La cyber-assurance, un marché en plein essor. Êtes-vous bien couvert ?

État des lieux

Chaque année, le cybercrime coûterait plus de 600 milliards de dollars à l'économie mondiale[1]. Et la tendance n'est pas près de s'essouffler. À l'heure où la transformation numérique bat son plein, les cybermenaces ne cessent de se complexifier. Pour ne rien arranger, les services cloud, l'Internet des objets et une myriade de terminaux mobiles viennent élargir la surface d'attaque d'entreprises de plus en plus dépendantes des interconnexions entre ces systèmes. Une aubaine pour des hackers de plus en plus habiles dans l'exploitation des vulnérabilités réseaux et logicielles. Incidents de sécurité de grande ampleur, obligation de signalement des violations de données, règlement général européen sur la protection des données (RGPD)... de nombreux facteurs placent désormais les polices de cyber-assurance sous le feu des projecteurs. Selon l'OCDE, le coût du cybercrime devrait atteindre 2 000 milliards de dollars d'ici 2019. Rien d'étonnant donc à ce que les entreprises tiennent à se protéger.

« Lutter contre le cybercrime est un combat coûteux, complexe et de longue haleine. Malgré les parallèles souvent établis avec le terrorisme ou les catastrophes naturelles, le cyber-risque présente ses propres spécificités en matière d'assurance. »

Insurance 2020 & beyond: Reaping the dividends of cyber resilience, PwC

Résultat : la demande de cyber-assurances croît à un tel rythme que le marché mondial des polices souscrites devrait peser pas moins de 14 milliards de dollars d'ici 2022[2]. Toutefois, ce marché n'en est encore qu'à ses balbutiements en raison d'une adoption relativement poussive dans certains pays, en particulier sur le segment des petites entreprises. Pour preuve, selon un rapport récent, 62 % des entreprises mondiales n'ont pas encore contracté de police de cyber-assurance dédiée[3].

Comme pour n'importe quel type de risque, les entreprises cherchent généralement à réduire leur exposition financière en cas de cyber-attaque. Pour cela, elles se tournent tout naturellement vers la cyber-assurance. Mais de leur côté, les assureurs sont de moins en moins disposés à appliquer des conditions contractuelles généralistes. En ce sens, ils exigent de l'assuré un diagnostic bien plus approfondi de ses vulnérabilités, processus, solutions de réduction des risques et plans de réponse à incident.

Ce document vous invite à faire le point sur le marché de la cyber-assurance et le besoin de compétences ad-hoc, avant d'aborder les différentes étapes du bilan des risques et vulnérabilités que les entreprises devront établir avant de souscrire un contrat d'assurance.

Un champ de menaces complexe

Les cybercriminels découvrent sans cesse de nouvelles techniques d'exploitation des vulnérabilités. Malgré tous les efforts déployés pour garder un coup d'avance sur les attaquants, les chercheurs et les entreprises ne pourront jamais prévenir toutes les attaques.

« D'ici fin 2020, 99 % des vulnérabilités exploitées continueront d'être des failles connues des professionnels IT et sécurité au moment de l'incident. »

Gartner

Aujourd'hui, l'innovation technologique est constamment prise de vitesse par l'ingéniosité des cybercriminels. Face à ce constat, de nombreuses entreprises souscrivent des contrats de cyber-assurance pour transférer les risques financiers d'une telle attaque. De leur côté, les assureurs sont tenus d'offrir des polices qu'ils pourront garantir, tout en remplissant leur devoir de conseil.

Le marché de la cyber-assurance se développe. Il représenterait même l'un des rares leviers de croissance et d'innovation dans ce secteur[4]. Mais avec des niveaux de maturité très variables à travers le monde, il reste encore relativement sous-exploité. Il n'existe d'ailleurs aucune approche standard de

1. Economic Impact of Cybercrime — No Slowing Down, McAfee et CSIS (Center for Strategic and International Studies) *2. Global Cyber Insurance Market Report, Allied Market Research*
3,7. Rapport Risk:Value 2018, NTT Security *4. Cyber security insurance – how can insurers quantify the risk?, PwC*

couverture des cyber-risques. Ainsi, au niveau mondial, 9 cyber-assurances sur 10 sont contractées par des entreprises basées aux États-Unis[5], tandis que seules 2 % des sociétés britanniques ont souscrit un contrat spécifique de cyber-assurance.

La cyber-assurance constitue également un terrain miné par de multiples ambiguïtés. En effet, certains assureurs peuvent refuser des indemnisations sur la base de clauses obscures et d'une interprétation complexe des contrats. Une information erronée peut invalider un contrat, comme le prouvent les nombreux dossiers d'indemnisation rejetés sur cette base.

Une entreprise doit prouver à son assureur que des mesures de protection ont été prises – dans une double optique d'évaluation et de réduction des risques – et qu'un système de Threat Intelligence et un plan de réponse à incident sont également en place. Seules ces informations permettront à l'assureur de bien cerner le niveau d'exposition du client.

Les entreprises qui envisagent de souscrire un contrat de cyber-assurance devraient tout d'abord s'interroger sur leurs besoins spécifiques. Comment choisir une couverture adaptée ? Existe-t-il un risque d'invalidation du contrat ? Quels sont les dispositifs de protection de l'information qu'exigent les assureurs ? Autant de questions auxquelles elles devront répondre.

Conclusions du rapport Risk:Value 2018

- Un tiers des sondés ne s'attendent pas à subir une compromission de leur environnement
- 47 % affirment que leur entreprise n'a jamais été compromise
- 62 % des entreprises n'ont pas encore contracté de police de cyber-assurance dédiée
- 22 % sont couvertes uniquement pour la perte de données

Les entreprises participantes ayant contracté une cyber-assurance pensent que divers éléments pourraient invalider leur police :

- Un défaut de maintenance ou de mise à jour de leurs systèmes (47 %)
- L'absence d'un plan de réponse à incident (36 %)
- Une inattention ou négligence des salariés (29 %)

Émergence des audits de cyber-résilience

Récemment, un groupe d'entreprises s'est associé pour proposer une cyber-assurance à couverture renforcée en conjonction avec des technologies Apple et Cisco sécurisées. L'offre comprend également un audit de cyber-résilience effectué par le cabinet londonien Aon. Une fois cet audit réalisé, les clients qui déploient les matériels et technologies préconisés pourront souscrire une police d'Allianz à des conditions plus avantageuses, notamment en matière de franchise. Cette initiative très intéressante soulève cependant un certain nombre de questions quant à l'orientation que pourrait prendre le marché des assurances.

En effet, si ce type de couvertures "améliorées" devenait la norme, les assureurs seraient-ils alors en droit d'imposer des fournisseurs de sécurité bien particuliers ? Qu'adviendrait-il de vos obligations contractuelles vis-à-vis de vos fournisseurs existants ? Et si les assureurs devaient imposer leur propre équipe de réponse à incident, cette dernière serait-elle aussi performante que votre partenaire existant ?

Chaque clause compte

Actuellement, ces offres groupées font figure d'exception. Compte tenu de la complexité des polices proposées sur le marché, il est essentiel de faire appel à un spécialiste pour décortiquer ensemble lesdits contrats avant de s'engager.

Bien des entreprises souscrivent des contrats de cyber-assurance sans les analyser dans le détail. Elles les signent sans véritablement passer en revue l'offre disponible, les coûts et les couvertures proposées. Par ailleurs, les clauses de ces contrats ne sont encore soumises à aucune règlementation ni aucune norme sectorielle. Très variables dans leur contenu, les polices ont déjà donné lieu à des désaccords sur la recevabilité des demandes d'indemnisation dont certains médias se sont faits l'écho – les compagnies d'assurance invoquant à cet effet certaines clauses obscures des contrats.

Le contrat couvre-t-il les données hébergées par un tiers ou dans le cloud ? Votre entreprise sera-t-elle indemnisée même si elle n'a pas appliqué tous les correctifs de sécurité ? Des accès d'anciens salariés non révoqués invalideraient-ils votre police ? Votre entreprise est-elle protégée si la violation de sécurité provient de l'appareil personnel de l'un de vos collaborateurs ? Que se passe-t-il si la compromission est antérieure à la date de souscription de l'assurance ? Une étude NTT Security[6] révèle que près de 21 % des vulnérabilités détectées sur les réseaux clients remontaient à plus de trois ans, et plus de 5 % à plus de 10 ans.

Soyons clairs : aucune police ne vous couvrira à 100 %. En cas de doutes sur certaines clauses de votre contrat, demandez conseil à un juriste.

« Aucun contrat d'assurance ne protègera jamais la marque ou la réputation d'une entreprise. »

Garry Sidaway, VP senior Security Strategy & Alliances, NTT Security

Protéger son entreprise est essentiel… mais qui en a la responsabilité ?

Au lieu de tout miser sur l'assurance, les entreprises doivent aborder le problème différemment. Certes, il est essentiel pour elles de souscrire une assurance pour couvrir une partie des pertes. Mais elles doivent en même temps prendre des mesures visant à réduire les risques. Nombre d'entreprises considèrent que cette responsabilité relève du service IT. Pourtant, le rapport Risk:Value 2018 de NTT Security révèle qu'aucun rôle exécutif n'assume formellement cette charge. Après tout, la sécurité informatique n'est pas qu'une question de matériels et de logiciels. Elle doit faire partie intégrante de la culture de l'entreprise et être relayée à chaque échelon de la pyramide : défendue par le PDG, mise en œuvre par le RSSI, et communiquée à tous les salariés de manière à les responsabiliser sur les bonnes pratiques à adopter. Là encore, selon notre rapport Risk:Value 2018, 61 % des collaborateurs n'auraient qu'une connaissance partielle de la politique de sécurité de l'information de leur entreprise. Et si votre entreprise fait appel aux services de sous-traitants et de fournisseurs externes, vous devrez leur donner des directives claires pour qu'ils adhèrent à vos politiques et pratiques de sécurité.

Vous n'éliminerez jamais totalement la probabilité d'un incident imputable à un tiers, mais vous devrez faire en sorte que toutes les parties concernées soient conscientes de leurs responsabilités.

Votre police d'assurance : un choix réfléchi

Petites ou grandes, toutes les entreprises dépendent, dans une certaine mesure, de leur infrastructure informatique. À tel point qu'en cas de panne ou d'immobilisation de leurs systèmes, elles

5. Insurance 2020 & beyond: Reaping the dividends of cyber resilience, PwC *6. NTT Security Global Threat Intelligence Report 2017*

s'exposent à des risques d'interruption de leur activité, de perte de revenus, de chute du cours de leur action et d'atteinte à leur image de marque. Malgré cela, les entreprises ne s'assurent pas correctement contre les attaques. Ainsi, ces dernières années, le refus de certains assureurs d'indemniser des clients dans le cadre de contrats usuels a donné lieu à un certain nombre de procès retentissants. Dans ces litiges, les tribunaux se sont la plupart du temps rangés du côté des assureurs. Les contrats d'indemnisation professionnelle ne proposent généralement pas le même niveau de couverture qu'une cyber-assurance, qui prévoit à la fois une protection contre le manque à gagner et un accompagnement dans la gestion de crise (RP, conseil juridique, experts forensiques, spécialistes informatiques) en vue de réduire l'impact de l'intrusion. Et ne vous imaginez surtout pas que votre contrat en responsabilité civile couvrira l'ensemble des coûts d'une violation de données : cela ne sera vraisemblablement pas le cas.

D'après nos données, 67 % des demandes d'indemnisation en cyber-assurance en 2017 concernaient des erreurs humaines.

Hiscox

Évaluation de votre exposition aux risques

Pour les assureurs, il est essentiel que leurs clients connaissent parfaitement leur exposition aux risques. Sans cela, il leur est impossible d'établir un contrat adapté à votre entreprise. Or, d'après les résultats de notre dernière enquête mondiale, seules 57 % des entreprises ont déjà mis en place une politique de sécurité de l'information.

Pour protéger la vôtre, vous devrez d'abord prendre l'entière mesure de votre exposition aux risques, à tous les niveaux de votre structure. Il vous faudra pour cela vous appuyer sur un ensemble de bonnes pratiques sectorielles. Dans un contexte de pénurie mondiale de compétences en cybersécurité, n'hésitez pas à demander conseil à un expert externe qui pourra dresser un bilan-risque exhaustif de votre entreprise : détection des zones à risques, recommandations, priorisation des actions, élaboration d'un plan stratégique de gestion continue du risque, etc. Ce bilan vous permettra d'identifier les faiblesses de votre dispositif de sécurité informatique, tout en mettant l'accent sur les points critiques nécessitant une attention immédiate. Il établira également un calendrier de mise en œuvre des actions correctrices requises, que vous pourrez communiquer à votre assureur comme preuve de votre sérieux sur les questions de sécurité.

Bonnes pratiques de protection contre le cybercrime

1. **Connaissance des risques** – Procédez à un bilan-risque annuel pour réévaluer votre exposition aux risques. Poursuivez vos actions de sensibilisation auprès de vos dirigeants pour maintenir le cyber-risque au rang de leurs priorités.
2. **Élimination des vulnérabilités connues** – Assurez la mise à jour régulière des matériels et des logiciels de sécurité, car c'est à force de persévérance que le cybercriminel atteint son but. Maintenez l'efficacité des protections de base.
3. **Télétravail et mobilité** – Définissez des règles strictes d'accès aux données. À mesure que les appareils personnels investissent la sphère professionnelle, vous devez protéger votre réseau indépendamment du périphérique d'accès.
4. **Sensibilisation et formation** – Formez vos salariés aux politiques et procédures d'intervention en déployant un programme de sensibilisation complet : campagnes d'affichage, conseils par e-mails, consignes de sécurité pour les nouveaux collaborateurs et formations annuelles sur ordinateurs.
5. **Gestion des incidents** – Établissez, exécutez et testez régulièrement vos plans de réponse.
6. **Monitoring** – Surveillez en permanence tous les systèmes d'information et de communication, ainsi que les journaux associés, pour détecter et neutraliser d'éventuelles attaques.
7. **Sécurisation du réseau** – Gérez le périmètre du réseau et filtrez les accès non autorisés.
8. **Protection anti-malware** – Établissez des défenses anti-malware et effectuez en permanence des analyses de détection.
9. **Gestion des privilèges des utilisateurs** – Limitez les privilèges des utilisateurs et surveillez leurs activités.
10. **Établissement d'un règlement intérieur pour l'utilisation des réseaux sociaux** – Les réseaux sociaux deviennent peu à peu l'un des principaux vecteurs du cybercrime. Sensibilisez vos collaborateurs aux règles de base d'une utilisation professionnelle acceptable et à des comportements responsables hors du travail.
11. **Diagnostics de sécurité** – Au moment d'acquérir les produits ou services de vos fournisseurs, puis au moins une fois par an, vérifiez leur respect de vos politiques internes et des obligations légales et réglementaires en vigueur.
12. **Définition et maintenance d'un processus de gestion des risques** – Si possible, adoptez une norme reconnue sur le plan international.

Prêt pour la cyber-assurance ?

Les tests de vos dispositifs de protection doivent évoluer au rythme des menaces. En effet, la souscription d'un contrat de cyber-assurance ne vous dispense aucunement de veiller à la protection de votre entreprise. Après tout, vous ne quittez jamais votre domicile sans verrouiller les portes et les fenêtres, sous prétexte que vous êtes assuré.

L'important est de cerner l'exposition aux risques de votre entreprise et de mettre en place un plan de réponse à incident. Dans son rapport annuel sur le sujet, l'assureur Hiscox a évalué la qualité des stratégies cyber de plusieurs entreprises pour mesurer leur degré de préparation aux cyberattaques. Résultat : près des trois quarts d'entre elles étaient classées dans la catégorie des « cyber-débutants ». Il leur reste donc énormément de chemin à parcourir. Pire, seulement 11 % des entreprises évaluées ont été reconnues comme « expertes ».

Pour dresser un tableau complet de votre exposition aux risques, vous devez faire l'inventaire de vos faiblesses aux niveaux de vos processus, de vos collaborateurs et de vos technologies. C'est là une première étape indispensable pour mieux vous préparer et entamer un dialogue constructif avec un cyber-assureur.

Soyez proactif

Jamais les risques d'attaques ne diminueront. Leur fréquence et leur sophistication sont au contraire appelées à s'intensifier.

Ingénierie sociale, APT, phishing, attaques perpétrées via les réseaux sociaux… des menaces en tout genre continuent de cibler les entreprises. Cependant, l'exploitation de vulnérabilités connues reste la cause racine de la plupart des violations de sécurité. D'après les estimations du Gartner, les failles zero-day sont à l'origine de seulement 0,4 % de toutes les attaques de ces dix dernières années. D'ici fin 2020, 99 % des vulnérabilités exploitées continueront d'être des failles connues des professionnels IT et sécurité au moment de l'incident.

D'où l'importance d'une application proactive des correctifs. Vous éliminerez ainsi la principale cause d'intrusion et de perte de données, et montrerez aux assureurs que votre entreprise sait s'y prendre pour prévenir et réduire les risques.

En souscrivant un contrat de cyber-assurance, vous transférez les risques et, au final, réduisez le coût d'une éventuelle attaque. Malgré tout, la garantie de ces contrats reste un défi pour les assureurs. C'est pourquoi les entreprises souscriptrices doivent faire tout leur possible pour déterminer leur exposition et prendre les mesures nécessaires pour limiter les risques. Elles démontreront ainsi que la sécurité de l'information et la gestion des risques font partie de leurs priorités.

Conclusion

Souscrire une assurance ne dispense pas de rester vigilant. C'est en substance le message qu'envoient les assureurs en excluant de leur couverture des scénarios à fort impact mais facilement évitables. Comme pour les assurances habitation, protection rime d'abord avec prévention. Lorsque vous quittez votre domicile, vous activez l'alarme et placez vos appareils électroniques et autres objets de valeur à l'abri des regards indiscrets.

De la même manière, une entreprise avisée mettra en place un dispositif de sécurité associant contrôles technologiques et contrôles des processus, sans oublier de former correctement ses équipes pour mieux lutter contre les violations de sécurité. La souscription d'un contrat d'assurance s'inscrira en complément – et non en remplacement – de ce programme de sécurité.

Les entreprises se doivent d'investir d'une part dans la protection de leurs ressources, et d'autre part dans le transfert des risques via une cyber-assurance adaptée en cas d'attaque. Ces exigences vont de pair, car il est primordial de mettre en place un dispositif préventif avant de souscrire un contrat.

Par ailleurs, il est sans doute temps pour les assureurs, les experts et les entreprises victimes de collaborer davantage. Compte tenu du caractère sensible de l'information, les assureurs hésitent souvent à communiquer sur leurs historiques d'incidents et leurs mesures de sécurité. Malheureusement, cette culture du secret freine le progrès et empêche les assureurs d'optimiser leur offre, et ce aux dépens de tous.

Les entreprises qui souhaitent transférer certains des risques de violation de sécurité se tourneront de plus en plus vers la cyber-assurance. Mais sa couverture ne correspondra pas toujours à leurs attentes.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.