optimind.
manage risk, build your future

MARS
2020

LA CYBER-ASSURANCE DES PARTICULIERS.

Besoin et marché

Les dernières décennies ont vu se développer les usages informatiques et l'interconnectivité des activités, notamment au travers d'un usage massif du web. Ce développement est appelé à perdurer voire s'amplifier et, dans ce cadre, un nouveau risque se développe et prend de l'ampleur : le cyber risque.

Ce risque émergent, qui touche à la fois les particuliers et les professionnels, est complexe à prévenir et à maîtriser. Optimind vous propose à travers cette publication une vision détaillée du risque ainsi qu'un passage en revue des offres et couvertures existantes et en développement.

Publication réalisée par l'Expertise Center IARD

R&D EXPERTISE CENTER IARD

L'expertise Center IARD vise au développement de l'expertise produit (connaissance des garanties et conditions d'application) ainsi qu'au suivi des évolutions réglementaires et de marché ayant un impact direct en matière d'assurance et de réassurance non vie. Il assure une veille active sur les projets de réforme et l'innovation et mène des travaux de fond sur les problématiques majeures de tarification, de provisionnement et de pilotage de portefeuille. L'ensemble des travaux menés alimentent nos activités de *benchmark*, de communication et contribue à la formation de nos consultants aux nouveaux besoins assurantiels (assurances connectées, nouveaux objets à assurer, traitement des données récoltées en masse, risques émergents).

Le cyber risque : un risque émergent.

La naissance du « cyber risque », un malentendu

Le premier gros incident cyber mondial répertorié a eu lieu en 1988 : loin d'être une attaque cyber orchestrée, cet incident n'était même pas intentionnel.

Ce dernier a été provoqué par Robert Morris, un étudiant âgé de 23 ans, qui décida de créer un programme permettant de connaître le nombre d'ordinateurs connectés à Internet. Il a ainsi, par erreur, propagé un ver informatique qui a saturé la mémoire vive de 5 % de l'ensemble des ordinateurs connectés à Internet à l'époque. Cet incident a permis la mise en place des premiers groupes dédiés à la protection à la fois technique et légale des données et de la confidentialité.

L'assurance cyber est naturellement apparue par la suite, d'abord aux Etats-Unis au début des années 2000, puis une dizaine d'années après en France.

> *L'ancêtre de l'assurance cyber risque est l'assurance « risques informatiques » que connaissent et garantissent les assureurs depuis les années 1980, essentiellement tournée vers les attentats par usage de virus et de « bombes logiques ».*

Qu'entend-on par « cyber-risque » ?

Le cyber risque regroupe tous les risques qu'une entreprise ou un particulier peuvent encourir suite à l'usage d'un système informatique, ensemble de moyens informatiques et de télécommunication ayant pour finalité de collecter, traiter, stocker et distribuer de l'information.

Cela peut donc porter atteinte à leurs systèmes électroniques / informatiques ou à leurs données. Ce risque peut survenir à la suite d'un acte malveillant / terrorisme (hackers…), d'une erreur humaine, d'une panne, de problèmes techniques, ou d'un événement naturel ou accidentel et a pour principales conséquences :

- des dommages corporels, matériels, et/ou immatériels (frais ou pertes financières), subis par l'entité et/ou causés par l'entité à des tiers ;
- une mobilisation de ressources internes ou externes ;
- une atteinte à la réputation de l'entité.

Aujourd'hui, tout équipement contenant une puce électronique est une cible potentielle pour les pirates. Les dommages résultant du risque cyber s'apparentent à des dommages IARD : ils peuvent être matériels, financiers mais aussi corporels. Ce risque diffère toutefois des risques que les assureurs ont l'habitude de couvrir.

En effet, contrairement aux assurances auto, MRH, santé… , le risque cyber peut être provoqué volontairement, tout comme le risque terroriste. Il est donc plus difficile à prévoir que les risques « classiques » qui sont accidentels, notamment à cause du caractère prémédité de l'acte. Au-delà des statistiques, il faut comprendre pourquoi une entreprise ou un particulier sera visé, quel genre de données l'attaquant peut y trouver, quel est sa motivation (certains « hackers » attaquent des sites web et les mettent hors d'usage juste pour le challenge)…

Parmi les exemples les plus courants de risque cyber, on retrouve le « Phishing », ce fameux e-mail frauduleux qui invite le destinataire à renseigner des informations confidentielles comme ses identifiants bancaires ou le mot de passe de sa messagerie.

Autre exemple courant qui touche aussi les particuliers : la demande de rançon via les « Ransomwares », des logiciels malveillants qui infectent un ordinateur en cryptant les données de l'utilisateur et qui, en échange de la clé de décryptage, demandent une rançon[1].

Qui sont les cibles ?

Les entreprises sont évidemment très exposées au risque cyber de par l'informatisation, l'automatisation des tâches et la dématérialisation des documents, mais les États ne sont pas exclus, comme en témoigne le vol du design de systèmes d'armes américaines en 2012, ou encore la coupure électrique générale en Ukraine en 2015.

Enfin, les particuliers n'échappent pas au risque cyber et restent une cible importante de ce risque via une exposition multiple : achat sur internet, cyber extorsion, harcèlement sur internet, usurpation d'identité etc. Ce sont des cibles de choix puisque la majorité d'entre eux sous-estime le risque d'attaque et ne connaît pas les bonnes pratiques pour limiter leurs conséquences.

Les particuliers peuvent également être des victimes indirectes d'une attaque cyber - par exemple lorsqu'un pirate informatique attaque une grosse entreprise et récupère par la même occasion les données clients.

L'accès constant à internet, la digitalisation des entreprises, la démocratisation et l'accès aux nouvelles technologies ont inévitablement mené à une exposition importante à ce nouveau risque, que l'on peut qualifier de « grandissant ».

Un risque « émergent », voire « grandissant »

Le cyber risque est apparu il y a quelques années et est en progression constante.

En 2017, ce n'était pas moins de 978 millions d'utilisateurs dans le monde qui ont subis une attaque cyber ainsi que

[1] *Récemment, le logiciel malveillant « Wannacry », qui a infecté des milliers d'ordinateurs dans le monde en 2017, est un exemple de ransomware.*

172 milliards de dollars dérobés (Symantec : Norton Cyber Security Insights Report 2017).

Ces chiffres datent déjà de quelques années, et on peut imaginer aujourd'hui qu'ils soient encore plus importants. En 2025, il est estimé que ce marché de l'assurance cyber pour les particuliers atteindrait entre 1,6 et 3,1 milliards de dollars en primes cumulées partout dans le monde (Swiss Re).

On peut le qualifier de risque émergent puisque sa nature et ses impacts réels ne sont pas encore bien compris par les assureurs et les réassureurs, principalement à cause d'un manque de données historiques et de statistiques fiables.

C'est un risque qui est également « grandissant », aussi bien en termes de nombres d'attaques que d'impact : indisponibilité des systèmes d'information, coût engendrés (aussi bien en perte qu'en réparation) importants, impacts en termes d'image en cas d'attaque sur le web…

Les moyens détenus par les attaquants se démocratisent de plus en plus et sont davantage perfectionnés, une attaque est de plus en plus difficile à enrayer.

D'après une étude de PwC, les particuliers sont encore plus soucieux du risque cyber que les entreprises, puisque 60 % des français se sentent personnellement exposés, contre 17 % des entreprises !

Tout semble indiquer que ce risque va continuer de croître, avec notamment le développement de l'IoT (*Internet of Things*), où de plus en plus d'objets seront connectés à internet.

Impact quantitatif des sinistres cyber

Il est très difficile de mettre des chiffres exacts sur la fréquence ou le coût de ces sinistres, les particuliers n'ayant aucune obligation de prévenir les autorités lorsqu'ils sont victimes d'une quelconque attaque cyber. Ainsi, aucune base de données libre n'existe sur la fréquence des attaques cyber visant les particuliers en France.

Concernant la sévérité, il reste délicat d'estimer le montant des pertes consécutives à une attaque cyber, car il existe de nombreuses conséquences indirectes, surtout pour les entreprises.

Afin de contenir l'incertitude concernant ce nouveau risque, les assureurs ont mis en place une indemnisation forfaitaire pour les particuliers. Un ordre de grandeur des coûts d'attaque cyber peut alors être donné. Par exemple, les assureurs indemnisent 1 000 € en moyenne pour une attaque *ransomware* (frais de reconstitution de données), et entre 1 000 € et 5 000 € pour une atteinte à l'e-réputation (ce montant pouvant aller jusqu'à 10 000 € pour certains acteurs).

Par ailleurs, certains assureurs décident d'encapsuler des garanties cyber dans leur contrat de protection juridique générale, où les plafonds sont dans ce cas plus étendus.

Le marché de l'assurance cyber particulier.

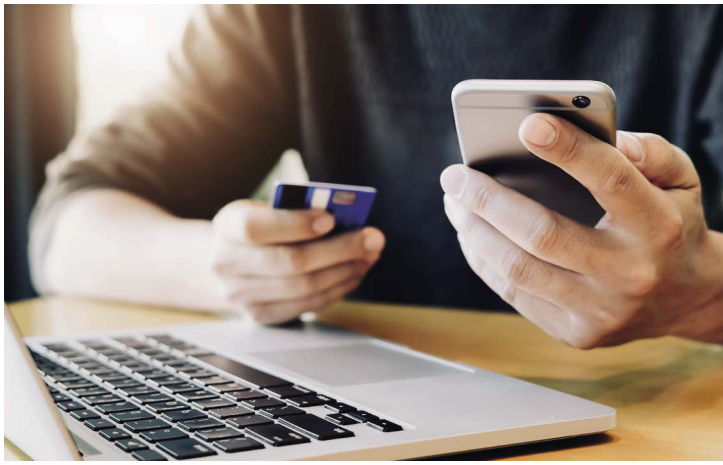
Risques cyber pour les particuliers

Les particuliers sont vulnérables à un large éventail de risques cyber. Un jargon a vu le jour afin de qualifier ces différents risques, transcrivant en même temps les différentes formes d'attaques observées.

Le *Phishing* et les *Ransomwares*[2] ont déjà été évoqué, et sont les principales attaques auxquelles les particuliers sont confrontés, mais il en existe bien d'autres : de nouvelles méthodes d'attaques apparaissent constamment.

Parmi les risques les plus fréquents, on retrouve :

- les dommages aux biens : dommages matériels d'appareils informatiques ;
- la fraude téléphonique : la surfacturation téléphonique suite au rappel d'un numéro payant ;
- l'atteinte à l'image : fausses rumeurs sur internet… ;
- la réputation sur internet : par exemple avec la diffusion de photos compromettantes sur les réseaux sociaux ;
- le détournement de fonds : l'introduction frauduleuse dans un système informatique dans le but de dérober des fonds ou valeurs ;
- la perte de données personnelles.



[2] *Virus de demande de rançon.*

Risque cyber	Exemple	Coût moyen
Phishing	Un faux e-mail de banque.	NC
Ransomwares	Un fichier téléchargé sur internet contient un virus *ransomware*.	15 000 €
Dommages aux biens	La détérioration de matériel informatique suite à une panne.	Entre 30 et 60 € pour la suppression de virus 100 € pour la récupération de données Entre 80 et 100 € pour le remplacement de la carte mère Coût moyen : 50 €/h
Fraude téléphonique	Un numéro payant appelle en demandant de le rappeler par la suite.	Surfacturation du type 3 € par appel + 3 € la minute par un numéro qui force à le rappeler
Atteinte à l'image	Faux compte de réseau social avec la photo de la victime.	2 229 € en moyenne pour une usurpation d'identité sur internet
Réputation sur internet	Photos compromettantes sur les réseaux sociaux.	Minimum 100 € pour la suppression d'un lien (entre 100 et 200 €/h)
Détournement de fonds	Utilisation frauduleuse du compte bancaire internet.	75 € en moyenne : 440 millions € pour la fraude à la carte bancaire en 2018 pour 6 millions de fraude (Observatoire de la sécurité des moyens de paiement)
Perte de données personnelles	Défaillance du système de Cloud.	NC

Mise en œuvre des assurances cyber

Pour pouvoir assurer un risque, l'assureur doit calculer la probabilité qu'un événement lié à ce risque se produise et quantifier son impact. La survenance de cet événement doit être licite, futur, indépendant de la volonté des parties et aléatoire.

Dans le cas du risque cyber en France, peu de données publiques existent et une évaluation de ce risque et donc la tarification d'un produit d'assurance s'appuient sur différents modèles basés sur des jugements d'experts juridiques et techniques.

Certains acteurs ont même décidé de s'associer avec des entreprises spécialisées en sécurité informatique afin de mettre en œuvre des assurances cyber dédiées.

La mise à découvert des garanties silencieuses liées au cyber risque

De par son caractère « récent », le risque cyber n'avait pas été anticipé dans les contrats d'assurance conçus avant l'accroissement de ce risque cyber et la création de contrats spécifiques. De ce fait, certains contrats d'assurance peuvent déjà couvrir en théorie des conséquences dommageables d'un cyber-risque.

C'est ce que l'on appelle « les garanties silencieuses » : une garantie qui n'avait pas été conçu à l'origine pour couvrir un sinistre cyber, mais que l'assuré peut déclencher dans la mesure où aucune exclusion explicite au cyber risque ne s'y applique.

Parmi les contrats présentant des garanties silencieuses, les contrats dommages aux biens se retrouvent en première ligne. Ils peuvent être déclenchés lorsqu'un incident cyber, qu'il soit malveillant ou accidentel, provoque des dommages matériels. Ces dommages et la perte d'exploitation associée sont indemnisés par ce type de contrat.

D'autres contrats contiennent également ce type de « garanties silencieuses », comme le contrat responsabilité civile, le contrat responsabilité des dirigeants, et le contrat fraude (les deux derniers sont typés pro).

Dans les contrats responsabilités civiles sont inclus les dommages matériels et immatériels causés aux tiers, mais également les frais de défense, entrants en jeu pour une entreprise subissant une fuite de données par exemple.

Le contrat responsabilité des dirigeants va quant à lui couvrir le dirigeant en cas d'attaque cyber envers l'entreprise. Les fuites de données qu'avaient subies Uber (2016) et Yahoo (2013 et 2014) ont permis le déclenchement de leurs contrats responsabilité des dirigeants (même s'ils avaient également une assurance cyber dédiée, des garanties silencieuses étaient présentes dans leur contrat classique et la demande d'indemnisation a pu être faite).

Enfin, les contrats fraudes vont couvrir toutes les fraudes qui sont assistées par ordinateur (faux ordre de virement, usurpation d'identité…). Les fraudes issues d'un logiciel malveillant pourront être couvertes à la fois par le contrat fraude et le contrat spécifique cyber.

Bien évidemment, l'assuré n'a pas vocation à s'enrichir en faisant appel aux garanties présentes dans ses différents contrats et/ou faisant appel à différents acteurs.

Prise de conscience des assureurs et modification des CG des contrats avec des exclusions explicites

Face à un sinistre cyber, les particuliers qui n'ont pas souscrit à un contrat d'assurance spécifique peuvent alors déclencher des garanties silencieuses.

Un assureur ne souhaitant pas développer sa gamme de contrat cyber dans l'immédiat est donc contraint d'ajuster les Conditions Générales de ses contrats existants pour se prémunir d'une sur-sinistralité liée à un risque qu'il n'avait pas anticipé.

En effet, le tarif de ces contrats n'étant pas calculé en tenant compte du risque cyber, les assureurs pourraient faire face à un problème de demandes d'indemnisation qu'ils ne sont certainement pas en mesure de supporter pour conserver un produit rentable.

Selon une étude de l'agence de notation Moody's Investors Service sur la cyberassurance, l'évaluation de la cyberexposition assurée est compliquée. Les assureurs doivent faire le tri entre garanties cyber dédiées ou intégrées dans les polices d'assurances multirisques traditionnelles. Ces derniers travaillent notamment à créer un inventaire des polices traditionnelles avec risques cyber intégrés.

Les compagnies ont déjà commencé à s'organiser, comme Allianz qui a annoncé avoir pris des mesures contre les garanties silencieuses, ou le régulateur britannique qui a demandé aux assureurs d'élaborer des plans d'actions.

Les assureurs devront envisager tous les cas probables d'attaques cyber et passer en revue tous leurs contrats existants pour savoir si ces risques y sont inclus ou non : des causes d'exclusion explicites devront être mises en place le cas échéant (ce qui n'aura pas d'impact sur le tarif du contrat qui n'a pas été prévu pour couvrir ces risques cyber). Cette nécessité devient d'autant plus urgente avec la hausse des objets connectés, qui créent de nouveaux risques et donc de nouvelles garanties silencieuses, sachant que le niveau de sécurité de ces objets est en général faible et qu'ils sont une porte d'accès facile au Système Informatique.

À titre d'exemple, concernant les serrures connectées, les interrogations suivantes peuvent être soulevées : un contrat MRH couvre-t-il un cambriolage par piratage de ce type de serrure ?

Au-delà de ce travail d'exclusion des risques cyber dans leurs polices classiques, ces derniers ne devraient pas rater l'opportunité d'ouvrir le marché du cyber risque : certains acteurs ont d'ores et déjà mis en place des produits spécifiques pour couvrir le cyber risque.

Assurance spécialisée cyber risques : existant et perspectives du marché.

Le marché français

Le marché de l'assurance cyber pour les particuliers est en plein essor. Avec des offres de plus en plus ajustées au besoin, un peu moins de 10 acteurs proposent des contrats cyber qui présentent des garanties ajustables.

Les garanties les plus souvent retrouvées sont l'atteinte à l'e-réputation, l'atteinte aux systèmes d'information, l'usurpation d'identité et la bonne livraison des achats en ligne.

Cependant, il existe des différences importantes entre les contrats concernant les moyens mis en place pour contrer l'attaque mais également les plafonds et les montants forfaitaires applicables :

Garantie proposée	Action de remédiation	Plafond / Montant forfaitaire
Atteinte à l'e-réputation	▸ Nettoyage et noyage des informations préjudiciables par une entreprise spécialisée ▸ Soutien psychologique ▸ Aide et protection juridique	AXA ▸ 5 000 € par litige (1 000 € pour le noyage) ▸ 1 000 € pour l'aide à la résolution (10 000 € pour un litige non amiable) ▸ 3 consultations psychologiques Cofinoga Par litige et par an : ▸ 530 € plafond amiable ▸ 10 000 € plafond judiciaire ▸ 2 000 € noyage/nettoyage (1000 € pour le nettoyage) Sofinco ▸ 1 500 € TTC / an (dont 1 000 € pour le noyage)
Atteinte aux systèmes d'information	▸ Frais de reconstitution de données ▸ Frais d'expertise informatique ▸ Aide et protection juridique	Reconstitution des données : 1 000 € (MAIF)
Usurpation d'identité	▸ Indemnisation du préjudice financier ▸ Soutien psychologique ▸ Aide et protection juridique	Préjudice financier : 3 000 € par an par sinistre (ADLP assurances)
Achats en ligne	▸ Remboursement en cas de non livraison ou de livraison non conforme ▸ Aide et protection juridique	Préjudice : 200 € (Kelip's assurances)
Fraude téléphonique	▸ Remboursement de la surfacturation téléphonique	30 €/mois (Sofinco)

Comme toutes polices d'assurances, les assurances cyber s'accompagnent de leur lot d'exclusions. Par exemple, on retrouve souvent l'exclusion de l'indemnisation des dommages matériels (...). En cas de demande de rançon via un *Ransomware*, certains acteurs considèrent illégal le fait de rembourser le paiement de cette rançon à l'assuré, puisque celle-ci participe au cyber-crime. En revanche les frais de reconstitution du système et des données suite à ce virus sont indemnisés. D'autres exclusions plus spécifiques existent, comme l'atteinte à l'e-réputation pour les journalistes qui n'est pas couverte.

Côté tarif, il faudra - à priori - compter une dizaine d'euros par mois en moyenne pour être assuré contre le cyber risque avec des offres à partir de 7 €/mois.

Le marché mondial

L'Amérique du Nord - et particulièrement les États-Unis, qui détenaient 90 % des primes en 2014 - domine le marché de la cyber assurance, juste devant l'Europe. La part de marché de la zone Asie-Pacifique reste limitée, les primes cumulées dans la région s'élevant à 50 millions de dollars[3] en 2017. Ce chiffre concernant l'assurance des entreprises devrait augmenter significativement dans les années à venir.

Une étude de Swiss Re évaluait, en 2018, les primes cumulées des assurances cyber dédiées dans le monde à 4 milliards de dollars, et prévoyait le chiffre de 7,5 milliards de dollars pour 2020. Le marché des assurances cyber spécifiques aux particuliers devrait naturellement suivre cette tendance : Swiss Re suggère que ce marché grimpe à environ 500 millions de dollars pour 2020, et entre 1,6 et 3,1 milliards de dollars pour 2025.

Les garanties proposées à l'international ne sont pas significativement différentes de celles que l'on peut trouver en France. Cependant, dans certains pays, le marché des assurances cyber y semble plus avancé : les polices sont plus ciblées, comme par exemple des assurances pour les agriculteurs et tout le système informatique de leur ferme (HSB MunichRe), et sont plus adaptées à l'ensemble du foyer (pack famille, protection pour la maison connectée...). Il existe également beaucoup plus de garanties pour la protection du compte bancaire en ligne, notamment chez Allianz Suisse et Delta Insurance en Nouvelle-Zélande.

Aux États-Unis, le marché est largement plus développé et les assureurs sont prêts à supporter un risque plus important moyennant une prime en ce sens. Par exemple concernant les plafonds de garanties, Chubb propose une indemnisation contre le cyber-harcèlement à hauteur de 250K$, contre 3K€ en France.

D'ailleurs, CHUBB propose aux particuliers souscrivant à leur contrat cyber une réduction pour un service d'assistance qui permet de sécuriser son réseau informatique, concept que l'on ne retrouve pas ou peu en France.

Concernant les chiffres sur les primes d'assurances, on observe aux Etats-Unis chez AIG, Chubb et PURE, trois assureurs bien implantés dans ce marché, des tarifs allant de 127$ à plus de 1 500$ par an, selon les garanties.

Quant aux similarités, on retrouve dans certains pays des couvertures pour les pertes de données personnelles (frais de restauration des données), la cyber extorsion (attaque par *ransomwares*), l'usurpation d'identité, le cyber-harcèlement, mais aussi des garanties de responsabilité civile, d'indemnisation en cas de fraudes informatiques et de litige pour les achats en ligne.

[3] *https://techwireasia.com/2019/02/why-cyber-insurance-market-set-to-surge-in-the-apac/*

Perspectives d'évolutions du marché

Outre le fait de connaître l'état actuel du marché cyber pour les particuliers, la véritable question reste d'être en mesure d'anticiper son évolution potentielle.

Une étude de PwC menée en 2015 montre bien qu'il s'agit d'un marché d'avenir : même si seulement 6 % des français sont couverts par une assurance dédiée au cyber risque, cette étude souligne que 60 % des français se sentent exposés au risque de cybercriminalité, et 88 % pensent que le risque d'exposition va augmenter d'ici 2 ans. 64 % de la population se disaient prêts à souscrire à ce type d'assurance.

Ces chiffres montrent une réelle prise de conscience du risque cyber par les particuliers, et que le marché de la cyber assurance pour les particuliers est très prometteur. Le rôle des assureurs va alors être d'une part, de clarifier leur police d'assurance cyber pour mieux cibler la demande, mais également de les démocratiser.

En effet, la France ne dispose pas encore d'offre du type « Family pack », ni de réduction dans le cas où des bonnes pratiques sont respectées (antivirus à jour, changement de mot de passe fréquent…) comme ce que l'on retrouve dans les polices d'assurances auto connectées.

Un nouveau mode de distribution des produits cyber pourrait être également prévu, à l'aide de partenariat avec les fournisseurs de matériel informatique (Darty, Boulanger, etc.), qui, tout comme les concessionnaires automobiles le font aujourd'hui, proposeraient à leurs clients une assurance cyber lors de l'achat du produit.

Ces évolutions possibles de l'offre permettraient une réelle progression du marché français, déjà en plein essor, d'autant plus que les français sont une population connectée : 88 % d'entre eux ont accès à internet, 58 % sont des utilisateurs actifs de réseaux sociaux, et ils adoptent de plus en plus les objets connectés : plus de 5 millions de produits se sont vendus en 2017.

Cette caractéristique de l'environnement en France, ainsi que la mise en application du RGPD qui améliore la façon de traiter les données personnelles au sein des entreprises et prévoit des sanctions en cas de vol des données pouvant donner lieu à divulgation de leur contenu, vont modifier le marché. Le renforcement de la réglementation va inciter les entreprises à s'assurer, et une base de données répertoriant les notifications d'attaques pourrait améliorer la connaissance des assureurs à propos de ce risque.

L'évolution constante des nouvelles technologies et de nos habitudes vis-à-vis d'elles font que ce marché de la cyber-assurance est en changement permanent. Par exemple avec l'augmentation du harcèlement en ligne, qui a doublé entre 2016 et 2018, et qui peut s'expliquer par la croissance de l'utilisation des réseaux sociaux.

À noter que des risques qui existaient déjà avant s'adaptent à ces nouvelles technologies, comme l'usurpation d'identité. Chaque individu peut alors subir une atteinte à l'e-réputation, même ceux n'ayant aucun accès à internet.

La vie professionnelle peut également se mêler avec la vie personnelle du particulier, ce qui accentue leur exposition.

Au-delà du ciblage de la clientèle, les assureurs doivent adopter une logique de *Servicing* pour les clients voulant s'assurer contre le risque cyber. En effet, ceux-ci n'ont pas seulement besoin d'indemnisation, mais également d'un accompagnement pour prévenir et gérer la situation délicate d'une attaque cyber.

Hiscox, l'un des leaders de marché, s'est par exemple associé à Provadys et Neotech, deux entreprises spécialistes en cyber risque, pour étendre ses services de cyber-assurance, mais aussi de prévention et accompagnement et de cyber-résilience (cellule de crise) aux laboratoires de biologie médicale.

De même, le partenariat Apple, Cisco, Allianz, Aon permet aux entreprises un service de « Cyber Risk Management » en plus d'une solution assurantielle.

La sensibilisation des clients est aussi un point clé de l'évolution de l'offre, à travers des sessions de *e-learning*, des audits préventifs, avec une communication différenciée selon les segments.

L'assureur n'est donc plus qu'un simple assureur dans ce domaine, mais également un prestataire de service de prévention et de gestion du risque (via des partenariats avec des sociétés spécialisés).

Enfin, la progression du marché de la cyber-assurance dépend à la fois des assureurs et des réassureurs : tant qu'il n'y aura pas d'offres matures de réassurance dans le domaine, les assureurs ne pourront pas se développer à grande échelle.

Conclusion.

Le cyber risque est un risque qui préoccupe : assureurs, professionnels et particuliers y sont exposés. Avec un nombre d'attaque fortement croissant, le caractère migrant du type d'attaques et leur diversité en fait un risque difficile à appréhender. Aujourd'hui, force est de constater que le marché de l'assurance cyber des particuliers se développe, répondant à une demande croissante de protection des assurés. De nouvelles offres ne devraient pas tarder à voir le jour, s'adaptant ainsi de manière toujours plus ciblée au nouveau visage de ce risque.

optimind.
manage risk, build your future

Optimind, acteur indépendant leader du conseil en gestion des risques, réalise 35 millions d'euros de chiffre d'affaires et réunit plus de 250 collaborateurs autour de cinq practices : Actuarial & Financial Services, Corporate Risk Services, Risk Management, Business Transformation, Business Process Outsourcing.
Optimind accompagne les organismes assureurs, banques et grandes entreprises autour de la définition de la stratégie, de la gestion des risques et de la transformation. Les services proposés couvrent chaque maillon de la chaîne de valeur des clients d'Optimind : Strategy, Finance, Risk, Compliance, Market, Human Resources, Digital Transformation, Data, BPO.

optimind.com

Strategy
Finance
Risk I
Compliance
Human resources
Digital transformation
Market I
DATA
Business Process Outsourcing

Contacts.

Practice Actuarial & Financial Services

Gildas Robert - senior partner - gildas.robert@optimind.com
Julien Chartier - partner - julien.chartier@optimind.com
Valérie Deppe - partner - valerie.deppe@optimind.com
Marie-Catherine Sarraudy - partner - marie-catherine.sarraudy@optimind.com

Presse

Marine de Pallières - Communication & Public Relations Manager - **marine.depallieres@optimind.com**