A+ CONSEILS

Clara DALLAY
clara.aplusconseils@gmail.com
+(33)6 48 45 01 53

Christelle ALAMICHEL
christelle@aplusconseils.com
+(33)6 31 09 03 83