COMMUNIQUÉ DE PRESSE

BESSÉ

CONSEIL EN ASSURANCES

SEULS 32% DES DIRIGEANTS D'ETI CONSIDERENT QUE LEUR ENTREPRISE EST TOUT À FAIT PREPAREE À AFFRONTER UNE CRISE CYBER

ENQUÊTE BESSÉ – IFOP SUR LES ETI FACE A LA MENACE CYBER

Paris, le jeudi 28 novembre 2019

La menace cyber évolue. Elle gagne en gravité, en probabilité et en imprévisibilité… Cela s'est traduit en 2019 par la multiplication des entreprises victimes d'attaques informatiques, quel que soient leur taille ou leur secteur d'activité. Les exemples sont nombreux : Altran, Norsk Hydro –Technal, Aebi-Schmidt, Fleury Michon, Eurofins, Asco, Ramsay Générale de Santé, Airbus, M6, Accord, Edenred…et bien d'autres qui n'ont pas souhaité communiquer… Aujourd'hui les entreprises de taille intermédiaire (ou ETI) comme les grands groupes sont les cibles de ces attaques et peuvent s'en trouver lourdement affectées… Pourtant peu d'entre elles sont aujourd'hui véritablement préparées à faire face à une telle menace.
Soucieux de les accompagner au mieux dans la gestion de ce risque d'ampleur, Bessé a mené, avec l'IFOP, une enquête spécifique auprès des ETI françaises. Celle-ci révèle notamment que la perception du risque cyber par les dirigeants d'ETI progresse mais qu'ils sous-dimensionnent encore sa portée stratégique et les moyens à déployer pour y faire face efficacement.

Qu'est-ce que le risque cyber ?

Si les dirigeants d'ETI et leurs équipes sont aujourd'hui en capacité d'anticiper et de gérer au quotidien les risques industriels qui pèsent sur leurs entreprises, ceux-ci le sont bien moins face à la menace cyber…

> *Selon **Pierre Bessé, président de Bessé**, « Le risque cyber, est singulier. Il appartient à une nouvelle génération de risques qui peut affecter l'entreprise dans sa globalité, dont la complexité est extrême et les caractéristiques diamétralement opposées à celles du risque industriel. »*

Le risque cyber est :

- Hautement **évolutif**, peu traçable et anticipable, souvent délocalisé
- Principalement **d'origine malveillante**, comportant de potentiels relais internes humains au sein de l'entreprise qui peuvent déclencher une crise par erreur ou négligence
- Un risque **systémique** pouvant toucher la totalité du bilan d'une entreprise, en une seule occurrence, avec une probabilité de survenance très élevée
  Les grandes entreprises sont « perçues à tort comme beaucoup plus exposées. Nombreux sans doute sont les dirigeants d'ETI qui pensent peut-être ne pas pouvoir s'offrir un tel luxe et espèrent tout à la fois passer à travers les gouttes… » ajoute **Jacques Fradin, docteur en médecine, spécialiste en psychologie cognitive**.

Les ETI Face à la menace cyber : une perception qui évolue mais des réponses sous-dimensionnées

Les résultats de l'enquête Bessé réalisée par l'IFOP[1] en octobre 2019 mettent en avant les points clés suivants :

1. **La perception, par les dirigeants d'ETI, du caractère stratégique du risque progresse** : 35% d'entre eux considèrent le cyber comme un risque stratégique. Cela signifie qu'une entreprise sur trois prend en considération la gestion du risque au niveau de ses organes de direction. Néanmoins la grande majorité des dirigeants d'ETI interrogées (55%) évalue ce risque comme important mais non prioritaire, et tout particulièrement ceux à la tête d'entreprises de moins de 1000 salariés (où ce taux passe à 61%) …
2. **L'estimation de leur exposition au risque cyber reste mitigée** : les dirigeants d'ETI estiment en moyenne à 5,8 sur 10 le risque de cybermenace pour leur entreprise. Plus précisément, 56% des sondés considèrent leur exposition à ce risque comme très importante ou importante, tandis que les 44% restants la qualifie de modérée (21%) voire faible à inexistante (23%).
3. **Seuls 32% des dirigeants d'ETI estiment que leur entreprise est tout à fait préparée pour affronter une crise cyber mais 89% des sondés se disent préparés et ce, quel que soit le niveau estimé d'exposition au risque**… Et parmi les 32% certains d'être préparés à affronter une attaque cyber, 53% considèrent être faiblement voire nullement exposés au risque cyber… En d'autres termes, les dirigeants qui jugent le niveau de la menace cyber faible voire inexistant estiment être autant prêts à affronter une attaque cyber que ceux qui évaluent la menace comme très importante. Or, les mesures et les moyens à mettre en œuvre pour affronter une crise cyber supposent un niveau de maturité élevé quant à l'appréhension de ce risque et des investissements à réaliser pour le maîtriser…
4. **Seuls 3% des dirigeants interrogés envisagent d'embaucher dans les 12 prochains mois un profil dédié à la gestion de la cybersécurité** : or le recrutement d'un spécialiste disposant des compétences dédiées ne se limitant pas à une vision technique de la sécurité informatique est généralement considéré comme un signe fort de la prise de conscience de la menace. …
5. **61% des dirigeants sondés disent que leur entreprise dispose d'assurances couvrant le risque cyber**. Mais, selon la Fédération Française des Assureurs (FFA) le volume de primes collectées en France en 2018 en assurance cyber est encore très faible (80 millions d'€) et le taux d'équipement des ETI estimé par certains à moins de 10%... Les dirigeants d'ETI disposent-ils d'une couverture contribuant à la cyber résilience de leur entreprise ? La question mérite d'être vérifiée.

> *« Les résultats de cette enquête marquent une progression de la prise de conscience des dirigeants d'ETI. Plus sensibilisés qu'hier, ils ont intégré la dimension stratégique du risque mais force est de constater que l'effort de sensibilisation doit être maintenu et les investissements à déployer pour se protéger encore à accentuer » ajoute Pierre Bessé.*

Bessé engagé dans la cyber-résilience…

Le risque cyber n'est pas un risque technique mais un risque stratégique. Cela implique de faire évoluer les solutions traditionnelles de traitement du risque pour mieux le maitriser en prévoyant notamment :

1. **La mise en œuvre d'une gouvernance spécifique transverse à l'entreprise permettant d'inscrire le risque cyber dans un processus agile d'amélioration continue globale et de favorisant les REX** (retour d'expérience) à tous les niveaux de l'organisation et de son écosystème.

[1] Enquête réalisée en novembre 2019 sur la base d'un échantillon représentatif de 150 dirigeants d'entreprises de taille intermédiaire (entreprise de 250 à 4999 salariés, dont le chiffre d'affaires est inférieur à 1,5 milliards d'euros)

2. **L'accompagnement les dirigeants et leurs équipes** : sensibiliser, faciliter, de l'amont à l'aval, former au management de risque, de crise, mutualiser les interventions d'experts spécialisés en gestion de crise etc.
3. **La construction de réseaux d'échanges et de coopération inter-entreprises** pour s'enrichir des différentes expériences vécues voire de mutualiser certaines ressources clés

> *« Il est essentiel de contribuer à renforcer la cyber-résilience de nos entreprises en communiquant sur les enjeux et les conséquences du risque cyber et, en favorisant le partage d'expérience et la diffusion des bonnes pratiques. » conclut* ***Pierre Bessé****.*

C'est dans cette optique que Bessé contribue à bâtir un espace propice à la réflexion et à la collaboration inter-entreprises, associant les personnalités du public et du privé, pour favoriser les échanges, les retours d'expérience entre dirigeants et diffuser les meilleures pratiques à adopter face à la menace cyber.

BESSÉ
CONSEIL EN ASSURANCES

Les hommes et les femmes de Bessé sont des experts ultraspécialisés dans le conseil et le service aux entreprises. Plus que simples courtiers, 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 450 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)1 44 18 65 58 / +(33)6 48 45 01 53

Christelle ALAMICHEL
christelle@aplusconseils.com
+(33)1 44 18 65 58 / +(33)6 31 09 03 83