Tendance de marché

Cyber-assurance : une offre multidimensionnelle à construire pour profiter des opportunités de marché

Publié le 21/10/2019

Avec l'informatisation généralisée des activités, la multiplication des échanges numériques ainsi que l'essor de l'externalisation de l'hébergement des applications et du stockage de données, apparaissent, de manière inhérente, de nouveaux risques, appelés cyber-risques, auxquels les acteurs privés et publics doivent maintenant faire face.

Dans ce contexte, les assureurs ont vu l'opportunité de se développer sur un nouveau marché en couvrant les conséquences financières des cyber-risques.

Le marché de la cyber-assurance est en effet un marché à potentiel du fait du périmètre de la matière assurable, de la fréquence et de la gravité des risques. Toutefois, des freins empêchent aujourd'hui son développement.

Voici un éclairage sur l'état du marché et les leviers possibles pour surmonter les obstacles !

Les cyber-risques : quèsaco ?

Introduction aux cyber-risques

Les cyber-risques désignent tout risque de perte financière, d'interruption des activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologies de l'information de cette dernière.

Ce risque de défaillance peut avoir différentes origines, comme une intrusion volontaire et non autorisée dans un système, souvent à des fins criminelles, une intrusion involontaire ou accidentelle d'un système sécurisé ou des risques opérationnels liés aux technologies de l'information en raison d'une mauvaise intégrité des systèmes ou d'autres facteurs.

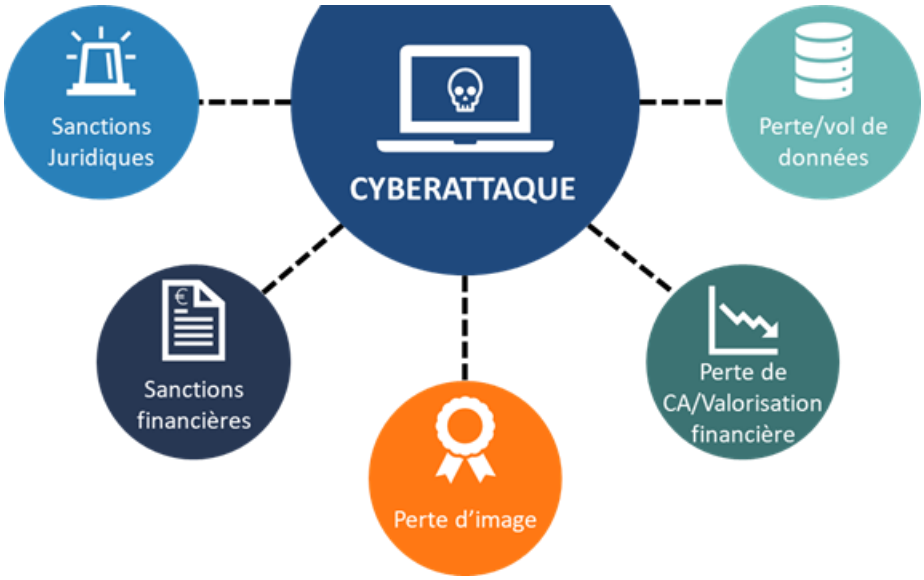
Les conséquences d'une cyber-attaque

Les cyber-attaques sont, parmi les cyber-risques, les plus craintes, celles-ci peuvent cibler tous les dispositifs informatiques : des ordinateurs aux serveurs, reliés ou non à Internet, en passant par les équipements périphériques tels que les imprimantes ou les appareils communicants comme les smartphones ou les tablettes. Il existe 4 types de cyber-attaques, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage et le sabotage.

Ces cyber-attaques peuvent être lourdes de conséquences, souvent financières, comme la perte de chiffre d'affaires en raison de la suspension de l'activité. Par exemple, la cyberattaque « NotPetya », survenue en juin 2017, aura fait perdre au groupe Saint-Gobain quelque 220 millions de chiffre d'affaires et 80 millions de résultat. Venue d'Ukraine, l'attaque avait touché des dizaines de milliers de PC et de serveurs au sein du groupe.

L'année 2017 marque un tournant dans la gravité des attaques. La croissance en nombre et en intensité des cyber-attaques a été remarquable. Mi-mai, l'attaque via le logiciel de ransomware « WannaCry » a touché de nombreux acteurs : entreprises privées mais aussi acteurs publics comme les hôpitaux britanniques ou le Ministère de l'Intérieur russe. En septembre, plusieurs piratages ont provoqué la fuite de données sensibles, comme le piratage du système informatique d'Equifax qui a mené au vol des données de 143 millions d'américains, provoquant une chute libre de son titre en bourse.

Ces attaques peuvent avoir des répercussions bien plus larges que des pertes financières ou d'information. A la suite d'un vol de données, ce sont l'image de l'entreprise et de la marque qui se retrouvent impactées. De plus, comme l'illustrent les exemples précédents, les conséquences d'une cyber-attaque ne sont pas réduites à la seule entreprise concernée. Celles-ci se répercutent sur de nombreuses parties prenantes. Dans le cas d'Equifax, ce sont des millions de citoyens américains qui ont vu des données sensibles les concernant (nom, date de naissance, mais aussi numéros de cartes bancaires) être subtilisées.



Les conséquences potentielles majeures d'une cyberattaque pour une entreprise

Acteurs publics et privés prennent progressivement conscience de la menace

Face à ces risques majeurs, on observe une prise de conscience par les entreprises et les collectivités de l'importance de la menace qui pèse sur leurs activités.

Cette prise de conscience se caractérise par la hausse constatée des investissements de cybersécurité et la mise en place de mesures de prévention et de sensibilisation au sein des organisations. D'après le traditionnel Baromètre des risques 2019 de l'assureur Allianz réalisé auprès de plus de 2 400 experts dans 86 pays, le cyber risque est devenu au niveau mondial, la principale crainte des entreprises (37 % des réponses), ex aequo avec l'interruption d'activité (37 %). En France, les entreprises en font même aujourd'hui leur risque numéro un.

Cette évolution est favorisée en 1er lieu par les expériences vécues et l'apprentissage forcé consécutif aux cyberattaques survenues, mais aussi du fait de l'évolution du cadre réglementaire et d'une communication plus importante sur le sujet de la cybersécurité.

Des cyber-attaques qui n'épargnent personne

Comme indiqué plus haut, le nombre et l'intensité des cyber-attaques ne cessent d'augmenter : les attaques ont progressé de +125% depuis 2015, et leur coût moyen a progressé de +72% depuis 2014.

Les cyber-attaques ne touchent pas que les grandes entreprises ou que les entreprises œuvrant sur des secteurs particuliers. Les attaques touchent toutes les structures : 4 entreprises françaises sur 5 déclarent avoir subi au moins une cyber-attaque en 2018 et la moitié d'entre elles, 4 attaques ou plus.

Il est à souligner aussi que les TPE et PME sont les cibles préférées des hackers. Avec des moyens et des dispositifs de protection limités, elles sont plus vulnérables. En 2017, 79 % des victimes d'une faille de sécurité étaient des PME.

Un cadre réglementaire qui contrait à prendre des dispositions préventives

La législation ayant trait aux cyber-attaques ou à leurs conséquences s'est fortement densifiée ces dernières années. Cela constitue d'ailleurs un facteur concourant à la prise en considération croissante de ces risques par les acteurs économiques.

La loi n°2017-399, entrée en vigueur en mars 2017, oblige les entreprises de plus de 10 000 salariés exerçant sur le territoire français à assurer un « devoir de vigilance » vis-à-vis d'elle-même et de ses sous-traitants. Elles sont ainsi sommées de s'assurer que toute mesure pour identifier, prévenir, éviter ou limiter toutes cyber-attaques et leurs impacts a bien été prise.

En mai 2018, un nouveau régime juridique de responsabilité en matière de protection des données personnelles est entré en vigueur au niveau européen (RGPD). Il vise, entre autres, à placer les entreprises face à leurs responsabilités en cas de cyber-attaque en mettant en place une « obligation de notification » (directive NIS).

Celle-ci oblige toute entreprise victime d'une cyber-attaque à en notifier l'autorité de contrôle compétente ainsi que les individus concernés par une potentielle atteinte à leurs données personnelles. Cette obligation expose les entreprises à la mise en cause de leur responsabilité par les victimes et ainsi à des poursuites judiciaires.

Une communication importante sur la cybersécurité

La prise de conscience de la menace est aussi favorisée par les mesures de sécurité et les actions de communication engagées par l'Etat et les pouvoirs publics.

En effet, dès 2015, la France s'est dotée d'une Stratégie nationale pour la sécurité du numérique. Destinée à accompagner la transition numérique de la société française, elle répond aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liées. Elle met en avant cinq lignes d'action :

1. Garantir la souveraineté nationale ;
2. Apporter une réponse forte contre les actes de cybermalveillance ;
3. Informer le grand public ;
4. Faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises ;
5. Renforcer la voix de la France à l'international.

La cyber-assurance : un marché qui se cherche

La cyber-assurance, un marché à potentiels

Evalué à 3,5 milliards de dollars en 2017, le marché de la cyber-assurance devrait atteindre les 9 milliards de dollars en 2020, avant de dépasser la barre des 20 milliards d'ici 2025.

En France, le volume total de primes atteignait 80 millions d'euros en 2018. Alimenté par une trentaine d'assureurs, ce marché promis à un bel avenir offre une capacité théorique totale de 700 millions d'euros.

En effet, la hausse de la fréquence et de la gravité des risques associée à des obligations réglementaires constitue un contexte favorable pour le développement de la cyber-assurance. Les entreprises ont intérêt à se doter de contrats de cyber-assurance afin de prévenir les dommages et frais engagés résultant d'une cyber-attaque.

Cependant, alors que 80% des entreprises déclarent avoir subi au moins une cyber-attaque en 2018, ***elles sont à peine 20% à avoir souscrit un contrat d'assurance spécifique.***

Des freins au développement qui tiennent des assurés mais surtout des assureurs eux-mêmes !

Le faible taux de couverture assurantielle des entreprises peut avoir 3 explications principales : la méconnaissance du risque et des couvertures possibles par les entreprises, la frilosité des assureurs et le manque de clarté des offres.

La ***méconnaissance du risque*** par certains acteurs économiques, principalement les TPE-PME constitue un 1er frein au marché de la cyber-assurance. En effet, le taux de couverture des entreprises s'avère très inégal. En France, d'après Marsh France, plus de 75 % des entreprises du CAC 40, plus de 40 % des sociétés du SBF120 et seulement de 2 à 5 % des PME seraient désormais équipées.

Ensuite, Solvabilité II impose aux assureurs de disposer de fonds propres à même de couvrir les risques qu'ils assurent. Or, à l'heure actuelle, ***l'absence de données fiables*** et éprouvées sur la cyber-sinistralité ***combinée à certaines conséquences difficilement mesurables financièrement*** – tels que l'atteinte à l'image de marque – rend les impacts d'une cyberattaque ***difficiles à évaluer et donc à couvrir***. Ainsi, l'un des enjeux principaux pour les assureurs comme pour les réassureurs est de maîtriser le cumul des engagements afin d'éviter d'être confrontés à des pertes à compenser trop importantes. Ce risque d'insolvabilité est par ailleurs renforcé par le fait qu'un même fait générateur peut potentiellement concerner de nombreuses entreprises assurées.

Enfin, ***l'offre et l'étendue de la couverture de certains contrats d'assurance restent floues*** au sujet des cyber-risques. Si les contrats dommage ou de responsabilité civile peuvent, dans certains cas, couvrir certaines conséquences d'un cyber-incident, ces derniers ne couvrent pas l'intégralité des impacts potentiels d'une cyberattaque. Si une entreprise souhaite que les frais de notifications soient pris en charge par un assureur, elle devra souscrire à un contrat spécifique de cyber-assurance. Les assureurs devront effectuer un travail de clarification de l'étendue de la couverture des contrats actuels afin de lever les incertitudes dues aux « silent cover » (impacts d'une cyberattaque potentiellement couverts par les contrats traditionnels). En France, ce travail de clarification de l'articulation des contrats concernés a débuté sous la direction de la FFA.

La conviction de Synaxia Conseil : proposer une offre multidimensionnelle pour lever les freins actuels et profiter des opportunités sur le marché des TPE-PME

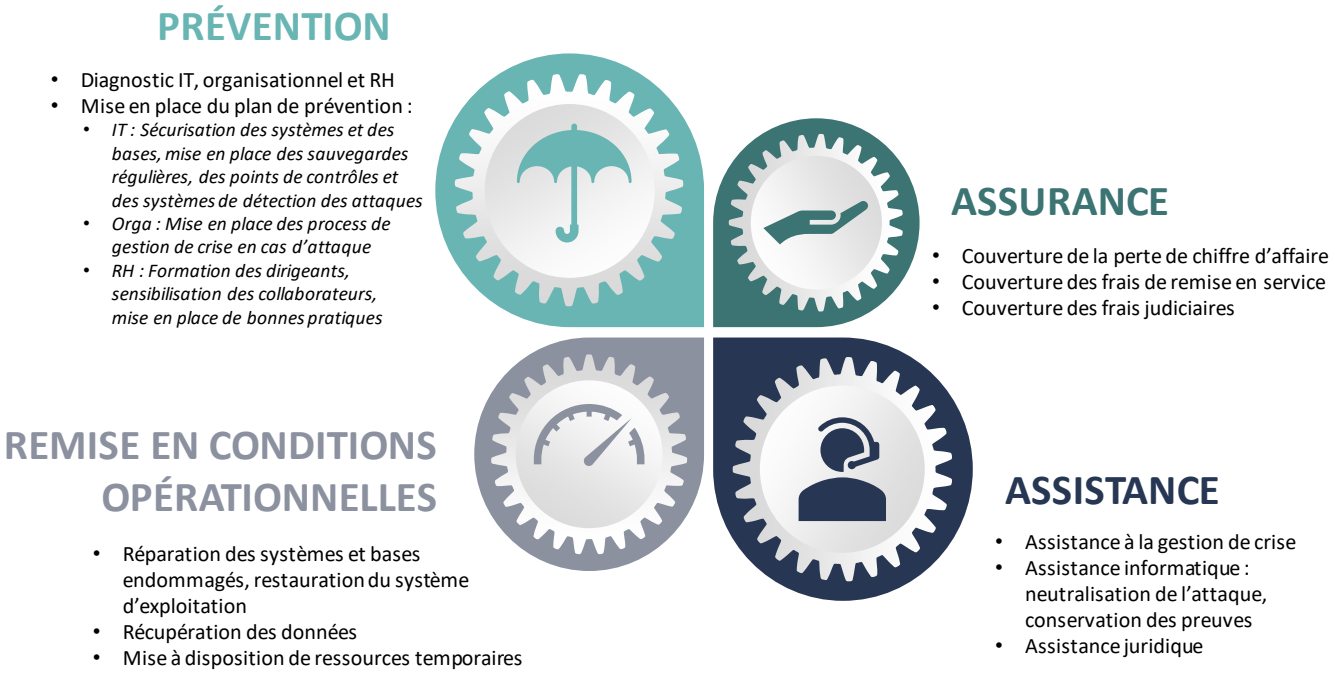
Afin de répondre au mieux aux besoins des entreprises, et plus particulièrement des TPE-PME, mais également d'améliorer la prévention des risques cyber et d'éviter l'augmentation exponentielle des sinistres, les assureurs gagneraient à proposer une offre assurantielle combinée à une offre technique et servicielle.

Les offres servicielles existent certes déjà : accompagnement à la remise en service du réseau et du système d'information, accompagnement juridique en cas de cyber-accident, ou encore mise à disposition de services de récupération des données. Pour autant, l'offre d'accompagnement en amont du sinistre reste encore limitée. Or, pour une entreprise de taille intermédiaire ne disposant pas des ressources humaines et techniques nécessaires pour assurer sa cybersécurité une offre d'assurance est adaptée pour l'aider en cas de sinistre mais n'en réduit pas les risques de survenue.

Les assureurs pourraient répondre à cette problématique en s'associant avec des partenaires (SSII, cabinet de conseil spécialisés, entreprises de cybersécurité) à même de réaliser un diagnostic IT, organisationnel et RH, de mettre en œuvre des mesures préventives (et ainsi assurer à l'entreprise une meilleure protection face aux cyber-risques) et d'accompagner

l'entreprise en cas d'attaque, et ce sur l'ensemble des conséquences : financières, informatiques, juridiques et organisationnelles.

Le ***'cyberpack'*** combinerait ainsi 4 composantes, au service de la maîtrise globale de ces risques : prévention, assurance, assistance et remise en conditions opérationnelles.



Une offre assurantielle et servicielle pour mieux répondre aux besoins des PME

Ce pack pourrait alors séduire bon nombre de TPE – PME, grâce au tout en un de l'offre.

Pour les assureurs, cela serait bénéfique à tout point de vue : commercial bien sûr mais aussi assurantiel : les dispositifs de prévention permettent de limiter la survenance et / ou la gravité des risques avérés et l'acquisition d'informations plus importantes et plus fines permettent d'affiner progressivement les modèles économiques et ainsi maîtriser les engagements de solvabilité.

Sources :

https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_rapport_cyber-risk_jan-2018_fr_web.pdf

https://www.lesechos.fr/idees-debats/cercle/assurance-et-cybersecurite-pourquoi-cest-encore-flou-pour-les-entreprises-1131063

https://www.lci.fr/high-tech/cybersecurite-pme-ou-grandes-societes-plus-de-neuf-entreprises-francaises-sur-dix-pas-pretes-en-cas-d-attaque-informatique-2119508.html

https://www.usinenouvelle.com/article/cyberattaques-les-consequences-sont-multiples.N374699

http://www.globalsecuritymag.fr/Cybersecurite-le-top-management-en,20190820,90017.html