ENQUÊTE IFOP POUR BESSÉ

NOVEMBRE 2019

LES DIRIGEANTS D'ETI FACE À LA MENACE CYBER

POINT DE SITUATION

BESSÉ

CONSEIL EN ASSURANCES

PIERRE BESSÉ
Président de Bessé

En mars 2018, nous éditions en collaboration avec PwC notre première étude consacrée à la perception de la menace cyber par les dirigeants d'Entreprises de Taille Intermédiaire. Sous la pression des actionnaires et des règles de conformité, les grands groupes internationaux avaient pris la mesure de l'enjeu. Nous souhaitions aborder ce thème avec les dirigeants d'ETI, moins sensibilisés mais tout aussi concernés et exposés.

Depuis, l'évolution de la menace s'est traduite par une forte augmentation du nombre d'entreprises victimes d'attaques cyber, en particulier des ETI françaises, de toute taille et de tout secteur d'activité, souvent durement affectées.

Dix-huit mois plus tard, il nous est donc apparu nécessaire de prolonger nos travaux de recherche à la faveur d'une enquête réalisée pour notre compte par l'IFOP.

Les résultats de cette enquête sont positifs. Ils soulignent que la prise de conscience du risque cyber par les dirigeants progresse et c'est une très bonne nouvelle.

Ils restent cependant contrastés et à interpréter avec circonspection. Bien plus sensibilisés qu'hier, les dirigeants d'ETI ont réagi et 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. Nos échanges permanents avec les dirigeants et l'ensemble des parties prenantes des sphères publiques ou privées, experts en la matière, ne font que le confirmer régulièrement.

Sans anxiété excessive, la vigilance s'impose : restons mobilisés et continuons à renforcer la cyber-résilience de nos entreprises !

Très bonne lecture.

Analyse de
JACQUES FRADIN

« Face à la menace Cyber, les dirigeants d'Entreprises de Taille Intermédiaire évoluent mais leurs réponses restent globalement sous-dimensionnées. Pourquoi ? Que faire ? »

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 ».*

L'attitude quelque peu attentiste, immobiliste, circonspecte des dirigeants d'ETI déjà observée en 2018 lors de la première étude réalisée par BESSÉ et PwC montre une évolution significative mais pas encore une révolution dans l'appréciation de ce risque majeur et de sa prise en charge.

Pourtant, la menace gagne en gravité, en probabilité, et en imprévisibilité…

Sans doute les mêmes facteurs persistent et le risque perçu comme à la fois trop :

- Flou, lointain, immatériel
- Incernable, inquiétant, complexe
- Objet d'un métier de l'interne, jusqu'ici souvent non stratégique…

Les grands facteurs de résistance au changement semblent donc réunis :

- La nouveauté qui rend le risque, par essence abstrait, plus irréel encore, au profit d'enjeux du quotidien plus pressants, plus concrets et tout à la fois plus bénins et rassurants
- La gravité et la complexité des risques qui incitent paradoxalement à l'attentisme voire au fatalisme : *« il est urgent d'attendre »*; *« laissons se décanter le risque »*, *« ce sont les risques du métier »*…

Ceci survient aussi dans un contexte où l'on voit :

- Se multiplier les risques nouveaux et non des moindres : climatiques, écologiques, technologiques, économiques, sociaux, géopolitiques, migratoires…
- La rencontre d'un *« modèle libéral décomplexé et triomphant »* depuis la chute du mur de Berlin, focalisé sur sa rentabilité à court terme…
- Un *« avenir incertain teinté de collapsologie »*…

A cela s'ajoute sans doute une dose de *« fuite en avant »* et on comprend aisément que l'actualité ne soit pas précisément propice aux réflexions de fond ni toujours à une sage gestion du futur en *« bon(ne) père(mère) de famille »*.

Enfin, et pour corser le tout, le risque Cyber appartient véritablement à un genre nouveau:

- Hautement évolutif, peu traçable et anticipable, décalé, délocalisé voire émanant de territoires *« complices »*
- Comportant de potentiels relais internes humains au sein de l'entreprise, conscients et malveillants ou déclenchant la crise par erreur ou négligence
- Avec des conséquences économiques potentiellement très lourdes et une probabilité de survenance pas si faible que cela…

Tout ceci semble donc faire de ce risque un luxe de grandes entreprises … 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 »*… ?

Que faire alors pour porter remède à ce risque singulier ?

Il semble logique de faire évoluer les solutions traditionnelles de traitement du risque en renforçant les capacités de résilience de l'entreprise pour faire face à une éventuelle crise cyber, dès les premières heures de la phase aigüe jusqu'à accompagner l'émergence de solutions durables, dans leur composante économique (trésorerie, réinvestissement…), stratégique, technique, et facteur humain (via notamment des ressources externes spécialisées).

Il pourrait revenir ainsi aux acteurs de la gestion de risque d'aller jusqu'à proposer tout ou partie d'un *« package gouvernance, anticipation, sensibilisation, prévention, protection traitement des risques, gestion des crises et des phases de rebond avec préparation aux agilités stratégiques, managériales et individuelles »*,

que les dirigeants et leurs équipes pourraient déployer pour tirer de ce *« nouveau monde »* plus d'opportunités que de périls et faire des accidents de parcours de nouveaux départs !

La rhétorique et les cibles de la communication de tous gagneraient aussi à changer, car :

- La dramatisation d'un risque incernable et peu maîtrisable est moins porteuse qu'une opportunité, qu'un projet, ou que toute autre expérience fédératrice
- L'attente l'est moins que l'action (curative, résiliente, préventive…)
- La décision solitaire l'est moins que la mobilisation et l'engagement des équipes
- La peur des agressions et de leurs effets l'est moins que l'identification des fragilités internes et celle, stratégique, des réformes structurelles, systémiques induites…

Enfin, pour aller plus loin dans la compréhension et l'optimisation du facteur humain, au cœur de la crise comme de ses solutions, on gagnerait à davantage partager quelques aspects très éclairants et opérationnels de la connaissance du fonctionnement de notre propre cerveau et de nos comportements.

La décision humaine subit en effet de nombreux biais :

- En situation de non contrôle, notre cerveau se met par défaut en posture de repli voire en évitement, en déni. Ceci explique sans doute pourquoi certains répondants à la présente étude IFOP se croient bien protégés… contre toute raison !
- Le manque ou l'excès de confiance en soi, qui découlent largement des mécanismes irrationnels de dominance, de soumission (car impliquant de très vieilles structures cérébrales comme les amygdales limbiques…), distordent notre perception de la réalité et des risques. Un sujet *« soumis »* est plus à même de surprotéger l'entreprise, privilégier 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, via une surestimation de sa capacité à faire face… voire une confiance très irrationnelle dans sa *« bonne étoile »* ! Ce qui peut là aussi entraîner un déni, pour des raisons diamétralement opposées à celles de la peur…
- Le risque subi (on se sent avant tout victime…) est aussi plus facile à gérer *« émotionnellement »* que le risque pris (notre responsabilité voire culpabilité est engagée, plus encore lorsque notre image sociale est engagée), ce qui peut pousser à la non-décision !
- Le manque d'authenticité dans les échanges, au sein de Comités de Direction par exemple, peut induire le *« paradoxe d'Abilène[1] , l'origine de décisions absurdes, chacun alors, en son for intérieur, ne croyant pas ou peu à leurs pertinences (« on ne sent pas la décision »*, mais, faute d'arguments précis ou par peur de briser un difficile consensus… on n'ose pas le dire) !…
Pour le prévenir, au-delà des classiques leviers *« objectifs »* de décision (pourtant largement issus de données du passé), on gagne à créer des conditions favorables, à laisser un temps bref (comme en brain storming ou groupe de parole) à l'expression de l'intime conviction, l'intutition, souvent pertinente et prospective (notamment lors de la phase finale de la prise de décision) en contexte nouveau, incertain et complexe, ainsi que le montrent de nombreuses études
- Une *« mauvaise décision »* est par ailleurs rapidement anxiogène, même pour les décideurs, et cela s'aggrave au fil du temps (stress cognitif, traduisant un conflit interne plus qu'un péril externe…)
- Les dirigeants et leur collectif gagnent donc généralement à apprendre à mobiliser leurs intelligences adaptatives et celles de leurs équipes, plus apaisantes et mobilisatrices qu'un management plus directif et (faussement) *« protecteur »* !

[1] Le paradoxe d'Abilene, présenté dans l'ouvrage *« The Abilene Paradox and Other Meditations on Management »*, du sociologue Jerry Harvey illustre la façon dont un groupe peut prendre des décisions absurdes.

[2] Dijksterhuis, Ap (2004). *«Think Different: The Merits of Unconscious Thought in Preference Development and Decision Making»*. Journal of Personality and Social Psychology. 87 (5): 586–598.

EN SYNTHÈSE :

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

Mes pistes de réflexion pour « le traitement singulier d'un risque singulier » sont les suivantes, elles seraient bien sur à adapter par les dirigeants aux spécificités de leurs entreprises :

1. Inscrire le risque dans un processus d'agilité et d'amélioration global, à la façon dont les acteurs de l'aéronautique et autres activités à risques majeurs l'ont depuis longtemps mis en oeuvre avec le REX (retour d'expérience), qui impacte tous les niveaux de l'organisation et tire de l'analyse des failles et initiatives de chacun un levier majeur de performance et d'innovation (« le plus lourd que l'air ne tombe plus ! »...).
2. Accompagner les dirigeants et leurs équipes : sensibiliser, faciliter, de l'amont à l'aval, former au management de risque, de crise, coachings (cognitifs) spécialisés préparant à une meilleure gestion de soi et des autres en situations difficiles, mutualiser des interventions d'experts spécialisés dans l'accompagnement de cellules de crise, pilotes de chasse, sportifs de l'extrême, personnels hospitaliers...
3. Faciliter la construction de réseaux de coopération entre entreprises ayant surmonté ce type d'événement et d'autres cherchant à s'y préparer ou à les gérer, à mutualiser leurs ressources...

De telles démarches, individuelles et collectives, sont souvent au cœur des leviers de développement et d'innovation : c'est ce que l'on appelle une EXTERNALITÉ POSITIVE (et pas des moindres !).

PARTIE 01

Méthodologie de l'enquête

01

MÉTHODOLOGIE

ÉCHANTILLON

L'enquête a été menée auprès d'un échantillon représentatif de 150 dirigeants d'entreprises de taille intermédiaire (entreprises de 250 à 4999 salariés et dont le chiffre d'affaires est inférieur à 1,5 milliard d'€uros).

MÉTHODOLOGIE

La représentativité de l'échantillon a été assurée par la méthode des quotas selon les critères détaillés (nombre de salariés et chiffre d'affaires) et de secteurs d'activité.

MODE DE RECUEIL

Les interviews ont été réalisées par téléphone du 7 au 25 octobre 2019. Seuls les membres de la Direction Générale ou du Comité de Direction ont été interrogés.

CE QU'IL FAUT RETENIR EN 5 POINTS CLÉS

#1

La perception du caractère stratégique du risque cyber par les dirigeants d'ETI progresse.

#2

Mais l'estimation du risque par les dirigeants d'ETI reste mitigée : sur une échelle de 0 à 10, les dirigeants d'ETI estiment en moyenne à 5,8 sur 10 le risque de cyber-menace pour leur entreprise.

#3

Le jugement des dirigeants sur leur capacité à affronter une crise cyber interpelle et n'est pas sans équivoque : seuls 32% des dirigeants d'ETI considèrent que leur entreprise est tout à fait préparée mais 89% des sondés se considèrent préparés quel que soit le niveau d'appréciation de la menace cyber pour leur entreprise.

#4

Seul 3% des dirigeants interrogés envisagent d'embaucher au cours des douze prochains mois un profil dédié à la cyber sécurité.

#5

61% des dirigeants sondés disent que leur entreprise dispose d'assurances couvrant le risque de cyber-attaques et ses conséquences financières.
Ce résultat est paradoxal au regard du faible volume de primes collectées par les assureurs en France.

La perception du risque cyber progresse mais les réponses des dirigeants d'ETI indiquent qu'ils sous-dimensionnent encore sa portée stratégique.

PARTIE 02

Résultats de l'enquête et analyse

02

35%

des dirigeants interrogés positionne désormais le risque cyber comme un risque stratégique

#1

La perception du caractère stratégique du risque cyber par les dirigeants d'ETI progresse

UN SUJET STRATÉGIQUE : 35 %

DÉTAIL

	%
SECTEUR D'ACTIVITÉ	
Industrie / BTP	41
Commerce / Services	31
TAILLE DE L'ENTREPRISE	
Moins de 1000 salariés	26
1000 salariés et +	59
CHIFFRE D'AFFAIRES	
De 50 à 99 millions	34
100 à 199 millions	26
Plus de 200 millions	45

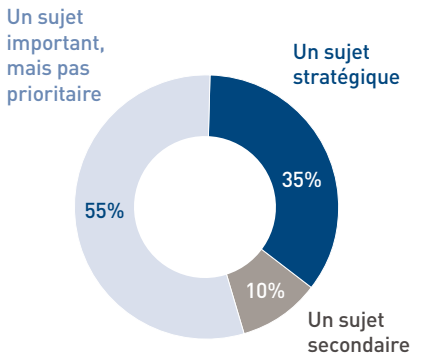
L'enquête Bessé/PwC auprès des dirigeants d'ETI publiée en mars 2018 soulignait que 76% d'entre eux avaient subi au moins un incident cyber au cours des douze derniers mois et étaient sensibilisés au risque mais le considéraient plutôt comme un risque technique que stratégique.

La médiatisation de ce risque, toujours aussi appuyée et la multiplication d'entreprises victimes sur le segment des ETI positionne désormais le risque cyber comme un risque stratégique pour 35% des dirigeants interrogés. Ce pourcentage passe à 45% pour les entreprises de plus de 200 millions de CA et à 59% pour les entreprises de plus de 1000 salariés.

C'est une bonne nouvelle. Cette dimension stratégique d'abord identifiée au niveau des très grands groupes s'étend progressivement vers l'ensemble des entreprises. Cela signifie qu'environ une entreprise sur trois prend en considération la gestion du risque cyber au niveau des organes de direction. Le sujet n'est donc plus uniquement un sujet technique réservé à la Direction des Systèmes d'informations. Les enjeux sont tels qu'il prend une ampleur bien supérieure dans sa prise en compte.

Toutefois et si la prise de conscience progresse, on note toutefois que pour une bonne majorité (55%) et encore plus pour les entreprises de moins de 1000 salariés (61%), le sujet est certes important mais pas prioritaire. Si la menace est identifiée à sa juste mesure, la majorité des dirigeants interrogés ne la projette pas dans leur propre organisation. Nous vérifions d'ailleurs ce point très régulièrement aux contacts d'interlocuteurs qui estiment toujours que leur entreprise ne constitue pas une cible en raison soit de son domaine d'activité ou d'une taille limitée.

AUJOURD'HUI LA CYBER-SÉCURITÉ DE VOTRE ENTREPRISE EST...



ENQUÊTE IFOP POUR BESSÉ

#2

L'estimation du risque par les dirigeants d'ETI reste mitigée : sur une échelle de 0 à 10, les dirigeants d'ETI estiment en moyenne à 5,8 sur 10 le risque de cyber-menace pour leur entreprise

La question est centrale. Au-delà de la prise de conscience des menaces et des enjeux liés au risque cyber, la bonne gouvernance de ce risque sera fonction de l'appréciation par les dirigeants des risques que leur entreprise encourt.

Les résultats de l'enquête sont mitigés : le risque est considéré comme très important ou important pour 56% des sondés mais comme modéré ou faible à inexistant pour 44% d'entre eux. Les résultats varient peu selon la taille de l'entreprise.

Parmi ceux qui estiment le risque comme non important, il est jugé comme faible ou inexistant par 23% des dirigeants et modéré pour 21%. Nous voyons plusieurs explications possibles à ces résultats dont l'appréciation reste souvent subjective par manque d'indicateurs pertinents.

- Une sous-estimation de la menace cyber dans sa globalité en négligeant notamment le risque d'un incident cyber du fait d'une négligence humaine interne à l'entreprise. La menace est encore souvent perçue comme extérieure et provenant de zones géographiques trop lointaines pour que les dirigeants estiment que leur entreprise puisse être une cible.
- La mauvaise appréciation de la menace tient aussi souvent à une sous-évaluation de la qualité des

actifs immatériels que possède l'entreprise ou une négligence sur le fait que l'entreprise puisse elle-même servir de vecteur pour nuire à d'autres du fait des interconnexions de son Service d'Information.

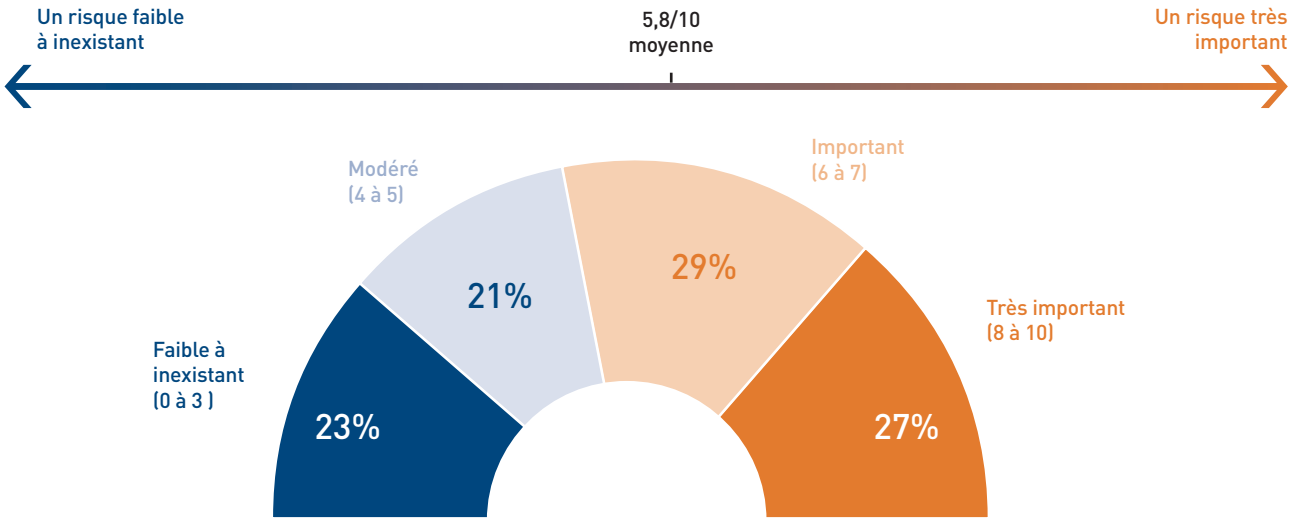
- Une sur-évaluation de la politique de cyber sécurité existante qui amènerait les dirigeants à penser qu'ils sont à l'abri.

A contrario et pour ceux qui estiment la menace comme importante (29%) voire très importante (27%), l'appréciation apparait plus conforme à la réalité des faits.

Parfaitement informés de l'état de la menace et des enjeux, ces dirigeants vont considérer que leur niveau de cyber sécurité et de préparation est insuffisant. Leur entreprise se retrouve de fait être vulnérable et donc exposée à tout moment.

PLUS PRÉCISÉMENT, SUR UNE ÉCHELLE DE 0 À 10, À COMBIEN ESTIMEZ-VOUS LE RISQUE DE CYBER MENACE DANS VOTRE ENTREPRISE ?

0 signifie que le risque est inexistant, 10 que le risque est très important, les notes intermédiaires permettant de nuancer votre jugement.



MOYENNE

5,8/10

DÉTAIL

	%
SECTEUR D'ACTIVITÉ	
Industrie / BTP	**6,4**
Commerce / Services	**5,4**
TAILLE DE L'ENTREPRISE	
Moins de 1000 salariés	**5,9**
1000 salariés et +	**5,6**
CHIFFRE D'AFFAIRES	
De 50 à 99 millions	**6**
100 à 199 millions	**5,4**
Plus de 200 millions	**6**

SEULS

32%

des dirigeants sont tout à fait certains d'être préparés à affronter une attaque cyber

#3

Le jugement des dirigeants sur leur capacité à affronter une crise cyber interpelle : seuls 32% des dirigeants d'ETI considèrent que leur entreprise est tout à fait préparée

Seuls 32% sont tout à fait certains d'être préparés à affronter une attaque cyber. Et parmi ceux qui considèrent que le risque est faible à inexistant, ce ratio monte à 53%.

Plus globalement les résultats ne sont pas sans équivoque car au total 89% des dirigeants interrogés répondent positivement.

Sur les 89% de réponses positives, la proportion est quasiment identique quel que soit le niveau d'appréciation de la menace cyber pour leur entreprise. Aussi, les dirigeants qui jugent le niveau de la menace cyber faible ou inexistant estiment être autant prêts à affronter une attaque cyber que ceux qui évaluent la menace comme très importante.

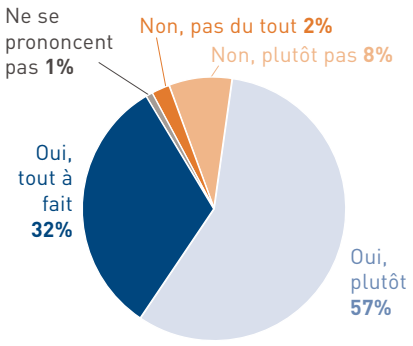
Ce taux de réponse interpelle car les mesures et les moyens à mettre à œuvre pour affronter une cyber attaque suppose un niveau de maturité élevé quant à l'appréhension de ce risque et des investissements à prendre pour y faire face.

Ce niveau de maturité ne peut par définition être au même niveau pour les entreprises exposées ou non exposées selon la vision des dirigeants, ne serait-ce que pour des questions de coûts.

Les retours d'expérience d'entreprises ayant été victimes de sinistres cyber majeurs reflètent une réalité bien différente ; de l'impréparation la plus totale à une préparation négligée ou à repenser sur de nombreux points.

L'optimisme de dirigeants ayant répondu positivement mériterait d'être challengé avec par exemple la réalisation d'exercices de tests en réel.

SELON-VOUS, VOTRE ENTREPRISE EST-ELLE PRÉPARÉE POUR AFFRONTER UNE CYBER-ATTAQUE ?



ENSEMBLE 32%

DÉTAIL

	%
SECTEUR D'ACTIVITÉ	
Industrie / BTP	26
Commerce / Services	38
TAILLE DE L'ENTREPRISE	
Moins de 1000 salariés	30
1000 salariés et +	36
CHIFFRE D'AFFAIRES	
De 50 à 99 millions	24
100 à 199 millions	33
Plus de 200 millions	43
RISQUE CYBER MENACE DANS SON ENTREPRISE	
Faible à inexistant	53
Modéré	28
Important	16
Très important	34

SEULS

3%

des dirigeants envisagent d'embaucher un profil dédié à la cyber sécurité

#4

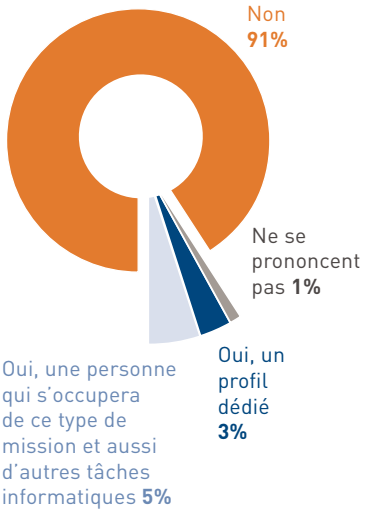
Seuls 3% des dirigeants interrogés envisagent d'embaucher au cours des douze prochains mois un profil dédié à la cyber sécurité ?

NON : 91 %

DÉTAIL

SECTEUR D'ACTIVITÉ	
Industrie / BTP	89
Commerce / Services	91
TAILLE DE L'ENTREPRISE	
Moins de 1000 salariés	91
1000 salariés et +	89
CHIFFRE D'AFFAIRES	
De 50 à 99 millions	93
100 à 199 millions	89
Plus de 200 millions	89
PERCEPTION DU RISQUE DE CYBER MENACE DANS SON ENTREPRISE	
Faible à inexistant	94
Modéré	97
Important	91
Très important	83

DANS LES 12 PROCHAINS MOIS, ENVISAGEZ-VOUS D'EMBAUCHER UNE PERSONNE EN CHARGE DE LA CYBER-SÉCURITÉ DE VOTRE ENTREPRISE ?



Là encore les réponses sont clairement tranchées. Neuf dirigeants sur 10 répondent par la négative.

Ils n'envisagent pas non plus de confier ce sujet à une personne déjà en charge d'autres tâches informatiques.

Les enjeux de cyber sécurité sont relativement récents. Ils impliquent des compétences dédiées qui ne se limitent pas à une vision technique de la sécurité informatique. Les sujets périphériques, tels que les aspects juridiques, organisationnels, humains ou gestion de risque font partie intégrante de la fonction. Et les experts en cyber sécurité sont rares ainsi que les formations adaptées. La pénurie d'experts en sécurité informatique pose de réelles difficultés à la fois pour les sociétés dédiées à ce métier que pour les entreprises en recherche de compétences dédiées.

Si aujourd'hui, certains voient leurs missions étendues aux questions de cyber sécurité, la question est de savoir si l'entreprise va leur permettre d'acquérir les compétences adéquates.

Une entreprise peut disposer d'un excellent juriste en droit des affaires. Sera-t-il pour autant un excellent juriste en droit du travail, droit fiscal ou droit numérique si l'entreprise lui confie ce rôle ?

61%

des dirigeants sont tout à fait certains d'être préparés à affronter une attaque cyber

#5

61% des dirigeants sondés disent que leur entreprise dispose d'assurances couvrant le risque de cyber attaques et ses conséquences financières

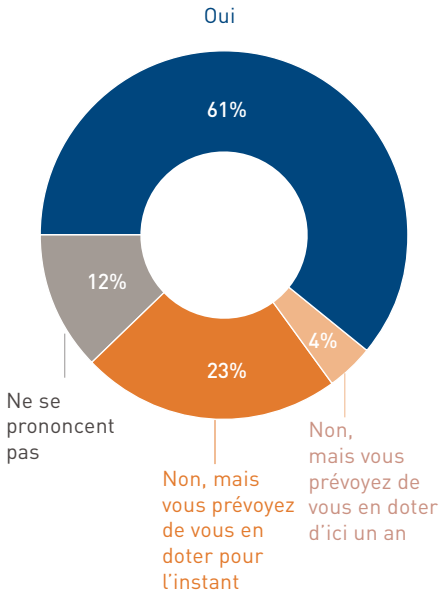
Ce résultat est quelque peu paradoxal : l'assurance dédiée à la couverture des risques cyber est en plein développement, mais selon la Fédération Française des Assureurs le volume de primes collectées en France en 2018 par les assureurs ne s'élève qu'à environ 80 millions d'Euros.

Ce volume de primes très faible souligne un taux d'équipement des entreprises extrêmement bas. La collecte de primes se concentre au niveau des grands groupes qui sont aujourd'hui presque tous assurés. Ce n'est pas encore le cas pour les ETI ou certains annoncent un taux d'équipement en assurance cyber de moins de 10%.

Les dirigeants qui se pensent assurés le sont-ils avec des garanties spécifiques adaptées à leur risque cyber ? Disposent-ils ainsi d'une couverture contribuant à la cyber-résilience de leur entreprise ?

Ces questions nous semblent devoir être vérifiées par les dirigeants d'ETI.

DISPOSEZ-VOUS D'ASSURANCES COUVRANT LE RISQUE DE CYBER-ATTAQUES ET SES CONSÉQUENCES FINANCIÈRES



ENSEMBLE **61%**

DÉTAIL

	%
SECTEUR D'ACTIVITÉ	
Industrie / BTP	**60**
Commerce / Services	**62**
TAILLE DE L'ENTREPRISE	
Moins de 1000 salariés	**55**
1000 salariés et +	**76**
CHIFFRE D'AFFAIRES	
De 50 à 99 millions	**56**
100 à 199 millions	**61**
Plus de 200 millions	**67**
RISQUE CYBER MENACE DANS SON ENTREPRISE	
Faible à inexistant	**62**
Modéré	**69**
Important	**54**
Très important	**61**

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