CIO.FOCUS

Les cyber-assurances, un outil au service de la résilience des organisations

EN BREF

Apparues il y a une quinzaine d'années, les cyber-assurances étaient jusqu'à présent souscrites majoritairement par les très grandes entreprises. Avec la hausse des cyber-attaques, l'outil commence lentement à se démocratiser, et intéresse aussi bien les RSSI que les Risk Managers.
Complémentaires des politiques de cybersécurité, qui visent à limiter la fréquence des incidents, les assurances cyber permettent de réduire l'impact des sinistres IT quand ceux-ci surviennent malgré tout. A ce titre, elles contribuent elles-aussi à la résilience des organisations.
Le rôle et le fonctionnement de ce type d'assurance restent encore méconnus de beaucoup d'entreprises, qui peinent à appréhender leur niveau d'exposition aux cyber-risques.
Ce CIO Focus dresse un état des lieux du marché actuel et de ses enjeux. Des experts détaillent également les spécificités de ce type d'assurance, leurs limites et les points d'attention à connaître.

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO :
26-28 rue Danielle Casanova 75002 Paris

Rédacteur en chef :
Bertrand Lemaire
blemaire@it-news-info.com
Tél. : 01 41 97 62 10

Principaux associés :
IT Facto et International Data Group Inc.

Président et Directeur de publication :
Nicolas Beaumont

Directeur général : Nicolas Beaumont

CIO est édité par **IT NEWS INFO**,
SAS au capital de 3000000 €

SOMMAIRE

/ INTERVIEWS

Philippe Cotelle (AMRAE) : « l'assurance cyber est un outil vraiment intéressant, mais difficile à manipuler »

Administrateur de l'AMRAE, Philippe Cotelle préside la Commission Systèmes d'information de l'association. Risk Manager d'Airbus Defense & Space, il supervise notamment les garanties d'assurance en cyber-risques de l'ensemble du groupe. Pour CIO, il fait le point sur les enjeux et le marché actuel de la cyber-assurance.

Philippe Cotelle, Président de la Commission Systèmes d'information de l'AMRAE : « la cyber-assurance est aussi un défi pour les assureurs. »

CIO : Quel est le niveau de maturité des entreprises en matière de cyber-assurance ?

Philippe Cotelle : Dans les grandes entreprises, la prise de conscience du risque cyber est établie, aussi bien au niveau des responsables de la sécurité que du comité exécutif. Presque tous les grands groupes ont souscrit une cyber-assurance. Les dirigeants ont compris que la médiatisation des incidents de cybersécurité pouvait les mettre directement en cause : l'assurance permet de montrer qu'ils ont pris en compte de façon effective ce type de risques.

Les entreprises de taille intermédiaire n'ont pas encore atteint le même niveau de maturité, même si celle-ci se développe. En revanche, il y a une vraie nécessité de prendre en compte ce problème dans les PME. Les petites entreprises rencontrent des difficultés à évaluer et à apprécier les cyber-risques, d'autant plus que les PME victimes de cyberattaques font rarement la Une des journaux, même en cas d'impact majeur.

CIO : Pourquoi ces difficultés dans les PME ?

Philippe Cotelle : Le risque cyber est diffus, transverse et multiforme. Il menace aussi bien les données que la capacité de production d'une entreprise, sa propriété intellectuelle, et peut même mettre en jeu des certifications sur les biens et services délivrés. Pour les dirigeants d'entreprises de taille moyenne, confrontés à une multitude d'autres risques, ce côté protéiforme rend le cyber-risque complexe à appréhender. De ce fait, sa priorité demeure moindre, et l'intérêt de souscrire une assurance supplémentaire reste à démontrer. La prise de conscience progresse très lentement, et la pénétration du marché des cyber-assurances dans les PME est encore faible. Par ailleurs, l'assurance cyber est un outil vraiment intéressant, mais difficile à manipuler car complexe. Elle couvre en effet un risque transverse, avec des impacts directs sur la capacité de l'entreprise à produire, à vendre ou à maintenir ses produits et services, mais aussi des conséquences en matière de protection des données personnelles des clients, sans compter de potentiels dommages à des tiers. Le plus compliqué pour un dirigeant de PME n'est pas de souscrire, mais de définir ce qu'il veut garantir financièrement.

CIO : Comment sensibiliser davantage les entreprises aux cybermenaces ?

Philippe Cotelle : L'AMRAE - avec quelques autres acteurs de référence - travaille beaucoup sur la sensibilisation des entreprises au cyber-risque, car celui-ci devient un enjeu majeur avec la digitalisation de l'économie, qui menace à la fois la pérennité et la résilience des organisations. Nous voulons accélérer la prise de conscience. Dans cette optique, l'association a entrepris des travaux avec l'ANSSI, afin de bâtir ce qui sera le guide de référence sur le risk management du numérique. Le but est d'aider toutes les entreprises, dont les PME et ETI, à mieux appréhender ce risque, en détaillant les concepts nécessaires à l'appropriation et à la maîtrise du risque cyber.

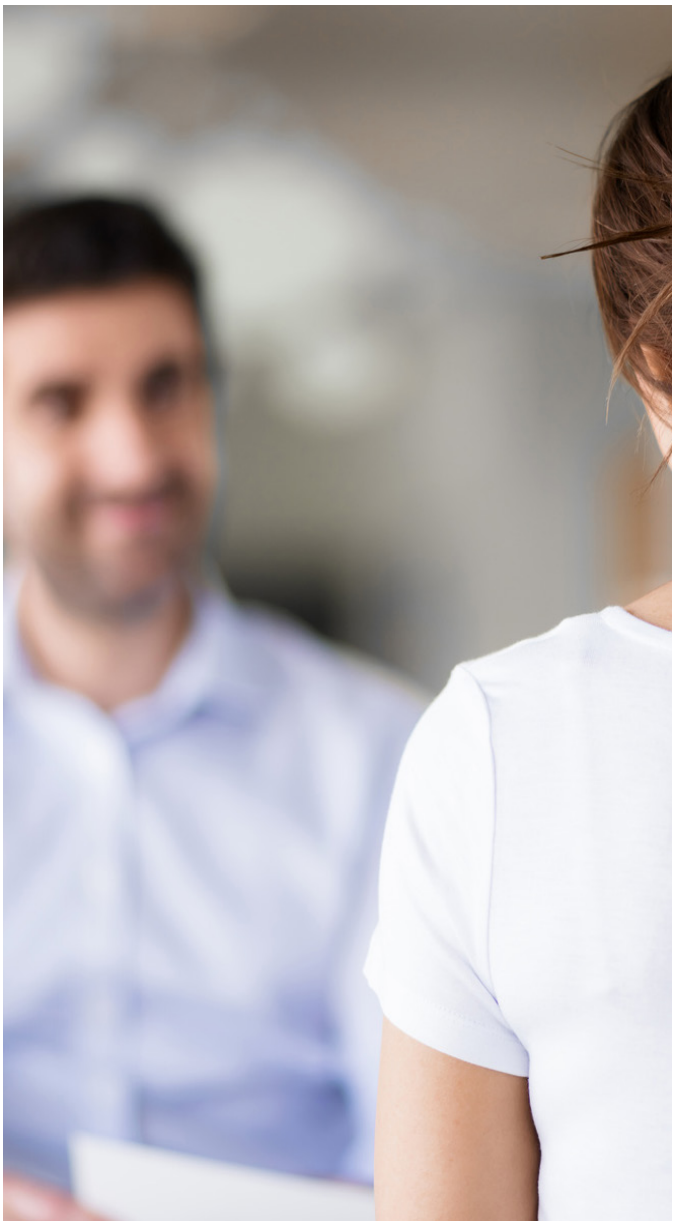
Dans ce guide, l'AMRAE partage des techniques de gestion du risque applicables au risque numérique, et l'ANSSI apporte sa crédibilité technique. Le but est d'assurer la cohérence des politiques de sécurité du SI dans le cadre d'une approche globale de risk management. La cyber-assurance devient un outil qui intègre cet aspect-là. Ce n'est pas l'Alpha et l'Omega pour gérer le risque numérique, et ce n'est pas non plus une voie facile : il faut avant tout comprendre son exposition au risque, afin que la couverture souscrite corresponde bien à la situation réelle.

CIO : Quel rôle joue la cyber-assurance par rapport à la politique de cybersécurité ?

Philippe Cotelle : Le cyber-risque est un vrai risque d'entreprise. La réduction et la prévention des cyber-risques forment la priorité, la cyber-assurance vient en complément.Pour convaincre la direction, il faut lui fournir des arguments concrets, en quantifiant le degré d'exposition de l'entreprise aux cyber-risques. Pour cela, il ne faut pas seulement le RSSI autour de la table, mais l'ensemble des responsables métier. Il revient à ces derniers d'estimer et de chiffrer l'impact : si par exemple, la direction commerciale ne peut pas réaliser de ventes pendant quatre jours, ou bien la DRH se retrouve dans l'impossibilité de verser les salaires...

CIO : A l'heure actuelle, à quels enjeux sont confrontées les entreprises qui souhaitent mettre en place ce type de mécanisme ?

Philippe Cotelle : La souscription d'un contrat de cyber-assurance représente un double enjeu pour les clients, à la fois en termes d'offre et d'efficacité. Au niveau de l'offre, il n'existe pas vraiment de contrat standard aujourd'hui. Une multiplicité de couvertures est possible : certains contrats se limitent à mettre à disposition des experts en cas de crise, d'autres couvrent les frais de notification et d'indemnisation en cas d'atteinte à des tiers sans assurer la partie « amende », probablement difficile à assurer du point de vue réglementaire. Des contrats indemnisent les pertes d'exploitation réelles et potentielles en cas d'interruption des activités, d'autres



les frais de récupération des données. D'autres enfin peuvent couvrir les éventuelles pénalités de retard dues aux clients si un cyber-incident bloque la production. Par ailleurs, certains contrats classiques couvrent également le risque cyber ou certains de ses impacts (dommages, responsabilité...), de manière explicite ou silencieuse.

Concernant l'efficacité, la meilleure publicité pour la cyber-assurance, c'est une entreprise bien indemnisée après avoir subi une attaque avec un impact important. Voir un directeur général témoigner que son assurance l'a aidé à redémarrer après une attaque de grande ampleur ou n'a pas accru sa fragilité à un moment de forte tension aiderait fortement à promouvoir la cyber-assurance. Or, force est de constater qu'à ce jour les grands cyber-sinistrés les plus médiatisés n'ont pas été indemnisés de façon optimale, ou qu'ils avaient suffisamment de ressources financières pour passer le cap. Les assureurs, pour accorder leurs garanties financières peuvent être très directifs, à l'instar de ce qu'ils font en matière de prévention incendie. Or aujourd'hui, ils ne sont pas en position de pouvoir imposer des standards en matière de cybersécurité.

CIO : Quelles sont les étapes importantes lors de la souscription d'un tel contrat ?

Philippe Cotelle : En fonction de l'activité de l'entreprise, de sa taille et de nombreux autres paramètres, son niveau d'exposition au cyber-risque varie fortement. Elle doit s'assurer que le contrat de cyber-assurance comporte bien les modules adaptés à sa situation. Il est donc primordial que tout le management prenne le temps de bien hiérarchiser les menaces, afin d'aller chercher ensuite la bonne couverture. L'expression des besoins est une phase cruciale. Il faut de la clarté, à la fois pour avoir la bonne couverture et pour obtenir le budget nécessaire. Établir une liste la plus précise possible des cyber-risques auxquels l'entreprise est exposée, en précisant à la fois la nature et le montant de l'exposition, est un travail compliqué. Il faut trouver une personne suffisamment motivée et investie pour mener à bien cette tâche. La FERMA (Federation of European Risk Management Associations) a récemment publié un document rédigé avec les assureurs et les

courtiers, intitulé « Preparing for cyber insurance », qui aide les entreprises à identifier les différents modules possibles et à faire un choix éclairé.

CIO : Comment percevez-vous la tendance du marché du côté des assureurs ?

Philippe Cotelle : Les assureurs n'ont pas la capacité d'assurance suffisante pour couvrir le risque du moment. En revanche, ils ont une capacité suffisante pour couvrir la demande actuelle. En France, le marché s'élève à environ 500 millions d'euros de primes.

La tendance est difficile à prévoir, car s'il y a un réel intérêt des assureurs à développer cette branche, ceux-ci sont également inquiets du risque qu'eux-mêmes prennent à couvrir les cyber-risques. Il y a une vraie prise de conscience aussi chez ces derniers que le digital est partout, et que donc le risque est partout. Par ailleurs, les réassureurs sont en train de mettre la pression pour clarifier les intentions des différentes parties : la capacité offerte va sans doute se stabiliser quelque temps.

La cyber-assurance est aussi un défi pour les assureurs, car ce type de contrat les oblige à casser les silos traditionnels de l'assurance, avec d'un côté l'assurance dommages, de l'autre la responsabilité civile ou l'assurance transports. Actuellement, ces problématiques sont confiées à différents départements, qui ne se parlent pas. Or, dans le cas du cyber-risque, nous avons un déclencheur technique et des impacts multiples. Un contrat de cyber-assurance doit couvrir dans un seul texte des conséquences gérées dans des branches différentes. Heureusement, en face, le Risk Manager a cette approche transversale.

CIO : Est-ce que les évolutions réglementaires ou la pression du marché peuvent inciter les entreprises à souscrire une cyber-assurance ?

Philippe Cotelle : En cas d'attaque, les entreprises qui ont mis en place une gouvernance des risques doivent s'attendre à être interrogées sur les mesures qu'elles ont mis en place pour réduire les conséquences de l'attaque. En particulier, il faut se demander qui peut vous reprocher de ne pas avoir travaillé sur ce risque : votre banquier, vos clients, vos actionnaires, vos salariés... Rappelons-le : une entreprise dont les risques sont gérés est durable et responsable.

Par ailleurs, les grands groupes ont également compris que leur exposition aux risques cyber dépendait aussi de leur supply chain et de leurs sous-traitants. Beaucoup d'attaques qui les visent ciblent leurs fournisseurs. Comme ils en subissent l'impact, ils sont en train de réfléchir pour imposer des obligations à leurs sous-traitants, à la fois en termes de cybersécurité et de cyber-assurance. Ces dernières favorisent en effet le retour à la normale chez les fournisseurs, en sécurisant des ressources techniques en cas de crise.

Il y a aussi une évolution au niveau européen pour mettre en place une certification de cybersécurité. Cette tendance peut amener les assureurs à accompagner ce mouvement. Les agences de notation commencent aussi à prendre en compte le cyber-risque, comme le montre par exemple l'abaissement de la note d'Equifax par Moody's à la suite des vols de données subis en 2017.

Il est également question d'étendre les normes RSE pour englober les enjeux numériques, parmi lesquels les cyber-risques. Enfin, des réglementations comme le RGPD médiatisent certains aspects des risques cyber. Si les cyber-assurances ne prennent pas en charge les amendes en cas de non-conformité, elles peuvent aider les entreprises à réparer les dommages potentiels causés aux clients. A ce titre, c'est une opportunité pour développer la prise de conscience.

UN ARTICLE RÉDIGÉ PAR
Aurélie Chandeze, Journaliste

/MARCHÉ

Cyber assurance : le marché s'adapte à la hausse des menaces

Outil complémentaire des politiques de cybersécurité, la cyber-assurance commence à être connue plus largement. Néanmoins, ce marché encore émergent est amené à évoluer face à la diversité des besoins et des menaces.

Jean Bayon de la Tour (Marsh) : « La malveillance informatique est à l'origine de 80% des sinistres déclarés. »

Selon la neuvième édition de l'enquête annuelle sur le coût du cybercrime, réalisée par Accenture Security et le Ponemon Institute, le nombre de failles de sécurité s'est accrue de 67% entre 2013 et 2018. Dans ce contexte, le risque pour une organisation de subir une attaque informatique a fortement augmenté. Une autre enquête, menée entre avril et juin 2019 par le réseau d'audit, de conseil et d'expertise comptable RSM dans 33 pays européens, révèle que 39 % des 597 grandes entreprises interrogées ont été victimes d'une cyber-attaque, même si dans 75 % des cas, celle-ci n'a pas été rendue publique. Un constat confirmé par Lari Lehtonen, responsable de l'équipe cyber risques chez le courtier Marsh : « sur les six premiers mois de 2019, nous avons observé le même nombre de cyberattaques que sur tout 2018. Le volume des attaques s'accroît. »

Dans les 355 organisations interrogées pour l'étude Accenture, le coût moyen des cyberattaques a connu une hausse de 72% en cinq ans. En 2018, ce coût moyen a atteint 8,8 millions d'euros en France, une hausse de 23% par rapport à 2017. Selon l'étude, ces coûts se répartissent dans quatre grandes catégories : les interruptions d'activité, les pertes d'information, les pertes de revenus et les dommages aux équipements. Malgré ces chiffres, les organisations peinent à faire de la cybersécurité une priorité. Si 65% des répondants de l'étude RSM sont convaincus que la cybersécurité est un enjeu qui concerne directement la direction, le sujet n'est abordé en conseil d'administration que dans 54% des cas. La plupart du temps, la sécurité informatique ne devient une priorité qu'une fois que l'entreprise a subi une cyber-attaque (59% des cas).

Réduire l'impact des cyber-sinistres

Dans ce contexte, les assurances cyber peuvent s'avérer un complément utile aux politiques de sécurité, permettant de diminuer l'impact des incidents quand ceux-ci surviennent. « Il y a deux grands types d'événements déclencheurs pris en compte dans les contrats de cyber-assurance : la malveillance informatique est à l'origine de 80% des sinistres déclarés. Les autres événements (erreurs humaines, bugs, pannes, fuites accidentelles de données) représentent les 20% restants », estime Jean Bayon de la Tour, responsable Cyber pour l'Europe chez Marsh. « Dans la plupart des sinistres, il s'agit simplement de couvrir les frais de prise en charge technique et juridique nécessaires pour la remise en route de l'activité », explique Timothée Crespe, Senior Broker et Cyber Leader chez Aon France. « En moyenne, ces interventions représentent des montants de quelques dizaines de milliers d'euros. Dans certains cas, plus rares, les assureurs peuvent verser des indemnités qui grimpent au-delà du million d'euros, voire davantage. »

Selon l'ABI (association des assureurs britanniques), sur 207 cyber-sinistres déclarés en 2018, 99% ont bénéficié d'une indemnisation. Un chiffre à nuancer, car l'ABI indique également que seules 11% des entreprises du Royaume-Uni ont mis en place ce type de contrat. En France aussi, la maturité des entreprises en matière de cyber assurance est assez faible. Selon le courtier Marsh, près de 90% des entreprises du CAC40 ont souscrit une cyber assurance, le reste couvrant ce type de risques sur d'autres contrats. En revanche, la proportion chute dans les entreprises de taille intermédiaire. Marsh estime qu'entre 20 et 25% des ETI sont couvertes. « Dans les PME, le taux d'équipement est encore plus faible, avec seulement 5% d'entreprises qui ont mis en place ce type de contrat », indique Jean Bayon de la Tour.

Un marché en train de gagner en maturité

Néanmoins, une prise de conscience est en train de s'opérer, comme en témoignent les observations des différents acteurs interrogés dans le cadre de ce dossier. « En 2017, la majorité des entreprises victimes de sinistres informatiques en France n'étaient pas couvertes par une cyber-assurance. En 2019, beaucoup d'organisations visées par des cyber-attaques étaient protégées et ont pu être indemnisées. Très clairement, cette garantie a prouvé son utilité, et les entreprises qui ont souscrit de tels

Ezechiel Symenouh (Gras Savoye Willis Towers Watson) : « Aujourd'hui les assureurs revoient leurs engagements, afin de mieux gérer ces derniers. »

contrats sont indemnisées », souligne Jean Bayon de la Tour. « Nous observons actuellement une bonne dynamique de souscription de la part des ETI », indique Ezechiel Symenouh, Cyber Risks Practice Leader chez Gras Savoye Willis Towers Watson. « Auparavant, les processus de décision pouvaient être assez longs, avec des dossiers en attente durant plusieurs années. Depuis deux ans, le marché de l'assurance cyber a atteint un point d'inflexion : les études se réactivent plus rapidement, en particulier quand un grand cas de cyberattaque fait l'actualité. L'époque où les entreprises considéraient les incidents cyber comme la théorie du cygne noir semble révolue. Les directions générales prennent conscience du risque, il arrive même que nous les rencontrions au début du processus. » De son côté, Timothée Crespe note que des entreprises commencent à communiquer ouvertement sur la cyber-assurance dans leur rapport annuel ou lors de la survenance d'incidents cyber, citant par exemple Altran ou Eurofins.

De l'importance de tester ses garanties cyber

Pour Léopold Larios de Piña, Vice-Président Formation de l'AMRAE et Risk Manager chez Mazars, la montée des cyber incidents permet aux entreprises de « tester » leurs garanties cyber, en évaluant dans quelle mesure souscripteurs et assureur ont l'intention de couvrir ces risques, ainsi que la solidité financière de l'assureur et

la technicité des équipes d'indemnisation. Globalement, les contrats existants semblent assez bien répondre aux enjeux des clients. La neuvième enquête annuelle Advisen sur la sécurité de l'information et la gestion des cyber-risques, financée par l'assureur Zurich, révèle ainsi que 70% des entreprises ayant souscrit une cyber-assurance sont satisfaites de cette dernière (sur 350 organisations, en majorité basées aux USA). Néanmoins, la même étude fait état de plusieurs entreprises qui n'ont pas été indemnisées car les cyber-sinistres subis étaient en dessous du seuil de franchise de leur contrat. Citons également quelques cas récents d'entreprises victimes du ransomware NotPetya, en litige avec leurs assureurs car ceux-ci refusent de les indemniser (Mondelez, DLA Piper). Par ailleurs, 60% des répondants de l'enquête Advisen/Zurich attendent davantage de clarté dans leurs contrats de cyber-assurance, afin d'éviter les recoupements avec d'autres contrats.

Un marché qui commence à devenir plus sélectif

Du côté des assureurs, le marché s'est bien étoffé. Marsh recense aujourd'hui une cinquantaine d'assureurs qui proposent des contrats de cyber assurance en France. « Au départ, ce marché était surtout porté par les assureurs anglo-saxons, mais tous les grands assureurs français ont aussi aujourd'hui une offre dans ce domaine », souligne Jean Bayon de la Tour. Selon le courtier Gras Savoye Willis Towers Watson, la capacité théorique cumulée du marché français de la cyber assurance s'élève aujourd'hui à environ 600 millions d'euros (500 millions selon l'AMRAE), avec un montant moyen de 25 millions d'euros par assureur. Tous les acteurs rencontrés s'accordent pour dire que cette capacité va se stabiliser, après plusieurs années de hausse. « En réalité, ce ne sont pas forcément ces montants-là qui sont déployés. Le marché de la cyber-assurance commence à être plus sélectif », pointe Ezechiel Symenouh. « Au début, les assureurs cherchaient à constituer leur portefeuille. Les primes étaient assez compétitives, compte tenu d'un faible historique sinistre, avec une volonté des assureurs de développer une branche en masse, en étant souple dans la souscription et en restant toujours dans une logique de mutualisation. Aujourd'hui, il n'y a pas une semaine sans déclaration de cyber-sinistre. Avec cette multiplication des sinistres, les assureurs font davantage attention à leur portefeuille et revoient leurs engagements afin de mieux les gérer. Ils sont plus regardants sur le niveau de sécurité du système d'information des entreprises et sur leur politique de gestion des données. Il arrive que certains assureurs déclinent le risque, s'ils considèrent que le niveau de sécurité informatique est insuffisant », détaille-t-il.

De son côté, l'AMRAE observe également une montée des tarifs et des franchises plus hautes, ainsi que des

difficultés à placer les très gros contrats (plus de 100 millions d'euros). Si la capacité du marché suffit à couvrir la demande actuelle, il faut avoir en tête que le niveau d'exposition réel est bien supérieur.

Les assureurs veulent mieux maîtriser leur exposition au cyber-risque

LMalgré une sinistralité en augmentation, le marché de la cyber-assurance reste profitable pour les assureurs, « un aspect important pour garantir l'indemnisation des clients », relève Jean Bayon de la Tour. Cependant, les assureurs ont entamé une remise à plat de leurs contrats afin de mieux maîtriser le niveau de risque

associé, notamment sous la pression des réassureurs et des autorités de régulation. « De grands assureurs comme AGCS (Allianz) ou AIG sont en train de revoir la couverture des risques cyber dans leurs contrats traditionnels, notamment car le régulateur au Royaume-Uni a demandé de spécifier clairement les risques couverts par chaque contrat. C'est une opportunité pour les assureurs de clarifier leur offre », estime Ezechiel Symenouh.

« L'une des difficultés, c'est que le risque cyber est partout », souligne Astrid-Marie Pirson, directrice de la souscription chez Hiscox France. Pour Léopold Larios de Piña, « l'enjeu pour les assureurs et les réassureurs consiste en la modélisation de leurs potentiels risques de cumul. En effet, si cent clients utilisent un même fournisseur de messagerie sur un même data center, alors en cas d'interruption de service de ce dernier à cause d'une inondation, ou d'attaque par déni de service, les services rendus aux cent clients risquent d'être perturbés en même temps ». Astrid-Marie Pirson confirme que les assureurs travaillent aussi au niveau systémique, autour de scénarios comme un incident chez Microsoft ou Amazon Web Services à l'échelle planétaire, des cyber-incidents à l'échelle d'une ville entière, ou encore des attaques simultanées sur les dix plus grosses entreprises mondiales.

UN ARTICLE RÉDIGÉ PAR
Aurélie Chandeze, Journaliste

/ STRATÉGIE

Souscrire une cyber-assurance : conseils et points d'attention

Comment se passe le processus de souscription ? Quelles garanties trouve-t-on dans un contrat type de cyber-assurance ? Quel est le rôle des courtiers ? Le point avec les experts.

Timothée Crespe (Aon France) : « La cyber-assurance doit être une partie intégrante des processus de gestion des incidents cyber. »

Apparues il y a une quinzaine d'années, les cyber-assurances étaient jusqu'à présent souscrites majoritairement par les très grandes entreprises. Avec la hausse des incidents de cybersécurité, l'outil commence lentement à se démocratiser. « Depuis 2017, la prise de conscience se développe sous l'effet de deux phénomènes : d'une part, la vague des ransomwares a montré que toutes les entreprises pouvaient être touchées par des cybermenaces.

Cela a permis de remettre sur le devant de la scène les conseils d'hygiène informatique de base. D'autre part, le RGPD impose un certain nombre d'obligations aux entreprises, quelle que soit leur taille, qui peuvent aller jusqu'à repenser le modèle opérationnel. Cela contribue à la prise de conscience des enjeux cyber, notamment en matière de protection des données », constate Astrid-Marie Pirson, directrice de la souscription chez l'assureur Hiscox France. Néanmoins, le rôle et le fonctionnement de ce type d'assurance restent encore méconnus de beaucoup d'entreprises, qui peinent à appréhender leur niveau d'exposition aux cyber-risques. « Les cyber-événements peuvent avoir des impacts sur les systèmes d'information de production de l'entreprise, pas seulement sur ses données », précise Ezechiel Symenouh, Cyber Risks Practice Leader chez le courtier Gras Savoye Willis Towers Watson.

« Les entreprises investissent dans la cybersécurité pour réduire la fréquence des attaques.
La cyber-assurance joue un rôle complémentaire, en apportant une couverture de la sévérité. C'est un outil au service des RSSI et directions informatiques », souligne Jean Bayon de la Tour, responsable Cyber pour l'Europe chez le courtier Marsh.

Des recoupements avec d'autres contrats d'assurance

Signe que le marché de la cyber-assurance est encore émergent, beaucoup d'entreprises pensent encore que les contrats classiques IARD (Incendies, Accidents et Risques Divers) couvrent les événements informatiques. Mais attention : « en matière de cyber-risque, il faut bien faire la distinction entre les dommages matériels et immatériels », prévient Jean Bayon de la Tour. « Les dommages matériels sont habituellement couverts par les contrats traditionnels : par exemple, si un robot utilisé en production se fait pirater et provoque des dégâts à son environnement physique, ces dégâts donneront lieu à une indemnisation sur les polices classiques. En revanche, si un malware bloque la chaîne, obligeant l'entreprise à interrompre sa production pendant trois jours, la perte financière associée ne sera pas couverte par les polices traditionnelles, mais le sera par les assurances cyber. Ce type de scénario est rarement envisagé par les entreprises. C'est pourtant une réalité », ajoute-t-il.

Autre élément à l'origine de cette croyance, des contrats de responsabilité civile et dommages incluent parfois la couverture de certains risques cyber. « C'est ce que nous appelons une « silent cover » : dans ces contrats, les risques cyber ne sont pas clairement exclus, ou ils sont couverts de façon limitée », explique Ezechiel Symenouh. « Cette situation pose des problèmes aux assureurs, par le cumul des garanties. Actuellement, ces derniers cherchent plutôt à sortir de cette situation. » Ce dernier rappelle également qu'aucun contrat classique ne répond de manière complète à la problématique des cyber-menaces. « Ainsi, la plupart des contrats traditionnels ne proposent pas d'assistance. Or, dans 75% des cas, les cyber-sinistres impliquent des actions de gestion de crise. C'est avant tout ce type de garantie que les entreprises recherchent : l'accès à une hotline, avec un panel d'experts à leur disposition, que ce soit sur le plan informatique, juridique, ou des relations publiques. »

Le volet d'assistance, une garantie essentielle

Quelles sont alors les garanties spécifiques offertes dans le cadre d'une assurance cyber ?

« Ce type d'offre repose sur deux piliers : la compensation financière des préjudices subis, mais aussi l'assistance, à travers l'envoi d'experts. Elle couvre à la fois les dommages directs sur le système d'information de l'assuré, et les préjudices éventuels subis par des tiers, comme les clients de ce dernier. C'est l'une des rares garanties qui protège ces deux mondes à la fois », pointe Jean Bayon de la Tour.

Pour Astrid-Marie Pirson, « il y a certaines garanties transverses incontournables dans ce type de police, comme le volet d'assistance. » La prévention tient également une place importante. Hiscox a par exemple développé une formation en ligne destinée aux salariés des petites entreprises. « Ce module a pour objectif d'aider les clients à diminuer leur niveau de risque. Si plus de 80% des employés suivent avec succès cette formation, nous proposons une baisse de la franchise à nos clients », détaille Astrid-Marie Pirson. Viennent ensuite plusieurs volets permettant de limiter l'impact financier des cyber-sinistres sur l'entreprise :

- Un volet couvrant les dommages subis par la société, comme les pertes d'exploitation, mais aussi la cyber-extorsion ou les frais de notification en cas d'atteinte aux données ;

- Un volet couvrant les dommages causés à des tiers, notamment les violations de données personnelles, la fuite de données confidentielles (par exemple des données concernant une opération en cours dans un cabinet de fusions-acquisitions), transmission involontaire de virus ou encore utilisation du système d'information de l'assuré en vue d'attaquer des tiers (pour des attaques par déni de service par exemple). « Ce volet englobe également la notion de cyber-responsabilité pour les sites Web ou sur les réseaux sociaux, avec les risques associés au défacement ou à l'incitation à la haine », précise Astrid-Marie Pirson.

- Un dernier volet permet de couvrir les frais associés aux enquêtes administratives et les sanctions éventuelles pouvant en résulter.

Vigilance sur certaines clauses préétablies

Comme toute assurance, les contrats cyber ont des limites. Classiquement, celles-ci concernent l'étendue des garanties et ce que l'assureur peut indemniser, qui dépend notamment de ce que l'assuré est en mesure de justifier. « L'indemnisation des assureurs vise à permettre aux entreprises de revenir à l'état antérieur au sinistre. Bien entendu, il ne s'agit pas de laisser un système d'information avec une grosse vulnérabilité, mais le but n'est pas non plus de financer tout un dispositif de cybersécurité », précise Timothée Crespe, expert cyber chez le courtier Aon France.

Une autre limite importante est évoquée par Astrid-Marie Pirson : « les contrats cyber actuels couvrent les pertes financières, pas les dommages matériels et corporels. La FFA (Fédération Française de l'Assurance) s'est intéressée par exemple aux incendies causés par des cyber-attaques, et la recommandation actuelle est plutôt de couvrir ce risque à travers des polices de dommages classiques. »

Par ailleurs, le marché est divisé sur deux sujets : la couverture du risque de sanctions et la prise en charge des demandes de rançons à la suite d'attaques par ransomwares. Certains assureurs hésitent en effet à couvrir ce type de conséquences en cas de cyber-attaque. Dans le cas des sanctions, il n'existe pour l'instant pas de jurisprudence de principe de la Cour de Cassation précisant si celles-ci peuvent être couvertes ou pas. « Seule certitude, si la sanction fait suite à une violation délibérée d'une réglementation, elle n'est pas couverte. En revanche, si une entreprise subit une sanction alors qu'elle a cherché à se mettre en conformité et peut le démontrer, il n'y a pas de position officielle, ni de la CNIL, ni de la FFA ou de la Cour de Cassation, qui interdit d'assurer ce risque », observe Astrid-Marie Pirson. Les enjeux sont similaires pour le cas des rançons, qui peuvent parfois se trouver mêlés à des enjeux de financement du terrorisme. « Dès lors que rien n'interdit aux entreprises de choisir de payer, il n'y a pas de raison d'interdire à l'assureur de les couvrir », estime la directrice de la souscription.

Enfin, début 2019 la firme de conseil spécialisée dans les assurances Mactavish, basée au Royaume-Uni, a provoqué une levée de boucliers sur le marché, en mettant en garde les entreprises contre huit failles rencontrées dans des contrats de cyber-assurance préétablis. Parmi celles-ci figurent notamment des restrictions sur le type d'événement déclencheur d'un sinistre, écartant les causes accidentelles pour se limiter aux actes malveillants, ou encore des clauses excluant la couverture d'incidents sur des systèmes en développement ou en cours de déploiement. Cette étude, ainsi que les réactions suscitées, rappellent la nécessité de rédiger des clauses claires et compréhensibles par l'ensemble des parties prenantes.

Bien définir son niveau de risque et le périmètre à couvrir

L'étape la plus complexe au moment de souscrire une cyber-assurance ne concerne pas tant le processus en tant que tel que la définition du périmètre à assurer. En effet, pour rendre ce type de produit plus accessible, les assureurs ont considérablement simplifié le processus de souscription, notamment pour les PME. « Aujourd'hui, ce n'est pas envisageable de faire trois audits et de soumettre un questionnaire de quinze pages aux clients qui souhaitent ce type de produit. Pour obtenir les informations nécessaires de façon moins douloureuse, nous nous appuyons sur des partenaires qui travaillent sur une approche statistiques des risques par typologie d'entreprise », décrit Astrid-Marie Pirson.

Pour les grands comptes, le processus passe en général par des réunions de souscription, généralement organisées par les courtiers. Pendant celles-ci, les assureurs, parfois accompagnés d'experts, échangent en direct avec les décideurs impliqués dans le processus : DSI, RSSI, Risk managers, parfois des représentants du département financier, du service chargé des assurances, voire même de la direction générale. « Lors de ces réunions, nous passons en revue différents points, comme la gouvernance des risques, la gestion opérationnelle des cyber-événements ainsi que les procédures de réponse aux incidents », explique Ezechiel Symenouh.

Certaines entreprises hésitent à se lancer dans ces démarches, de crainte de se faire dicter leur politique de cybersécurité par les compagnies d'assurance. « Les assureurs ne s'immiscent pas dans le système d'information, ce ne sont pas des prescripteurs », rassure Jean Bayon de la Tour. « Leur démarche est plutôt de comprendre l'exposition au risque de chaque client et ce qui a été mis en face pour la réduire », indique Lari Lehtonen, responsable de l'équipe cyber risques chez Marsh. « En théorie, les assureurs doivent se faire un avis sur le niveau de sécurité pour évaluer la prime. Mais c'est très compliqué de définir des critères pour établir si un système d'information est bien sécurisé, les organisations étant très diverses. Pour les PME, les critères restent assez standard. Pour les grands comptes, les risques sont traités au cas par cas. Aujourd'hui, les assureurs sont plus dans une approche qualitative que quantitative. Plus le RSSI fait du bon travail, plus les primes seront faibles. », complète Jean Bayon de la Tour. « Il ne faut pas perdre de vue que quoi qu'une société fasse, elle ne peut pas se prémunir complètement face aux cyber-risques. Sa politique de sécurité va juste jouer sur la fréquence des attaques : tout le monde se fait hacker, même la NSA. Le risque n'est jamais nul », insiste Lari Lehtonen.

Intégrer la cyber-assurance aux dispositifs de résilience

Pour bien évaluer son exposition au risque, Timothée Crespe conseille de bâtir des scénarios en interne afin d'évaluer les pertes potentielles. Sur ces étapes, RSSI et Risk Managers ont un rôle essentiel à jouer, pour veiller à rédiger le cahier des charges de la manière la plus claire possible. Timothée Crespe évoque aussi la nécessité d'effectuer des arbitrages chez les assurés, afin de répartir les différentes primes d'assurance de façon pertinente. « Les cyber risques concernent avant tout des actifs intangibles, essentiellement les données. C'est surtout là que les assurés cherchent à se couvrir, plutôt que sur le hardware. En effet, en cas de problème sur l'infrastructure, une entreprise peut généralement rétablir assez vite ses activités si ses données sont disponibles. En revanche, si ce n'est pas le cas, les employés ne peuvent tout simplement pas travailler. »

Enfin, il faut prévoir en amont les éléments à collecter en cas d'incident, afin de pouvoir fournir les justificatifs nécessaires pour la prise en charge. « Pour les pertes d'exploitation, c'est assez simple, les états financiers permettent de les chiffrer. En revanche, si l'entreprise fait appel à des prestataires, il faut bien conserver les différentes factures et lister l'ensemble des frais engagés », insiste Timothée Crespe. Ce dernier rappelle également, à juste titre, qu'il faut considérer la cyber-assurance comme une partie intégrante des processus de gestion des incidents cyber, destinée à assurer la résilience de l'entreprise.

Les courtiers, un accompagnement en amont comme en aval

PPour Ezechiel Symenouh, dans le domaine de la cyber-assurance les courtiers sortent de leur rôle traditionnel, pour aller vers l'accompagnement en amont. « Nous cherchons à sensibiliser nos clients. Nous avons par exemple des consultants qui cartographient les risques et qui évaluent la maturité des employés en matière de sécurité informatique. Nous permettons aussi aux clients de se benchmarker par rapport à leurs pairs. » Tout comme les assureurs, les courtiers aident également les organisations à quantifier le risque, à l'aide d'outils et de modèles actuariels. « Nous expliquons ce qu'apporte une cyber-assurance par rapport aux assurances responsabilité et dommages, comment elle peut compléter les contrats existants », relate Timothée Crespe.

Dans leur activité classique, les sociétés de courtage aident les clients à construire leur cahier des charges et soumettent ce dernier aux assureurs. « Nous aidons les Risk Managers à mobiliser en interne tous les acteurs nécessaires afin d'engager le processus de souscription », précise Timothée Crespe. Les courtiers évaluent également les assureurs sur des critères qualitatifs, examinant leur performance en gestion de crise et en gestion des sinistres. « Pour la gestion des sinistres, nous prenons en compte trois grands critères : la présence d'un bon centre d'appel, disponible 24 heures sur 24 et dans les langues des clients ; les experts techniques, aussi bien en cybersécurité que sur les aspects juridiques ; et enfin l'existence d'un réseau international capable de traiter les risques au niveau global, pour les clients qui ont des filiales à l'étranger », détaille Jean Bayon de la Tour.

Enfin, en cas de sinistre avéré, les courtiers assistent les clients dans la gestion des sinistres, en les aidant notamment à évaluer les pertes associées à l'incident, afin d'être le mieux indemnisés possible. « Souvent, les clients n'ont pas une idée précise de la perte qu'ils subissent », observe Ezechiel Symenouh. « Nos experts les aident à quantifier cette dernière de manière précise, afin de présenter les éléments nécessaires pour obtenir de l'assureur la meilleure indemnisation ».

UN ARTICLE RÉDIGÉ PAR
Aurélie Chandeze, Journaliste

/ STRATÉGIE

1 entreprise sur 100 seulement a une assurance couvrant les cyber-risques

Comme d'autres risques, les cyber-risques peuvent être couverts par une assurance. Mais bien peu d'entreprises ont sauté le pas.

Amanda Maréchal, souscriptrice cyber chez QBE, a expliqué le périmètre pouvant être couvert par une cyber-assurance à l'occasion d'une présentation le 10 septembre 2019.

La résilience du SI doit être approchée avec une logique de gestion du risque. Quelles sont les menaces pesant sur le SI, quelle sont les gravités et les probabilités de chacune ? Qu'est-ce qui est pertinent de faire pour contrer ces risques... ou les assumer ? Parmi les moyens pour couvrir un risque encouru, il y a le recours à l'assurance. Ce moyen est d'emploi très marginal. « 1 % des entreprises seulement ont un contrat d'assurances cyber-risques » a ainsi déploré Françoise Mari, directrice lignes financières chez l'assureur QBE, à l'occasion d'une présentation le 10 septembre 2019. Or le coût induit par les cyber-attaques ne cesse d'exploser, pouvant mettre réellement en difficultés les entreprises victimes.

Si la compagnie d'assurances elle-même couvre un risque sur le plan financier, elle s'appuie sur des partenariats avec des experts dédiés pour une assistance plus technique. Dans le cas de QBE, Inquest est proposé aux clients pour l'assistance à la gestion de crise et Sysdream pour les tests d'intrusion et la formation des collaborateurs. L'intérêt de l'assureur comme de son client est en effet que le risque ne se réalise pas. Malgré tout, les expertises et prestations menées ne sont jamais communiquées à l'assureur (comme un examen médical dans le cas d'une assurance-vie). Françoise Mari a rappelé les chiffres bien connus de l'Etude Ponemon 2018 : une intrusion est détectée en moyenne au bout de 163 jours au niveau mondial, avec une forte disparité. Ainsi, si aux Etats-Unis la durée de découverte est en moyenne de 90 jours, elle est de 175 jours en France et parfois plus de 400 en Asie.

La sauvegarde ne vous sauvera pas

Le principal type d'attaque (92 % des cas) est le classique phishing. L'arnaque au président et l'ingénierie sociale sont également devant des attaques véritablement techniques telles que le DDoS (attaque par déni de service). Les ransomwares pénètrent les systèmes en général avec la complicité involontaire des collaborateurs, simplement par mail. Il y a cependant des intrusion via des failles web ou utilisant les API de télémaintenance, avec les ouvertures béantes dans la sécurité impliquées par les autorisations accordées aux télémainteneurs. Une attaque par ransomware bien menée commence par le chiffrement des sauvegardes accessibles. Lorsque le chiffrement des données d'exploitation commence et l'attaque est détectée, les sauvegardes sont déjà inutilisables. Il reste bien sûr la possibilité de rendre physiquement inaccessibles les sauvegardes (off-lines).

Pour l'entreprise, une cyber-attaque a des conséquences financières importantes. Il s'agit d'abord du coût de réparation (logicielle et datas). Parfois, cela inclut des coûts de ressaisie. Mais le plus lourd réside probablement dans l'arrêt d'exploitation voire les atteintes à la réputation, grévant l'activité même de l'entreprise. Enfin, une atteinte à des données personnelles peut entraîner des amendes au titre du RGPD : jusqu'à 4 % du chiffre d'affaires mondial.

La cyber-assurance a son périmètre dédié

Le sujet est controversé car il existe une interdiction de couvrir une condamnation pénale par une assurance mais certaines polices couvrent les amendes administratives infligées par la CNIL. « Ce type de couverture est bien présent dans les contrats d'assurance, pour autant que ce soit légalement assurable. Nous attendons donc de voir comment cela va être traité au regard des dernières sanctions pécuniaires prononcées par la CNIL et celles à venir » a affirmé Amanda Maréchal, souscriptrice cyber chez QBE. Bien évidemment, la discrétion sur les heureux bénéficiaires comme sur les compagnies concernées est de mise. Malgré tout, l'atteinte aux données, dans le sens donné à ces termes par le RGPD, et l'atteinte au SI sont les deux grands événements déclencheurs d'une indemnisation au titre d'une cyber-assurance.

L'assurance peut également couvrir les dommages propres internes à l'entreprise comme les coûts d'investigation, le surcoût d'exploitation, la participation de personnels ou de prestataires à l'enquête officielle, la perte d'exploitation, la restauration des systèmes, les fonds versés dans le cadre d'une extorsion, les frais de communication (notamment la notification RGPD aux personnes concernées par une atteinte à leurs données). A l'inverse, certains dommages sont en principe couverts par d'autres assurances comme les dommages corporels (si la panne informatique a entraîné un dysfonctionnement qui a provoqué un accident de personne), les dommages matériels, les défaillances d'infrastructures, les transferts frauduleux de fonds (en dehors du paiement des rançons)... Comme les rapports d'expertise restent confidentiels, l'assureur va fixer une prime d'assurance en se basant sur l'activité de la société, les types de données personnelles collectées, l'organisation et la gouvernance, la sécurité du SI mise en place, l'efficacité du PRA et du PCA et les statistiques de sinistres.

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO