COMMENT « DÉBLOQUER » LE MARCHÉ DE L'ASSURANCE CYBER EN FRANCE ?

CYBER SECURITY Insights*

les alumni de Télécom ParisTech s'engagent pour la cybersécurité

Par Charles d'AUMALE (1997), François GRATIOLET (1999), Stéphane SOLLAT (2009), François-Xavier VINCENT

SOMMAIRE

Pourquoi ce Livre Blanc ?

Nous avons décidé de nous lancer dans l'analyse des « bloqueurs » de l'assurance cyber en France et dans la structuration de recommandations pour « débloquer » le marché pour plusieurs raisons :

- en tant qu'ingénieurs, nous sommes attachés à la compréhension des problèmes et de leurs résolutions ;
- en tant que spécialistes des technologies de l'information, nous souhaitons que leur utilisation soit la plus large possible tout en maitrisant les risques ;
- en tant que diplômés d'institutions françaises, nous estimons qu'il faut protéger nos actifs et participer au leadership des secteurs français de « la cyber » et de l'assurance.

Pour la réalisation de ce Livre Blanc, nous avons approché un certain nombre d'acteurs reconnus, pour avoir une vision panoramique du sujet et confronter les perspectives : utilisateurs, clubs professionnels, assureurs, experts… Nous avons ainsi recueilli des éléments précieux, sous forme de fiches d'entretien, de réponses à questionnaires, ou d'articles. Beaucoup sont présents dans cet ouvrage ; qu'ils soient tous remerciés.

Avant-Propos

Par Jean-Claude Laroche,
Président du Cercle Cybersécurité, CIGREF

L'assurance du cyber-risque

Un enjeu pour les grandes entreprises

Le développement de l'assurance du cyber-risque répond à un besoin croissant des entreprises. L'actualité nous rappelle, hélas de manière récurrente, que le cyber-risque n'a rien de virtuel et que ses conséquences sur l'activité de l'entreprise et sa réputation, peuvent être dramatiques.

Au cours du séminaire de printemps du CIGREF, le 11 mai 2017 dernier, deux représentants de l'Institut Français des Administrateurs de sociétés ont présenté aux praticiens du numérique des grandes entreprises françaises, le rapport d'un groupe de travail de l'IFA sur le rôle du comité d'audit en matière de cybersécurité, publié en mars 2016. Désormais, pour les administrateurs de sociétés, « les enjeux liés à la cybersécurité deviennent une des priorités des travaux des comités d'audit » au sein des conseils d'administration ! Ce même rapport préconise que le comité d'audit puisse « apprécier le degré de prise en compte des cyber-risques dans le dispositif de gestion des risques ». Pour les entreprises, l'assurance est bien entendu l'un des instruments principaux de ce dispositif.

En octobre 2016, le CIGREF a publié un rapport sur un thème analogue, intitulé « Le cyber-risque dans la gouvernance de l'entreprise : comment et pourquoi en parler en COMEX ». Nous écrivions dans ce rapport que « la gestion du risque cyber a des impacts en termes assuranciels et la question de la couverture du risque cyber est grandissante dans les entreprises. Mais il s'agit d'un risque nouveau, qui ne bénéficie pas encore de définition officielle : comment est pris en compte le risque cyber aujourd'hui dans les assurances ? Quel périmètre couvrent-elles ? Comment sont prises en compte les données personnelles ? » Nous mettions alors principalement en relief que ce thème de l'assurance du cyber-risque pose de nombreuses questions aux entreprises, auxquelles les assureurs doivent apporter des réponses adaptées au contexte de chacune d'elles. Ce thème est inscrit à la feuille de route du Cercle cybersécurité du CIGREF, que je préside.

C'est donc tout naturellement que le CIGREF a accepté de participer à l'étude, conduite par le groupe Cybersécurité de Télécom ParisTech, sur le marché français de l'assurance cyber. Le CIGREF partage son ambition d'améliorer la compréhension de l'assurance cyber en France et de contribuer à son développement pour renforcer la cybersécurité des organisations. Formulons le vœu que le travail important réalisé pour la rédaction de ce livre blanc permette d'éclairer nos entreprises sur ce qu'elles peuvent attendre dans l'avenir en matière d'assurance du cyber-risque.

Démystifier l'assurance cyber

L'assurance cyber est un sujet multiforme, encore assez peu développé, parfois polémique ; et la première problématique consiste justement à définir de quoi il s'agit ! En effet, la compréhension du concept, et de ce qu'il recouvre, peut varier significativement selon les parties prenantes.

Un premier challenge consiste en l'appellation elle-même ; assurance cyber, cyber-assurance, ou autres variantes peuvent dès l'abord susciter une certaine réserve :

- D'une part, avec l'utilisation du terme *cyber*, ô combien à la mode voire galvaudé, mais dont la signification laisse parfois perplexe : est-ce un synonyme d'informatique, d'internet, de dématérialisation, de traitement algorithmique, d'un peu de tout cela ?
- D'autre part, les préjugés ou frilosités pouvant entourer les assurances, liés entre autres au fait qu'une véritable expertise est souvent nécessaire pour souscrire une assurance correspondant à ses besoins et pour en respecter les clauses. Et à cette frilosité des souscripteurs correspond souvent celle des assureurs, pour lesquels il s'agit d'un domaine relativement nouveau, avec donc un historique limité et des besoins d'expertise spécifiques pour bien comprendre les risques assurés.

Ecartons déjà le premier point, en convenant avec la plupart des grands acteurs et experts du domaine que « *la cyber* » renvoie à l'information, son traitement et sa protection, en incluant les personnes, processus, systèmes et technologies y participant.

- Cela inclut donc l'informatique, sans y être limité, et au cœur se trouve l'information, « pétrole » de l'économie moderne : des données (personnelles, des clients, des employés, stratégiques, industrielles…), des savoir-faire, ou encore des procédés ; leur « valeur » étant entre autres déterminé par l'impact potentiel d'une atteinte à leur disponibilité (*puis-je utiliser l'information au moment où j'en ai besoin*), leur intégrité (*l'information est-elle suffisamment fiable pour mon usage*) et leur confidentialité (*l'information n'est-elle communiquée qu'à ceux qui en ont un besoin légitime*).
- Avec cette complexité supplémentaire qu'une atteinte à l'information, outre des conséquences économiques, légales, ou d'image, peut avoir des répercussions très concrètes dans le monde physique – par exemple sur les systèmes industriels, les implants médicaux, ou encore les véhicules connectés.

Seconde problématique, ce qui est couvert – ou non. Car une assurance permet de se protéger, dans un cadre contractualisé, contre des conséquences dommageables voire catastrophiques ; et on voit bien du bref exposé ci-dessus que les conséquences d'une atteinte à l'information peuvent être de natures très diverses, ainsi d'ailleurs que les causes (accidentelles, délibérées, naturelles…) ayant été à l'origine de cette atteinte.

Dans l'idéal, la souscription d'une assurance cyber sera le déclencheur d'un cercle vertueux d'amélioration continue de la sécurité de l'information : l'entreprise souscriptrice identifie l'information qui a le plus de valeur pour elle, ce qui peut la menacer, les failles qui pourraient être exploitées pour ce faire, et met en place une approche par les risques de la sécurité de son information. L'assurance cyber s'insère ainsi dans l'écosystème de gestion de ses risques cyber, les primes versées constituant un véritable investissement, dans le cadre d'une relation de confiance avec l'assureur.

A l'opposé, souscrire une assurance cyber sans compréhension des enjeux ni avoir mené une vraie réflexion stratégique peut conduire à un laisser-aller dommageable en matière de cybersécurité : on pense avoir transféré tous ses risques cyber à l'assureur, on peut donc se dispenser d'investir dans des mesures de sécurité adaptées ![1]

Alors qu'une simple comparaison – certes un peu réductrice mais fondamentalement correcte – avec une assurance plus classique fait bien comprendre l'inanité de cette approche : souscrire une assurance incendie ne dispense pas de mettre en place des mesures de prévention ou des systèmes de détection d'incendie, ni d'en vérifier régulièrement la pertinence, faute de quoi l'assureur pourra légitimement refuser de couvrir, en tout ou partie, un sinistre.

Dernier écueil : le marché est encore peu mature, particulièrement en Europe[2], et la plupart des assureurs, quoiqu'intéressés à développer une offre d'assurance cyber, manquent encore de recul, de visibilité et d'expertise dans ce domaine, comme rappelé en début de cette introduction. Ce qui fait que les offres ne sont pas nécessairement bien adaptées aux besoins de tous les types d'entreprises, ou parfois vues comme insuffisamment transparentes en termes de couverture ou de tarification.

Dans ce tableau, le régulateur a un rôle à jouer mais est dans une position inconfortable, eût égard aux éléments potentiellement conflictuels rappelés ci-dessus, et souvent aux mêmes manques d'expertise que ceux identifiés chez les assureurs comme chez leurs clients.

La volonté politique pourrait néanmoins faire la différence : dans le rapport[3] sur l'assurance cyber publié en 2015, le gouvernement UK annonce vouloir faire de Londres une place mondiale pour l'assurance cyber…

Le présent Livre Blanc s'attache ainsi non seulement à expliciter les « bloqueurs » sous-jacents à l'exposé précédent, mais aussi à présenter un certain nombre de recommandations concrètes pour débloquer l'assurance cyber, s'adressant à toutes les parties prenantes : les professionnels de l'assurance, les clients, et les pouvoirs publics.

1/ L'exemple récent de l'attaque WannaCry (mai 2017) montre l'importance de respecter les règles d'hygiène informatique tout en complétant les actions techniques et organisationnelles par des polices d'assurance cyber adaptées.
2/ Les estimations du marché mondial de l'assurance cyber en 2016 sont de 2 à 3 Md$. On peut estimer 80% du marché aux US, principalement sur les enjeux de data breach et de privacy (notamment à cause des lois des différentes états sur le sujet) ; 10% du marché au UK, en particulier à travers les Lloyds ; 10% dans le reste du monde (principalement l'Europe)
3/ https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

Perspective économique

Quelles sont les conditions d'émergence de l'assurance cyber ?

Par Ali JAGHDAM,

Enseignant-chercheur à l'Ecole de Management Léonard de Vinci ;
inspiré de l'ouvrage du même nom

Le constat

L'évolution extrêmement rapide des cyber-risques ces dernières décennies en volume mais surtout vers un type d'attaques plus organisées et ciblées (80% des cyber-attaques ont une motivation criminelle causant une perte de plus de 3 trillions de dollars !), ouvre un nouveau chapitre dans la politique des assurances vis-à-vis des risques. Cette évolution n'a pas pu être rattrapée par le marché de cybersécurité (faible niveau d'investissement…) et encore moins par celui de l'assurance cyber (offre inadaptée…) qui reste « timide » et peu innovant face aux attentes des entreprises.

En effet, l'assurance s'est adaptée aux nouveaux risques informatiques en deux temps. Dans un premier temps, avec l'apparition des premières attaques virales, les assureurs ont proposé à leurs assurés des extensions des polices déjà existantes. La révision des primes correspondait aux frais d'audit et d'inspection courante de la mise en place d'anti-virus et des firewalls. Or, la gravité des sinistres a pris de l'ampleur et de nouveaux types d'attaques plus organisées sont apparus. Les assureurs se sont montrés plus prudents, et plusieurs exclusions ont commencés à figurer sur ces polices. Dans un second temps, et depuis le début des années 2000, de nouvelles polices spécifiques à la cybercriminalité ont été proposées par quelques assureurs anglo-saxons (AIG, Chubb, Lloyd's, ACE, XL…) et récemment par des assureurs européens (ALLIANZ, AXA…) sous des conditions techniques et économiques plus ou moins acceptables. L'analyse de quelques contrats montre que ceux-ci sont plafonnés et que la prime est souvent indexée sur l'effort d'autoprotection des assurés.

Les risques cyber font encore plus peur aux assureurs qu'aux assurés !

L'un des fondements de la réalisation d'un transfert du risque d'un agent économique sur un autre (i.e. d'un contrat d'assurance) est, d'une part, la crainte du premier quant à la réalisation d'un certain aléa contre lequel il veut être protégé (agent risquophobe). Et, d'autre part, l'acceptation de couvrir ce risque par le deuxième moyennant une mutualisation qui le rend neutre à ce risque. Cette inégalité dans les degrés d'aversion au risque, dans ce sens, est l'essence même d'un marché d'assurance.

Il apparaît que cette inégalité n'est pas dans le bon sens pour ce qui est des cyber-risques et que ceux-ci font encore plus peur aux assureurs qu'aux assurés !

Si actuariellement l'assurabilité d'un risque dépend d'un certain nombre de caractéristiques objectives qui devaient être toutes réunies pour que l'assureur puisse appliquer les techniques usuelles de tarification, les cyber-risques se trouvent aux limites du champ de l'assurable et échappent complètement aux modèles les plus sophistiqués de tarification.

En effet, d'une part, en plus du caractère relativement rare et catastrophique en termes du niveau des pertes des cyber-crimes, d'ailleurs, tout comme les

catastrophes naturelles (sauf que ceux-ci sont maitrisées par régionalisation sur le marché de l'assurance), il vient s'ajouter un troisième facteur : celui de l'interdépendance des cyber-risques (i.e. entre les assurés potentiels) et ce à l'échelle mondiale (les cyber-risques n'ont pas de limites géographiques). D'autre part, les assureurs n'ont pas de recul suffisant ni d'historique suffisants sur les sinistres et les impacts financiers du fait de la frilosité des entreprises à communiquer sur l'impact des cyber-attaques subies, et de l'évolution permanente et rapide des nouvelles technologies de l'information et de communications et donc des cyber-risques aussi.

Il est donc clair que ni théoriciens ni praticiens ne sont satisfaits de nos capacités actuelles à mesurer d'une manière crédible l'effet économique des actes de malveillance commis sur les réseaux d'information. Il n'existe, jusque-là, aucune méthodologie standard à cet effet et les estimations du coût de la cybercriminalité pour les entreprises (basées sur des enquêtes ou sur des méthodes plus objectives) sont, le moins que l'on puisse dire, « spéculatives ».

Les remèdes à l'émergence d'un marché stable de l'assurance cyber

Le déblocage du marché de l'assurance cyber revient en grande partie à l'inversion du sens de l'inégalité de l'aversion aux cyber-risques entre assureurs et assurés.

Augmenter l'aversion aux cyber-risques des entreprises

Selon l'approche économique du transfert du risque, la condition principale d'assurabilité se réduit à l'acceptation par l'assuré du prix du transfert proposée par son assureur. Autrement dit, comment rendre « raisonnable » aux yeux des assurés la prime d'assurance toujours jugée trop élevée par ces derniers par maque de conscience de la gravité des conséquences économiques des cyber-risques ?

La modification de la perception par les entreprises des cyber-risques encourus passe principalement par leur faire prendre conscience des conséquences économiques d'une absence de couverture contre ce type de risques. Il faut sensibiliser les entreprises à la cybercriminalité et médiatiser les sinistres. Le partage et la divulgation de l'information sur l'état de sécurité, les incidents subis, les montants des pertes... augmentent remarquablement le degré d'aversion au risque. Les entreprises peuvent bénéficier d'un « effet direct » de la divulgation d''information sur leur demande d'assurance cyber et d'un « effet stratégique » sur les prix. Des centres de collecte d'informations, à l'instar des CERT (Computer Emergency Response Team), doivent être mis en place partout dans le monde. Cela permet de réduire les incertitudes et de mieux faire connaître les cyber-risques par tous les acteurs économiques. Quant aux pouvoirs publics, ils sont les mieux placés pour obliger les entreprises à communiquer et à partager leurs expériences de sécurité. Ceci pourrait changer la perception générale de la cybercriminalité par le monde professionnel.

Diminuer l'aversion aux cyber-risques des assureurs

Pour pouvoir faire absorber ce type de risque par les bilans des assureurs, il faut contourner les obstacles actuariels confrontés par ces derniers dans leur offre d'assurance cyber. Les assureurs doivent être rassurés à leur tour quant à leurs engagements financiers.

Deux solutions pourraient être envisagées : développer le marché de la réassurance et se rapprocher du marché de la cybersécurité et des pouvoirs publics.

Le marché de la réassurance est incontournable pour ce type de risques. En septembre 2016, le réassureur suisse Swiss Re, a mis en service des solutions adaptées aux cyber-risques et les principaux réassureurs de la place devraient se positionner sur des solutions préventives, avec des solutions de formations spécifiques et l'accompagnement à des « stress tests » réguliers.

Par ailleurs, un rapprochement avec le marché de cybersécurité et les pouvoirs publics pourrait aboutir à une solution par :

- (a) La réduction de la probabilité d'attaque : (qui ne dépend que de la volonté de nuire des cybercriminels) par le renforcement du référentiel légal international pour contourner l'existence des « paradis numériques » permettent aux criminels d'héberger des serveurs, diffuser des contenus illicites ou réaliser des actions illicites en toute impunité.

- (b) La réduction de la probabilité de réussite de l'attaque par, d'une part, la création d'un environnement de confiance envers le marché de cybersécurité (problème du lemons market) par la certification et le contrôle permanant de la qualité de service, et d'autre part, par l'augmentation du niveau de l'investissement des entreprises en cybersécurité en renforçant les normes de sécurité au sein des entreprises au gré des évolutions technologique.

Un contrat package : « cyber-assucurité »

Le risque moral est l'un des principaux obstacles à offrir un contrat adéquat d'assurance cyber. En effet, les entreprises doivent savoir que la couverture assurantielle vient compléter tout processus de sécurité et non pas s'y substituer. L'effort de sécurité doit être toujours à son optimum. Ainsi, donner aux assureurs la possibilité d'intégrer le marché de cybersécurité en offrant un service de cybersécurité tout comme les sociétés d'outsourcing (sans pour autant glisser dans l'ingérence), semble être un facteur rassurant qui contourne fortement l'aléa moral et réduit l'aversion au risque des assureurs.

Cela permet de proposer un contrat à deux volets aux assurés : un contrat d'assurance couvrant les dommages subis, et un accompagnement sur mesure en ingénierie. De tels produits deux en un que l'on peut appeler « cyber-assucurité » pourraient donc être la clé de voute pour les assureurs, et représenter un levier de croissance des produits d'assurance cyber.

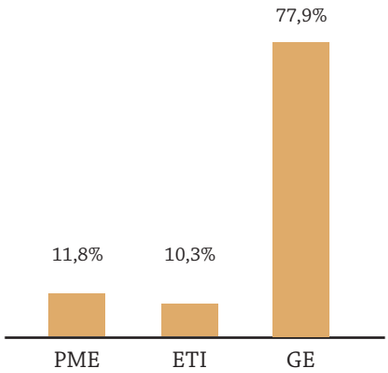
Résultats commentés des enquêtes menées auprès du CESIN[1] et du CIGREF[2]

Début 2017, des enquêtes ont été menées auprès du CESIN et du CIGREF pour comprendre les enjeux et les perceptions de l'assurance cyber auprès de leurs adhérents. Nous leur avons posé les mêmes questions. Un de nos objectifs étant de comprendre les éventuelles divergences de vues entre RSSI et DSI. Néanmoins, compte tenu du nombre de réponses, nos analyses se basent principalement sur les résultats du CESIN[3].

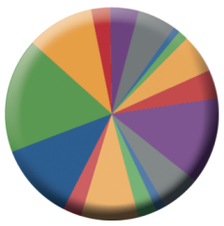
Analyse des chiffres du CESIN

Profils des réponses
Les graphes ci-dessous montrent les types d'entreprises représentées et les profils des répondants.

Profils des entreprises

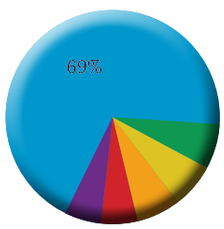


Profils des entreprises



- service financier 18%
- assurance 17,6%
- industrie 10,3%
- service 2,9%
- technologie 4,4%
- utilities 5,9%
- éducation 1%
- conseil 1,5%
- services aux entreprises 5,9%
- santé 4,4 %
- distribution 13,2%
- média 5,9%
- télécomunication 1,5%
- transport 2,9%
- administratif 8,8%
- collectivités locales 2,9 %

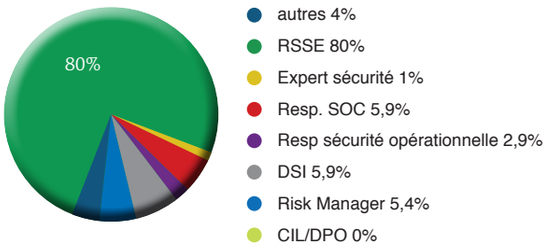
Chiffres d'affaires des entreprises



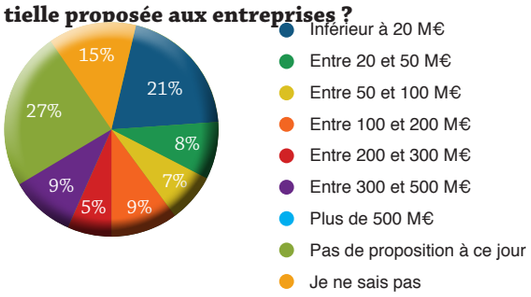
- plus de 1Mds €
- de 150 M€ à 1 Mds €
- de 150 M€ à 1 Mds €
- de 50 M€ à 150 M €
- de 5 à 50 M €
- moins de 5 M €

1/ Club des Experts de la Sécurité de l'Information et du Numérique
2/ www.cigref.fr ; association qui regroupe les DSI de 140 grandes entreprises
3/ 68 réponses côté CESIN et une vingtaine côté CIGREF

Profils fonctions



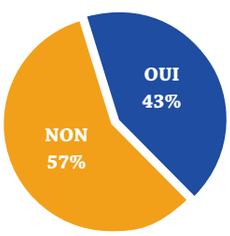
Montant maximal de la couverture assurantielle proposée aux entreprises ?



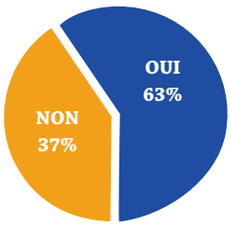
Typologie des souscripteurs d'assurance cyber

A travers les réponses du CESIN, nous comprenons qu'il existe un grand clivage dans les réponses et l'appréciation du sujet dans les entreprises. En effet, 27,9% déclarent avoir souscrit une police d'assurance spécialisée cyber et ce, sans faire usage d'une option dans une assurance classique. Ce chiffre est à mettre en contraste des 32,4% « de non mise en étude du sujet » pour 2017, en rappelant que les réponses sont issues à 77,9% de grandes entreprises.
Malgré une majorité de non-souscription à une couverture cyber (57%), l'avenir demeure encourageant avec les 20,6% de « non, mais à l'étude » qui devraient porter la souscription à 63% de police d'assurance cyber et faire reculer les « non » à 37%.

Avez-vous souscrit une assurance cyber ?
Avril 2017



Projection à terme



Oui, produit dédié cyber	**27,9%**
Oui, en option d'une assurance	**7,4%**
Une souscription prévue dans l'année à venir	**7,4%**
Non, mais sujet à l'étude	**20,6%**
Non, sujet n'est pas à l'étude	**32,4%**
Je ne sais pas	**0,44%**

Dans cette perspective de croissance des souscriptions d'assurance cyber, les entreprises déclarent vouloir couvrir en priorité le risque de « Pénalités contractuelles ou réglementaires suite à une attaque cyber ».

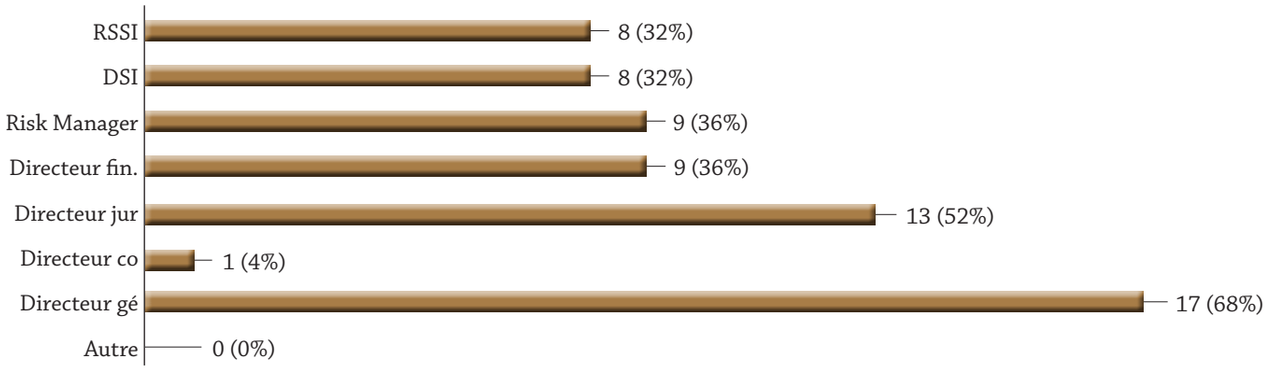
56% : Pénalités contractuelles ou réglementaires, suite à une attaque cyber
40% : Impacts sur les tierces parties
40% : Frais d'expertise technique pour retour à la normale, suite à une attaque cyber
40% : Perte d'exploitation, suite à une interruption business liée à une attaque de Déni de Service
36% : Frais de communication et gestion de crise, suite à une perte de réputation lors d'une attaque
36% : Frais de re médiation, suite à un ransomware
16% : Frais de notification, suite à une violation de données à caractère personnel
16% : Frais de monitoring (comptes bancaires, usurpation d'identité…), suite à une violation de données à caractère personnel

La question de la gouvernance de l'assurance cyber

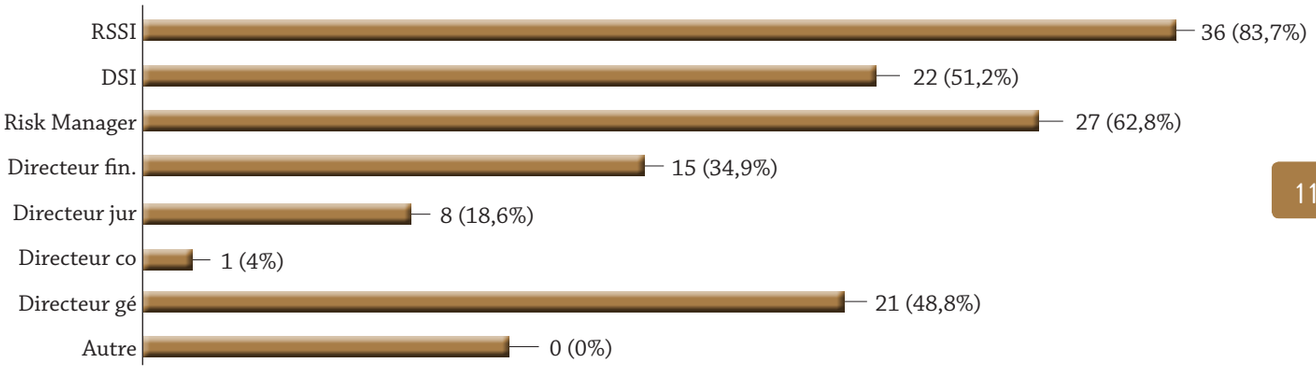
Nous avons noté des chiffres mettant en lumière une gouvernance contradictoire quant à la souscription d'une police d'assurance cyber :

- la Direction Générale est le principal décideur (à 68%) mais avec une implication qui apparaît limitée (48,8%) ;
- si l'implication des RSSI est très forte (83,7%), celle des Risk Managers (62,8%) devrait être au moins au même niveau – d'ailleurs les résultats de l'enquête auprès du CIGREF montrent une implication comparable de ces deux fonctions (environ 85%).

Si une telle assurance cyber devait être souscrite, selon vous, quelle(s) fonction(s) prendrai(en)t la décision ? (Plusieurs réponses possibles)



Quelle(s) fonction(s) est impliquée dans la décision de souscrire une assurance cyber ? (Plusieurs réponses possibles)



Les freins à l'adoption de l'assurance cyber

L'enquête fait un éclairage sur la nature des « bloqueurs », contrariant la généralisation des contrats d'assurance cyber dans les entreprises.

Les assureurs peinent à « modéliser et qualifier les risques cyber par secteur d'activité » (64,7% de sondés), ce qui ne facilite pas la mise en place de modèles statistiques comparatifs (51,5% des sondés) et rend « les offres insuffisamment lisibles actuellement » (55,9% de sondés).

Les entreprises pointent « la difficulté à modéliser et à quantifier les risques en interne » (58,8% des sondés), ainsi que « des offres trop coûteuses » et « des solutions non adaptées aux entreprises ».

La « multiplicité des standards sur la question de la cybersécurité » et le « manque de statistiques publiques d'incidents cyber » ne facilitent pas le partage de référentiel commun du risque entre les compagnies d'assurances et les entreprises. En effet, les risques assurantiels et risques Sécurité du SI ne recouvrent pas les mêmes périmètres dans le cas d'une attaque cyber, au risque d'une mécompréhension de ce qui est réellement couvert par l'assurance cyber.

Les évaluations préalables des systèmes contre le risque cyber restent très majoritairement basées sur du déclaratif (questionnaires et/ou entretiens) : entretien avec l'assureur (51,5% de sondés), questionnaire détaillé (administré par un spécialiste interne ou externe : 41,9%) ou questionnaire simple (pouvant être rempli par un non spécialiste 16,3%).

En revanche, seulement 4,2% des sondés déclarent avoir eu « un audit sur site de 1 ou 2 jours d'un partenaire expert sécurité de son assureur ». Il est à noter que 23% de sondés n'ont reçu aucune proposition d'audit à la souscription de leur assurance cyber.

Une **absence d'exigence inter-entreprises de police d'assurance cyber :**

- 80% des entreprises ne proposent pas à leurs clients des attestations de police d'assurance cyber. 8% proposent un engagement fort basé sur un SLA ou de responsabilité pour tiers.
- 56% des entreprises ne demandent aucune attestation d'assurance cyber. 12% n'en n'ont aucune idée. 28% compensent par une exigence de SLA avec pénalités. Seulement 4% des sondés exigent du fournisseur informatique/données une attestation d'assurance cyber.

Un **manque de mobilisation pour associer police d'assurance cyber**

et prestations d'expertise cyber : 39,5% des offres ne prévoient aucune prestation d'expertise ; quant aux autres, 55,8% des sondés n'ont jamais reçu de propositions concrètes d'expertise.
Seulement 4,7% ont bénéficié de prestations en amont à la souscription d'une assurance cyber.

Les référentiels
L'ISO 2700x est plébiscité (50% de sondés) en laissant les référentiels du NIST et de l'ETSI ISI à 11,8% chacun. Mais il est à noter que les professionnels expriment une relative insatisfaction dans les référentiels cités, car 38,2% estiment qu'il faudrait « une combinaison de standards » et d'autres, qu'il ne faudrait au contraire « aucun standard » 35,3%.

Les facteurs principaux d'adoption[4] de l'assurance cyber

- A 70,6% : la croissance des attaques va enclencher des souscriptions
- A 58,8% : la prise de conscience des dirigeants et de leurs responsabilités
- A 52,9% : les règlements en vigueur ou à venir
- A 47,1% : la valeur de l'information à protéger
- A 32,4% : la connaissance du coût moyen des attaques cyber
- A 25,0% : l'exigence des clients et partenaires

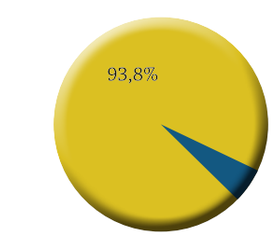
Résultats croisés du CESIN et du CIGREF

L'ensemble des commentaires, des analyses et finalement des recommandations des professionnels des deux organisations convergent, même si la fonction RSSI au CESIN (80%) a une plus grande représentation qu'au CIGREF (50%). A l'inverse, avec 18,8%, le Risk Manager est mieux représenté dans les réponses du CIGREF, contre 4,4% au CESIN. Plusieurs recommandations ont retenu notre attention, soulignant le rapprochement nécessaire entre les métiers de la cyber sécurité, du Risk Management, des autres Directions métiers et de la Direction Générale et ce, pour une meilleure efficacité et clarté de l'assurance cyber :

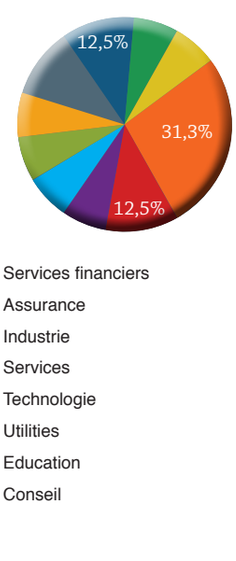
- « Que les RSSI comprennent que l'assurance cyber est un outil du portfolio de défense » ;
- « Besoin d'une visibilité sur le ROI d'une assurance et sur les coût factuels et connues d'une cyberattaque » ;
- « Il faudrait disposer d'analyse présentant pour la France les coûts des cyberattaques afin que les DG voient l'intérêt d'une assurance au regard des impacts financiers ».

Données du CIGREF

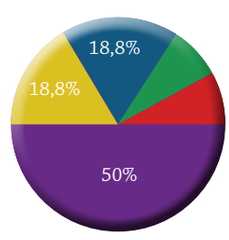
Profils des entreprises



Répartitions des activités



Profils des répondants



4/ Nous rappelons que les enquêtes ont été menées avant l'attaque WannaCry de mai 2017

Témoignages d'experts du marché

Quelques questions à Gérard GAUDIN, fondateur et Président du club R2GS[1] et de l'ISI[2] à l'ETSI

Comment définissez-vous le risque cyber ?

C'est le risque d'atteinte au système d'information de l'entreprise ou lié à l'usage des réseaux sociaux, du fait de la malveillance et de l'erreur ou de la négligence.

Les membres de R2GS ont participé à l'enquête Télécom ParisTech. Pouvez-vous commenter les principales tendances ?

Les principales tendances constatées peuvent être résumées de la façon suivante :

- **Maturité encore faible de la demande,**
- **Couverture des pertes d'exploitation recherchée en priorité,**
- Croissance du risque cyber et sanctions financières liées aux nouvelles réglementations vues comme une double incitation à examiner ce type d'assurance.

Quelle(s) méthode(s) vous paraissent les plus appropriées pour modéliser, quantifier et comptabiliser le risque cyber ? Quelle méthode(s) utilisez-vous dans vos activités ou travaux ?

La méthode la plus appropriée, qui est celle que j'ai mise au point pour le compte de grandes entreprises et organisations en France et en Europe, est la suivante :

- Élaboration d'un Top 10 des risques cyber par métier pour un secteur d'activité économique donné (par exemple, 15 métiers dans le secteur bancaire et financier),
- Chaque type de risque du Top 10 est défini comme la combinaison de la probabilité ou fréquence d'occurrence de l'incident de sécurité et de la sensibilité de la cible (type DIC-Disponibilité Intégrité Confidentialité et niveau et type d'impact).

La composante « fréquence » peut être évaluée sur la base du standard ETSI ISI-001 et de ses 98 indicateurs, auxquels sont associés des chiffres statistiques d'état de l'art.

Selon vous, quels sont les principaux freins actuels à l'achat d'une assurance cyber ? Quel levier principal voyez-vous pour « débloquer » le marché ?

Selon moi, les principaux freins actuels sont les suivants :

- **Séparation entre les entités Risques opérationnels et RSSI dans les entreprises,**
- **Modélisation des risques cyber par secteur d'activité économique encore largement insuffisante voire inexistante,**
- Chiffres sur les incidents absents, partiels ou insuffisamment partagés.

Le levier principal pour débloquer cette situation est l'élaboration de modèles de risques cyber avec des chiffres associés.

1/ Club de Réflexion et de Recherche en Gestion opérationnelle de la Sécurité
2/ Information Security Indicators

Quelques questions à Alain BOUILLE, fondateur et Président du CESIN

Les membres du CESIN ont participé à l'enquête Télécom ParisTech. Pouvez-vous commenter les résultats et les principales tendances ?
Cette enquête est importante pour les professionnels de la SSI car l'offre de couverture assurantielle rentre pleinement dans les solutions de gestion des risques avec la diminution du risque par des mesures de sécurité, l'acceptation du risque ou à l'inverse leur suppression en évitant la situation à risque. En revanche les offres existantes depuis de nombreuses années de couverture de la perte d'exploitation ou de la responsabilité civile sont insuffisantes par rapport aux attaques cyber que subissent aujourd'hui les entreprises.
La réflexion sur la couverture des risques cyber par des assurances prend une place importante dans les réflexions des dirigeants d'entreprise. Le RSSI se trouve impliqué dans la réflexion ainsi que la direction juridique et le risk-manager lorsqu'il existe.

Quels sont les principaux risques cyber que les membres du CESIN assurent-ils ou cherchent à assurer ?
Au vu de l'enquête nos membres ont déclaré à 56% que le principal risque qu'ils voulaient couvrir était le coût des pénalités contractuelles ou réglementaires, suite à une attaque cyber, en particulier si l'attaque a pu concerner des données personnelles. Ensuite à égalité, ils souhaitent couvrir les pertes d'exploitation, les frais d'expertises, et les impacts sur les tierces parties.

Selon vous, quels sont les freins actuels à l'achat d'une assurance cyber ?
Les offres sont aujourd'hui insuffisamment lisibles. On a pu constater que la compréhension du risque par les assureurs et par les RSSI ne recouvre pas la même chose. Ce n'est pas étonnant car les métiers sont différents, mais cela rend le dialogue difficile et entraine une crainte de se retrouver dans une situation où on se retrouverait non couvert malgré la souscription de l'assurance en raison d'une interprétation différente de l'attaque au plan technique.

Il y a actuellement des difficultés à modéliser et quantifier les risques cyber en interne et par les assureurs. Les entreprises trouvent les offres trop coûteuses sans doute par un manque de chiffres statistiques publics d'incidents cyber et des coûts engendrés.

Quels conseils pratiques donneriez-vous aux fournisseurs de solutions d'assurance cyber ?
Il faut avant tout un référentiel de définitions communes aux deux métiers avec des critères précis d'interprétations, même si ce référentiel devra être actualisé au fur et à mesure de l'avancée des technologies et des menaces cyber. Comment assurer des environnements que nous-mêmes sommes en train de découvrir comme le *cloud* ou les IoT.

Il faut que l'offre soit lisible à la fois pour le dirigeant d'entreprise, pour les services juridiques et pour les RSSI. Comme nous l'avons indiqué précédemment la définition d'une cyberattaque est très complexe et beaucoup d'entreprises craignent de tomber sous le cas d'une exclusion de la couverture contractuelle (stéréotype des petites lignes qui font qu'on se retrouve dans un cas non couvert).

Quelques questions à Laurent HESLAULT, Symantec, Directeur EMEA des stratégies de cybersécurité

Pouvez-vous nous dire quelques mots sur Symantec et l'assurance cyber ? Quelles solutions proposez-vous à vos clients ?
Compte tenu de leur complémentarité, la convergence des solutions de sécurité et d'assurance nous a très tôt paru inéluctable. Il y a trois ans, Symantec a créé la structure dédiée « Cyber-Insurance Group ». Sa mission est d'une part, d'adresser les besoins des assureurs et réassureurs qui recherchent des outils de support spécifiques dans la compréhension des cyber-risques, notamment sur les aspects *Pricing, Underwriting et Cat Modelling*, et d'autre part la création de partenariats actifs pour proposer une meilleure protection globale à nos clients respectifs.

Selon vous, quels sont les principaux freins et leviers pour accélérer le marché de l'assurance cyber ?
Nous assistons à la rencontre de mondes très complexes (dont l'un d'ailleurs très règlementé). Chacun doit faire un pas vers l'autre pour collaborer à l'émergence de produits qui répondent réellement aux attentes des clients. Pour avancer rapidement et de manière pertinente, un grand nombre d'experts du monde de l'assurance ont été intégrés dans l'équipe Symantec Cyber-Insurance Group, au contact de nos experts en cybersécurité. Beaucoup de questions mais surtout de nombreuses idées n'ont pas tardé à émerger comme notamment une vision simplifiée des cyber-attaques, une définition plus accessible des cyber-risques, de leurs impacts et des solutions de réduction, combinée à une clarification des couvertures ou indemnisations. Nous avons d'ailleurs pu montrer à travers une étude réalisée aux USA que la plupart des « cyber-questions » posées lors de la phase amont par les assureurs sont considérées par les DSI et RSSI comme « absurdes et de peu de valeur ». Une vraie collaboration à long terme est la clef.

Quels conseils pratiques donnez-vous aux souscripteurs d'assurance cyber ?
La cybersécurité est un monde où le bon sens joue un rôle important. Cependant la partie technique peut s'avérer rapidement très complexe. Un bon niveau d'information est donc nécessaire pour une évaluation efficace et néanmoins pertinente de la situation, dans un environnement en bouleversement permanent. Une gestion fine, et mise à jour fréquemment, des cyber-risques pesant sur l'organisation est fondamentale. A la cyber dépendance, nous devons opposer la cyber résilience, qui elle-même s'appuie sur l'humain, l'organisationnel, la technologie et l'assurance.

Quelques questions à François BEAUME, AMRAE, Président commission Systèmes d'Information

Pouvez-vous nous présenter l'AMRAE ? Quels sont les travaux conduits par l'AMRAE sur les risques cyber et l'assurance ?
L'Association pour le Management des Risques et des Assurances de l'Entreprise rassemble plus de 1000 membres appartenant à 750 entreprises françaises publiques et privées. L'association a notamment pour objectifs de développer la « culture » du Management des Risques dans les organisations et d'aider ses membres dans leurs relations avec les acteurs du monde de l'assurance et les pouvoirs publics. Elle les conseille dans l'appréciation des risques, dans la maîtrise de leurs financements et leurs dépenses d'assurance. Sa filiale AMRAE Formation, pour répondre aux besoins de formation professionnelle de ses adhérents ou de ceux qui légitimement s'adressent à elle, dispense des formations diplômantes, certifiantes et qualifiantes de haut niveau. L'AMRAE, de par sa commission Systèmes d'Information, travaille sur les différents aspects des risques Cyber :
- Identification et évaluation du risque
- Prévention et réduction
- Financement
- Gestion de crise et de sinistres
- Retours d'expérience

Ces travaux se concrétisent notamment par des publications telles que :
- Livre blanc « La maîtrise du risque Cyber sur l'ensemble de la chaîne de valeur et son transfert vers l'assurer » (IRT System X)
- Livre collection Maîtrise des risques : RM et RSSI en partenariat avec le CLUSIF
- Livre collection Dialoguer : La gestion du Risque Numérique dans l'entreprise
- Cahier technique « Comment identifier, évaluer, traiter et financer les risques SI ou Cyber » en partenariat avec le CESIN.

Comment définissez-vous le risque cyber ? Quelles sont les méthodes actuelles permettant de modéliser et quantifier le risque cyber ?
Par risque cyber on entend tout ce qui touche à l'atteinte, la violation ou la perte de données, mais également les intrusions de réseau ou encore la détérioration d'actifs immatériels sans atteinte au système d'information et/ou les conséquences d'une atteinte au système d'information. L'identification de ce risque passe par un échange avec les fonctions concernées par sa gestion (SI, juridique, RH, communication…) ainsi qu'avec les directions stratégie et métier pour appréhender toutes les dimensions.

Selon vous, quels sont les principaux risques cyber que les Risk Managers assurent-ils ou cherchent à assurer ?
Les événements ou faits générateurs qui vont être assurés sont divers par nature :
- Dommages matériels (incendie, dégât des eaux…) accidentels ou malveillants
- Dommages immatériels (virus, cryptolockers, attaques ciblées, erreurs humaines, cyber fraude, fraude…).

avec une couverture :
- Des dommages causés aux tiers
- Des dommages subis par l'entreprise assurée y compris le volet pertes d'exploitation et frais de notification.

En outre ces polices offrent souvent un volet « service » axé sur une assistance à la gestion de crise dans toutes ses dimensions (juridique, IT, communication…).

Comment voyez-vous le marché de l'assurance cyber et son évolution ?
Le marché Cyber, est majoritairement développé en Amérique du nord, et commence seulement en Europe. Le marché Européen est cependant en plein expansion depuis quelques années. Cette expansion s'accélère du fait des évolutions réglementaires récentes (loi de programmation militaire…) ou à venir (RGPD…) et de la montée des périls cyber (*WannaCry* ou autre).

Les capacités disponibles augmentent et les offres se sophistiquent.

A ce jour environ la moitié des assureurs Européens n'offre pas de garantie Cyber et pourrait dans le futur élargir leurs offres sur cette branche et faire évoluer les capacités et les offres.

Quelle est selon vous la gouvernance idéale de ce risque ? Qui décide sur les sujets d'assurance cyber ?
Toutes les entreprises ont aujourd'hui une stratégique d'expansion s'appuyant sur le numérique. Des nouveaux risques et dépendances naissent de ces opportunités. Le risque cyber n'est plus un risque technique mais bien un risque d'entreprise. Une gouvernance du risque cyber doit être mise en place pour permettre au management d'apprécier l'exposition pour son entreprise et de prendre les décisions nécessaires dans le cadre d'une gestion globale des risques. La qualité de gestion du risque cyber contribuera à la valorisation financière de l'entreprise.

Quelques questions à Christian REBER Boston Consulting Group, Partner & Managing Director

BCG

Comment voyez-vous le marché de l'assurance cyber ? et celui de la réassurance cyber ?
Le marché de l'assurance cyber n'est qu'au tout début de son développement. La demande pour des polices reste faible, notamment en Europe, et ceci malgré un nombre croissant d'acteurs – compagnies, secteur public – se rendant compte des menaces de la cybercriminalité et des possibilités de pannes et de failles de leurs systèmes informatiques. Les cas de « Hacking » des dernières années ont fait réaliser à tous les intervenants les conséquences potentiellement dramatiques : des coûts très importants de remise en service, de communication et de dédommagement des clients, une réputation endommagée et une perte de confiance des clients, avec un impact souvent important sur la capitalisation boursière.

Du côté du secteur de l'assurance, les obstacles pour le développement consistent surtout en la difficulté de mettre un prix sur des risques sur lesquelles il n'y a que peu de données historiques, et dont on ne connaît pas l'étendu potentiel des dommages. Aujourd'hui, les couvertures proposées par les assureurs sont souvent insuffisantes, et les couvertures plus importantes seraient trop chères.

Ceci dit, le marché voit connait une croissance importante et des développements importants, d'une part avec pour la capacité des assureurs de mieux « comprendre » et de mettre à disposition des couvertures plus importantes, et d'autre part pour avec une la demande qui augmente - la cybercriminalité arrive toujours sur la première place des risques que craignent les entreprises du secteur privé.

Quelles sont les différentes stratégies des principaux acteurs de l'assurance en matière de cyber ?
Les assureurs tentent d'avancer le marché en se créant une base de connaissance et d'expertise à la fois qualitative et quantitative. Ils travaillent souvent en partenariat avec des acteurs du secteur technologique pour mettre en place des mécanismes de protection. Certains courtiers ont mis en place des produits qui permettent à leurs clients d'accéder à des grands blocs de couverture, facilitant ainsi l'accès au marché. On voit aussi des initiatives pour standardiser les contrats, et beaucoup de travail est fait sur les exclusions.
En parallèle, le secteur étudie les possibilités offertes par les instruments du marché des capitaux pour « porter » ces risques.

Compte tenu de vos expériences internationales, quelles sont vos recommandations pour « débloquer » le marché de l'assurance cyber en France ?
Le marché de la cyber-assurance en France n'est pas plus ou moins développé que celui des autres pays du continent – c'est-à-dire il est petit faible, mais en croissance. Pour avancer dans cette direction, des efforts continuels et en termes de communication et d'éducation sont nécessaires pour créer la demande. En même temps, approfondir la compréhension des risques et de la capacité de les quantifier restent primordiaux. De nombreux assureurs n'ont pas encore l'appétit de couvrir des risques de cybercriminalité. Malheureusement, c'est à travers les cyberattaques du futur que le secteur apprendra. On le voit aux Etats-Unis, où les volumes se sont envolés, grâce aux assureurs qui ont pu créer une compréhension plus globale et plus profonde des facteurs de risques et des conséquences des évènements de cybercriminalité.

Guide pratique d'achat d'une assurance cyber

Par Jean-Christophe Gaillard (1991),
Fondateur et Directeur Associé chez Corix Partners,
cabinet de conseil particulier en Gestion d'Entreprise basé à Londres et spécialisé en Stratégie, Organisation & Gouvernance de la Sécurité. Il co-préside également le groupe Cyber Sécurité de l'association d'alumni de Télécom ParisTech.

Le marché de l'assurance cyber est loin du niveau de maturité de nombreux autres secteurs de l'assurance professionnelle, et fait face à de sérieux facteurs de blocage qui compliquent les choses pour courtiers, souscripteurs et régulateurs. Ces problèmes limitent également la valeur que de nombreux acheteurs pourraient retirer de produits d'assurance cyber.

- L'évolution très rapide des menaces et l'absence de mécanismes fiables de partage d'information autour des cyber-attaques rendent difficile l'application de modèles actuariels traditionnels.
- Même si les choses s'améliorent lentement, de nombreux acteurs du secteur manquent cruellement d'expérience pratique en matière de cybersécurité.
- Les régulateurs sont enfermés dans un dilemme entre risque systémique et risque de mévente, qui limite leur capacité à agir de façon claire.
- Enfin, il n'y a pas encore suffisamment de cas juridiques significatifs pour déterminer de façon claire dans quels sens le marché pourrait évoluer.

Fondamentalement, personne ne peut prédire les futurs vecteurs de cyber-attaques, et les acheteurs potentiellement intéressés par des produits spécifiques de l'assurance cyber ne peuvent pas s'attendre en pratique à être couverts à jamais contre des risques inconnus. Donc une approche mesurée s'impose aux acheteurs potentiels, en particulier aux PME, avec une attention particulière à porter aux 4 points suivants.

Où en êtes-vous vraiment en matière de cybersécurité ?

L'assurance cyber ne sera jamais une solution miracle et la présence réelle et démontrable de mesures de sécurité appropriées sera toujours le prérequis fondamental à n'importe quel remboursement par n'importe quel assureur. Avez-vous une compréhension claire des menaces cyber auxquelles vous faites face ? Seriez-vous en mesure de démontrer de façon fiable un niveau suffisant d'adhérence aux bonnes pratiques en matière de cybersécurité ?

Etes-vous déjà couvert ?

Des options de l'assurance cyber sont déjà incluses dans beaucoup de polices commerciales et il est essentiel de vérifier ces aspects avant de considérer une assurance cyber spécifique, et de déterminer si la couverture existante est suffisante (au regard des cyber menaces auxquelles l'entreprise fait face et des pratiques existantes au sein de l'entreprise en matière de cybersécurité).

Attention au contenu réel des polices spécifiques de l'assurance cyber

Les divers facteurs de blocage du secteur détaillés plus haut peuvent amener assureurs et souscripteurs à se couvrir contractuellement de façon stricte et rendent absolument essentiel de lire en détail les contrats d'assurance cyber spécifiques. Assurez-vous de bien comprendre toutes les exclusions et leur signification exacte (et si elles peuvent s'appliquer dans votre cas) : Une bonne compréhension commune du langage technique entre toutes les parties est absolument essentielle car l'absence de précédents et la grande diversité d'interprétation de certains termes pourraient vous obliger à des poursuites dans des cas extrêmes.

Attention à la valeur réelle des services à valeur ajoutée (services d'assistance juridique, d'assistance en réponse aux incidents…)

Certains courtiers rajoutent ces couches de service pour rendre leurs produits plus attrayants (et se dédouaner d'accusations de mévente au regard des exclusions qu'ils imposent par ailleurs) mais ce ne sont pas au sens strict des produits d'assurance, et les acheteurs potentiels doivent absolument considérer s'ils ont un besoin réel de ces services, s'ils y ont déjà accès par ailleurs, ou s'ils pourraient se les procurer à meilleur prix (en cas de besoin) via des partenariats existants (avec des cabinets juridiques ou de relations publiques par exemple). Beaucoup de ces recommandations sont des mesures de bon sens qui s'appliqueraient à nombre de décisions dans ce domaine, mais la faible maturité du secteur de l'assurance cyber (relative aux autres secteurs de l'assurance professionnelle) les rend essentielles pour l'acheteur potentiel sur le court à moyen-terme.

Nos recommandations

Du côté de la demande

Demander les attestations de police d'assurance cyber dans les appels d'offres

Cela peut paraitre procédurier mais quoi de plus incitatif que les clients demandent à leurs fournisseurs de décrire la façon dont ils couvrent les risques cyber (en plus des aspects techniques et opérationnels). Certaines sociétés commencent à le faire en particulier dans les domaines de l'externalisation de systèmes d'information. En revanche, cela est beaucoup moins répandu dans les domaines connexes. Faites le test : demandez à votre concessionnaire automobile ou à votre fournisseur d'énergie comment il couvre le risque cyber pour tiers ! Ainsi, une entreprise en exigeant de ses fournisseurs de solutions *cloud* leur police d'assurance cyber inciterait l'écosystème digital à monter en maturité sur les enjeux de cybersécurité.

Acheter des produits simples d'assurance cyber

Il faut apprendre en marchant. Alors quoi de plus simple que de souscrire une première police d'assurance cyber sur un périmètre restreint et avec une garantie précise (par exemple les risques de perte d'exploitation, suite à une interruption business liée à une attaque en Déni de Service). L'enjeu pour les acheteurs est de challenger les assureurs et courtiers, de faire monter en compétence les responsables internes de l'entreprise, et de voir comment les éventuels sinistres seraient pris en compte.

Du côté de l'offre

Expliquer ce qui est déjà couvert par les polices d'assurance existantes

Cela s'appelle le « silent cover », c'est-à-dire qu'une partie des conséquences d'un dégât cyber peut déjà être prise en compte dans des contrats de responsabilité civile, de dommages… Or de nombreuses entreprises ne savent pas ce qui est couvert et ce qui ne l'est pas. Les compagnies d'assurance doivent clarifier les garanties et exclusions de leurs produits d'assurance classiques comme cyber.

Faire connaitre l'offre d'assurance cyber

La compréhension de l'offre d'assurance cyber a bien avancé depuis ces trois dernières années mais il demeure encore de nombreuses entreprises qui n'en comprennent pas les enjeux. L'éducation du marché peut notamment passer par la mise en place de comparateurs de solutions d'assurance cyber, et par des guides d'achat ou de sensibilisation (par exemple le guide[1] sur les cyber-risques coproduit par le CESIN et l'AMRAE, les travaux menés par System-X, l'AMRAE, la FFA et FERMA sur le l'assurance cyber[2], ou le livre blanc du CLUSIF en cours de parution).

Favoriser les offres technico-assurantielles

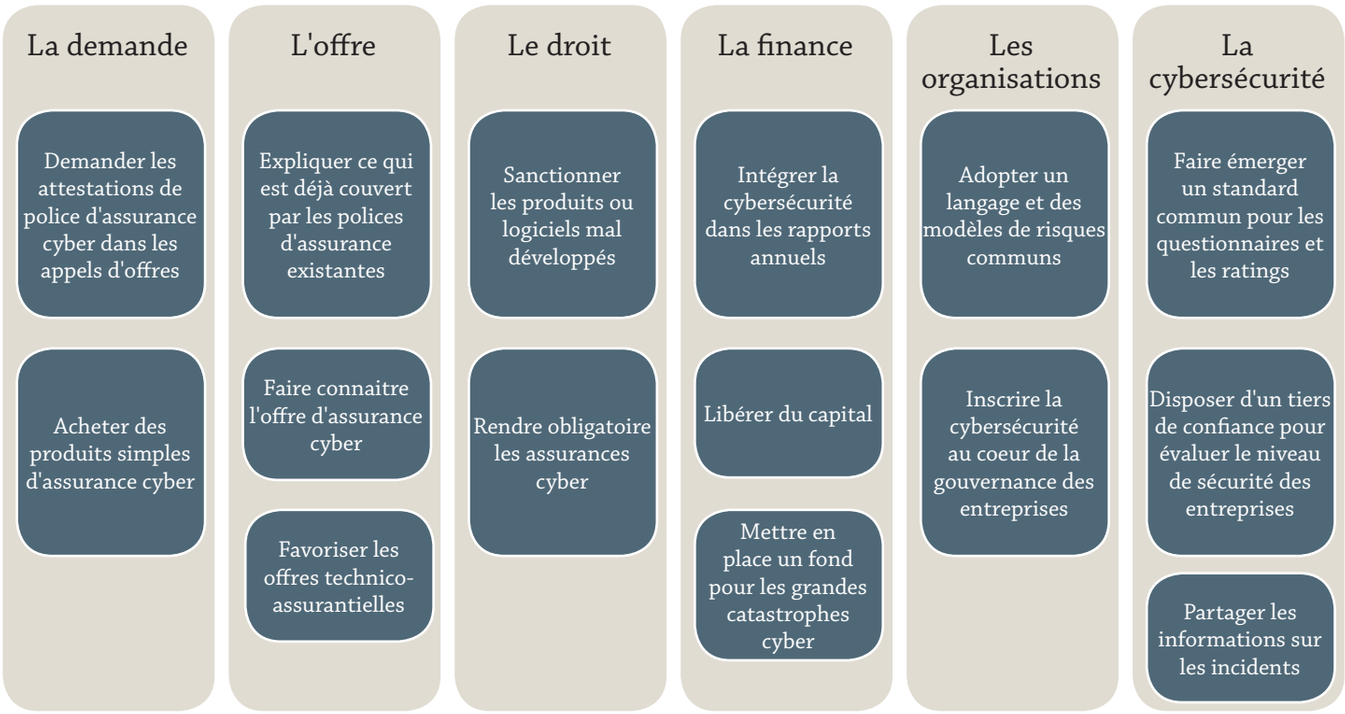
Il s'agit de proposer des offres d'assurance couplées à des prestations de services (réponse aux incidents, investigation, gestion de crise, communication…), notamment pour les PME et ETI. Il arrive bien souvent que suite à une attaque, les entreprises se retrouvent démunies et ne savent pas vers qui se tourner. Il y a aussi l'enjeu de mesurer les vulnérabilités de l'entreprise. Il existe ainsi déjà des offres qui couplent aspects techniques et assurantiels pour en permanence mesurer les risques cyber et, le cas échéant, conseiller à la société cliente de renforcer sa sécurité.

Du côté du droit

Sanctionner les produits ou logiciels mal développés

Dans les domaines alimentaire, pharmaceutique, chimique, financier… il existe de nombreuses règles sectorielles quant à la qualité des produits. En cas de non-conformité avérée, les fournisseurs sont fortement pénalisés. Or, quand des milliers d'objets connectés se transforment en plate-forme d'attaques distribuées de déni de service (DDoS) car ils sont mal conçus ou mal développés, les conséquences pour les constructeurs sont pratiquement inexistantes. Il est de leur responsabilité de mettre en place le « security by design » et de rappeler leurs produits

1/ www.amrae.fr/cyber-risques-outil-daide-à-lanalyse-et-au-traitement-assurantiel
2/ System-X, « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance », juillet 2016



s'il est avéré qu'ils sont notoirement vulnérables et attaquables (comme Jeep l'a fait pour un logiciel embarqué vulnérable). En outre, cela contribuera à la maitrise du risque systémique.

Rendre obligatoire les assurances cyber

Il existe de nombreux domaines où les assurances sont obligatoires. Pourquoi pas dans le domaine cyber ? Nous pensons que cela sera le cas dans quelques années, comme le laisse présager l'introduction de textes juridiques et réglementaires relatifs à la cybersécurité et à la protection des données à caractère personnel. Cela passera sans doute par la souscription d'assurances cyber dans le cadre de codes de bonne conduite de certaines filières, comme le bâtiment intelligent ou la voiture connectée.

Du côté de la finance

Intégrer la cybersécurité dans les rapports annuels

Tous les rapports annuels disposent désormais de plusieurs pages sur la responsabilité sociale et environnementale de l'entreprise. Certains mentionnent en quelques lignes les risques cyber dans le chapitre risques majeurs. C'est clairement insuffisant. Mentionner la souscription d'une assurance cyber permettrait aux investisseurs d'apprécier les démarches entreprises par le management pour améliorer le niveau de cybersécurité et la pérennité de leur entreprise face aux risques cyber. Cela participe d'une démarche de sécurité durable[3].

Libérer du capital

Dans certaines professions réglementées comme la finance ou l'assurance elle-même, il existe des exigences de réserve de capital (Bâle, Solvency). Or, la souscription d'une police d'assurance cyber permet de réaffecter une partie de ce capital.

Mettre en place un fond pour les grandes catastrophes cyber

Dans les domaines du terrorisme ou des catastrophes naturelles, il existe des fonds spécifiques pour couvrir les dommages au-delà d'un certain montant. Nous préconisons la mise en place d'une démarche similaire dans le domaine de l'assurance cyber pour couvrir tout ou partie des risques systémiques ou des grandes catastrophes cyber (« *black swan* »). Le fond pourrait être constitué à partir d'une taxe sur les contrats de responsabilité civile et/ou sur les produits et services liés aux technologies de l'information, voire à partir de pénalités financières conformément à la recommandation « Sanctionner les produits ou logiciels mal développés ».

Du côté des organisations

Adopter un langage et des modèles de risques communs

Dirigeants, Risk managers, RSSI, DSI, DAF… ne parlent pas le même langage. Certains ont des cultures et des approches financières, d'autres techniques et d'autres opérationnelles. Cela ne facilite pas la compréhension et la prise de décision. Il convient de présenter les risques cyber en risque business. En d'autres termes, la question n'est pas de connaitre le détail technique d'une attaque mais de comprendre son impact sur l'entreprise, en particulier en termes d'image et de pertes financières. Facile à recommander mais difficile à évaluer en raison de la nature intangible de certains actifs de l'entreprise, et de l'absence de modèles de risques cyber partagés sur le marché.

3/ www.observatoire-fic.com/la-securite-durable-appliquee-a-la-cybersecurite/

Inscrire clairement la cybersécurité au cœur de la gouvernance de l'entreprise

Certaines entreprises américaines commencent à nommer des spécialistes de la cybersécurité dans leur conseil d'administration. Si cette dynamique n'est pas transposable à toutes les entreprises, la démarche d'élever le niveau de compétences des membres impliqués dans la gouvernance des entreprises est à accélérer. Cette démarche est notamment préconisée par le rapport « *Advancing cyber resilience : Principles and Tools for Boards* » du World Economic Forum[4] rédigé avec le BCG et HP. La prise en considération du risque cyber à son juste niveau milite à placer les RSSI non pas sous la tutelle des directions informatiques mais par exemple au niveau de la direction des risques ou de la direction générale. De plus, former les DSI et RSSI aux techniques de l'assurance permettrait de faciliter le dialogue avec les risk managers.

Du côté de la cybersécurité

Faire émerger un standard commun pour les questionnaires et les ratings

Quoi de plus déroutant que de recevoir les questionnaires des cyber-assureurs. Ces questionnaires de « santé » sont perçus comme trop généraux ou trop intrusifs, et ont pour objet d'évaluer la maturité des pratiques de cybersécurité des futurs assurés. Certains s'inspirent de standards techniques de cybersécurité plus ou moins répandus. Il existe ainsi clairement une nécessité de voir émerger un standard commun pour faciliter le dialogue entre assureurs, courtiers et acheteurs. Parallèlement, ces dernières années ont vu apparaître des agences de notation (« *rating* ») des risques cyber. Si cette initiative est heureuse pour connaître le niveau de cybersécurité d'une entreprise et pouvoir comparer les entreprises, les méthodes utilisées pour les scorings demeurent souvent obscures et propriétaires. Un standard commun pourrait s'inspirer par exemple du NIST *cybersecurity framework*[5] aux États-Unis, des standards ETSI ISI (*Information Security Indicators*)[6] ou des règles d'hygiène informatique de l'ANSSI[7]. En analysant la chaîne de valeur de l'assurance cyber, il est probable que les réassureurs joueront un rôle clef dans l'émergence d'un standard de cybersécurité.

Disposer de tiers de confiance pour évaluer le niveau de cybersécurité des entreprises

Même si les agences de notation classiques (Moody's, Standard & Poor's, Fitch) commencent à intégrer l'évaluation des risques cyber, des sociétés technologiques américaines spécialisées dans l'évaluation de la performance des entreprises en matière de cybersécurité se développent depuis quelques années. Les ratings proposés aujourd'hui par les premiers acteurs du secteur sont effectués à partir de données publiques et d'analyses des adresses IP externes des entreprises considérées (vulnérabilités, spam, botnets…). Cela veut dire que seul le haut de l'iceberg est étudié. Pour aller plus loin, il conviendrait d'interroger directement les entreprises pour prendre en considération leurs faiblesses (ou forces) organisationnelles, opérationnelles, comportementales… Elles risquent d'être réticentes à fournir des données sans certaines garanties de confidentialité des informations. D'où la nécessité de disposer de tiers de confiance indépendants pour les ratings. Nous préconisons la création d'une agence de notation cyber au niveau européen, qui aurait un effet bénéfique sur le marché de l'assurance cyber et également pour la souveraineté européenne.

Partager les informations sur les incidents

Plusieurs textes juridiques et réglementaires actuels ou à venir (LPM, GDPR, NIS[8]…) exigent de la part des entreprises victimes d'attaques de déclarer leurs incidents auprès de régulateurs. Il convient de partager ces informations en anonymisant l'origine et le détail des sinistres. L'objectif est de participer à la constitution de bases de données pour mieux modéliser et quantifier les risques. En effet, des agences de modélisation de risques (RMS, AIR) commencent à développer des scénarios catastrophes mais il faut des données fiables pour les alimenter. A l'instar du DHS (*Department of Homeland Security*) aux Etats-Unis qui envisage de supporter le marché de l'assurance cyber par la création d'une base de données[9], nous préconisons la mise en place d'une base similaire en France et en Europe afin de faciliter l'échange anonyme d'informations sensibles au sein d'un environnement sécurisé et de confiance.

4/ http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf
5/ https://www.nist.gov/cyberframework
6/ http://www.etsi.org/technologies-clusters/technologies/information-security-indicators
7/ https://www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf
8/ Loi de Programmation Militaire, General Data Protection Regulation, Network and Information Security directive
9/ Etude APREF www.apref.org/sites/default/files/espacedocumentaire/note_apref_cyber_risque.pdf

Les auteurs

CHARLES D'AUMALE

Charles d'Aumale (1997) a 20 ans d'expérience dans les télécommunications et les technologies de l'information. Il débute sa carrière chez France Télécom aux Etats-Unis puis travaille en France dans des sociétés de stockage informatique et de reconnaissance d'image. Il développe ensuite le segment des objets communications (Internet of Things) chez Bouygues Telecom. Il participe aux stratégies NFC et MVNO d'Orange. Il dirige enfin la partie sécurité de la société française Ercom, particulièrement connue pour ses téléphones chiffrés. En 2015, il crée la société TRUST AND TECH. De 2012 à 2015, Charles a activement participé au groupe de travail sur le volet cybersécurité de la Nouvelle France Industrielle sous la direction de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Informations). Charles est membre du groupe cybersécurité de Télécom ParisTech. Charles est ingénieur de Télécom ParisTech (1997) et MBA de l'INSEAD (2006).

E-mail : charles.daumale@trustandtech.com • https://www.linkedin.com/in/charlesdaumale/

FRANÇOIS GRATIOLET

François Gratiolet (1999) est le Président de BUSINESS DIGITAL SECURITY, cabinet de conseil en stratégie et marketing dans le domaine du digital et cybersécurité. Précédemment Deputy Head of Group IT risk, Security & Assurance La Poste ou Chief Strategy Officer EMEA Qualys, il travaille depuis 18 ans à des projets de transformation business et de gestion des risques IT pour des grands groupes et à des missions de conseil en stratégie, marketing, évangélisation et développement d'affaires pour des start-ups, éditeurs technologiques ou fournisseurs de services. Diplômé de l'Executive MBA de l'ESCP Europe (2011) et de Télécom ParisTech (1999), il est certifié ISACA CISM, CISA et Risk Manager ISO 27005. Il est membre de l'IFA et du groupe cybersécurité de Télécom ParisTech.

E-mail : francois.gratiolet@business-digital-security.com • https://www.linkedin.com/in/businessdigitalsecurity/

STÉPHANE SOLLAT

Stéphane Sollat (2009) a plus de 20 ans dans les services numériques, distribués, mobiles et managés. En 1996 il réalise l'une des 1ères plate-forme web/intranet avec 1 millions d'utilisateurs d'une mutuelle assurance. En 2000, il est directeur des services managés Planar Synelec, leader mondial des salles de contrôle, où il implante le centre de supervision (NOC). A compter de 2004, il dirige des projets de plateformes de distribution numérique multi écrans pour l'industrie des médias et de la mobilité. En 2009, Il copilote le démonstrateur d'un projet ANR dans l'IoT et le M2M avec Télécom ParisTech, Oracle, SFR et le Crédit-Agricole. Stéphane est désormais consultant spécialisé dans des projets de Smart City et de bâtiments intelligents. Il a un BTS génie électrique et système industriel (1993) et Master of Science ATOMS de Télécom ParisTech (2009). Il est membre du groupe cybersécurité de Télécom ParisTech, du French IdO Privacy rattaché à la DGE du Ministère des finances et président de la sous-commission data de la SmartBuildingAlliance.

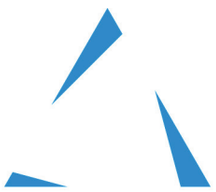
E-mail : sollat.consuting@gmail.com • https://www.linkedin.com/in/stephanesollat/

FRANÇOIS-XAVIER VINCENT

François-Xavier Vincent a plus de 18 ans d'expérience en cybersécurité, et travaille depuis 2008 au sein de la holding du Groupe AXA, où il a été Group CISO avant d'élargir son périmètre aux risques liés à l'information et à la technologie. Il a précédemment été chargé des aspects sécurité et interopérabilité d'un programme stratégique du ministère de la défense, avant de rejoindre l'ANSSI où il s'occupait entre autres du développement de la méthode EBIOS. Dans ces deux postes, il représentait également les intérêts nationaux auprès de l'OTAN et d'autres instances internationales. François-Xavier est ingénieur de l'Ecole Centrale de Lille (1992), titulaire d'un Executive MBA de l'ESSEC (2003), ancien auditeur du Haut Comité Français pour la Défense Civile (2013), et est certifié *Lead Auditor* ISO 27001, CISM, CRISC et COBIT *5 Implementer.*

E-mail : fx.vincent@gmail.com • https://www.linkedin.com/in/fxvincent/

Avec le soutien de
BUSINESS DIGITAL SECURITY et TRUST & TECH



BUSINESS DIGITAL SECURITY
Secure & Accelerate your business