Retrouvez tous nos articles sur insight.stanwell.fr

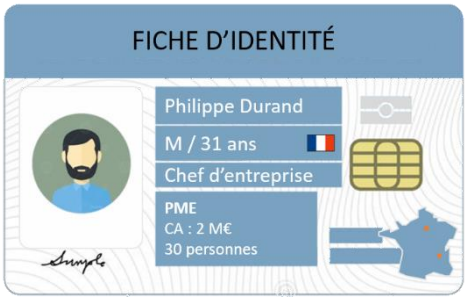
DE L'EXPLOSION DES CYBER-RISQUES A L'EMERGENCE DE L'ASSURANCE CYBER (PARTIE 1)

Eric de Tinguy
+337 63 79 29 42– e.detinguy@stanwell.fr
*Co-auteur : **Albéric Lugagne de Faucher***

02/02/2018

Non, le cyber-risque ce n'est pas pour les autres

L'exemple d'une PME



Il y a 5 ans, Philippe Durand a créé avec son coassocié, Guillaume, une start-up d'aide à domicile pour personnes âgées. Maintenant, c'est une PME qui opère dans plusieurs grandes métropoles françaises et compte une trentaine de personnes pour un chiffre d'affaires de 2 millions d'euros.

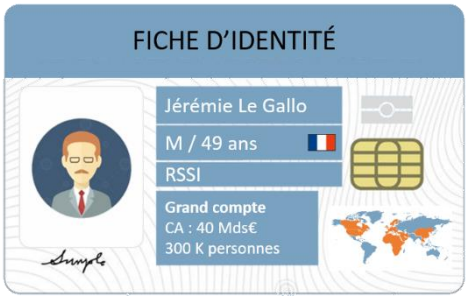
Aujourd'hui, comme chaque matin, Philippe arrive à 9h et allume son ordinateur et là… rien ne fonctionne. Impossible d'ouvrir ses fichiers. Soudain, une petite fenêtre s'ouvre et lui annonce que ses données ont été cryptées et qu'il lui faudra verser une rançon pour les récupérer.

Dix minutes plus tard, Philippe est en grande discussion avec son coassocié Guillaume : « On a un peu plus de dix-neuf heures pour payer les 6 000 euros de rançon". Pour eux c'est une somme significative étant donné la taille de leur entreprise. L'angoisse de Philippe ne fait que se renforcer lorsque Guillaume lance : "D'accord, et si nous payons cette rançon, sommes-nous sûrs de récupérer nos données ?".

Un peu plus tard arrive le Responsable de l'Informatique, David. Mis au courant, ce dernier commence par procéder au blocage de tous les postes pour stopper l'hémorragie et décide de contacter son assureur. En effet, 6 mois auparavant, David avait souscrit pour le compte de l'entreprise à un contrat de cyber-assurance proposant assistance, réparation et indemnisation en cas de cyber-attaque. Un conseiller reçoit l'appel et, après avoir écouté David, le met en relation avec un technicien qui intervient à distance.

Après plusieurs heures de travail et autant d'itérations avec David, au cours desquelles le technicien a suivi un protocole d'audit à chaud, celui-ci réussit à récupérer une partie des fichiers et à sécuriser la faille informatique. Cependant, une grande partie des données est perdue et suite à son audit, le technicien qualifie la perte d'exploitation et transmet directement une demande de compensation financière au back-office de gestion des sinistres chez l'assureur. Il adresse des préconisations d'ordre général à David, notamment en ce qui concerne l'envoi d'un mail de notification à la clientèle.

L'exemple d'une grande entreprise



Jérémie Le Gallo travaille pour un groupe de grande distribution qui réalise 20 000 fois le chiffre d'affaires de la PME de Philippe. Et pourtant, lui aussi est affecté par le cyber-risque. Il fait même partie intégrante de son quotidien. En tant que Responsable de la Sécurité du Système Informatique (RSSI ou CISO en anglais), il assure la sécurité, l'intégrité et la disponibilité du système d'information et des données sur un périmètre de 1 000 hypermarchés dans seize pays, soit plus de 338 000 employés. Il peut s'appuyer sur des Risk Managers locaux et leurs équipes, et reporte au Directeur du Système d'Information (DSI).

Dans son domaine, Jérémie est considéré comme ce que l'on appelle communément « un bon élève » : l'entreprise est couverte par l'un des tout premiers contrats de cyber-assurance sorti sur le marché et à sa demande expresse, un Security Operation Center (SOC) a été mis sur pied suite à la médiatisation d'attaques informatiques de grande envergure. Il s'agit d'une cellule de crise cyber dédiée aux évènements IT qui regroupe Jérémie, les risk managers de chaque pays et les responsables d'applications métiers. Enfin, le système de cybersécurité s'appuie sur une multitude de bonnes pratiques telles que l'utilisation de mots de passe robustes, un système d'exploitation et des logiciels à jour (navigateur, antivirus, bureautique) ou encore la sensibilisation des collaborateurs aux dangers des pièces jointes venant d'expéditeurs inconnus (phishing). Qui plus est, les différents protagonistes de la SOC ont été préparés à des scénarios catastrophes type à travers une série exercices dédiés, organisés au cours de l'année passée.

On peut donc dire qu'en matière de cybersécurité, l'entreprise de Jérémie est à la pointe de l'état de l'art. Jusqu'à présent, les risques avérés cyber ont été mineurs. Cependant, un jour une intrusion a lieu et est traitée comme un incident de routine, et l'entreprise continue à fonctionner normalement en apparence. Mais cette première intrusion a permis aux hackers de récupérer des données sensibles qui leur ont permis par la suite de mener une attaque de plus grande envergure. Deux semaines plus tard, ces terminaux cessent brusquement de fonctionner dans les filiales espagnoles, italiennes et grecques du Groupe.

C'est seulement à ce moment que la SOC est activée. Elle prend tout de suite la décision de déconnecter les machines infectées. Malheureusement, malgré cette mesure, l'attaque continue pendant 3 jours et les hypermarchés touchés sont au chômage technique, générant des pertes d'exploitation historiques.

La cellule de crise du Groupe (Direction Générale, Chief Risk Officer, Service Juridique, RH, Communication) ayant pris le relais, la décision est prise de contacter l'assureur du Groupe. Ce dernier les informe des modalités d'indemnisation financière au regard des garanties cyber-risques souscrites mais aussi de l'activation de services cyber adaptés aux problématiques d'un grand compte. Le réseau d'experts mis à disposition par l'assureur offre au Groupe une assistance juridique experte en cyber-risque, une aide aux relations publiques et un centre d'information dédié au sinistre.

A posteriori, l'assureur mobilise une des ressources technico-commerciales permettant d'établir un diagnostic à froid du sinistre. Elle identifie les causes profondes et les points de vulnérabilité. Elle établit également un plan de prévention ajusté et procède à la réévaluation de la couverture assurantielle.

Ces deux scénarii fictifs permettent de visualiser à quoi ressemble le cycle de vie d'une cyber-assurance. Néanmoins, il existe une multitude de types de risques cyber, que les assureurs doivent comprendre et quantifier au mieux afin de proposer des solutions adéquates.

Au fait, qu'est-ce qu'un cyber-risque ?

Tout d'abord, il convient de démystifier le concept « cyber », dont l'utilisation semble galvaudée. Est-ce qu'un cyber-risque est relatif à l'informatique, à l'internet, ou encore à d'obscurs algorithmes destinés à faire fonctionner des robots ?

Cyber est en fait un préfixe apparu à l'avènement de la robotique, avec la création du terme cybernétique par Norbert Wiener en 1948 pour décrire un champ scientifique où est étudié la maîtrise des machines. Le terme vient du grec *kubernêtês* (« pilote, gouvernail ») car à ce moment, Wiener tente d'élaborer un missile capable d'abattre les V1 et V2 allemands, ces fusées sans pilotes destinées à causer un maximum de dégâts en Angleterre. Le concept s'est plus tard étendu à l'informatique, avec l'émergence de mots bien connus comme « cyberespace » ou « cybercafé ».

La synthèse de ces deux domaines, robotique et informatique, a ouvert de nouveaux horizons qui sont désignés maintenant sous le nom de « révolution digitale ». Les risques cyber qui y sont associés renvoient donc à l'information, son traitement et sa sécurité, en incluant les acteurs, processus et technologies y prenant part.

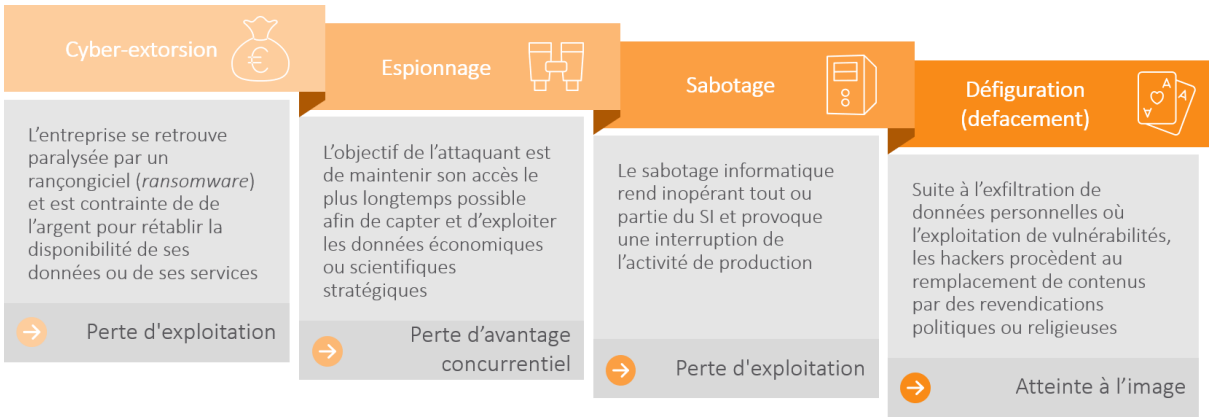
Le cyber-risque est un sujet polymorphe, encore assez flou, parfois équivoque. La première étape consistera donc justement à définir de quoi il s'agit !

Typologie des cyber-risques et ordres de grandeur

Une brève typologie des cyber-risques

Assez récemment, les malware WannaCry et Petya ont recentré notre attention sur la cybersécurité. Cependant, l'évolution rapide des risques cyber et l'explosion des attaques font la une des journaux depuis maintenant plusieurs années et trahissent une tendance de fond. La nouveauté vient surtout du fait que les attaques sont de plus en plus structurées et ciblées : une cyber-attaque mondiale pourrait engendrer des pertes allant jusqu'à 53 Mds$, c'est-à-dire autant qu'un puissant ouragan par exemple[1]. Les entreprises ont donc toutes les raisons de s'inquiéter, puisqu'elles font maintenant face à une probabilité accrue d'attaque, avec des conséquences toujours plus lourdes.

4 types de risques cyber peuvent les affecter[2] :



Les 2 techniques principalement employées pour accomplir ces crimes sont le déni de service par la saturation d'un réseau ou d'un serveur, et le phishing ou hameçonnage via l'envoi d'e-mails frauduleux.

Le cyber-risque n'a rien de virtuel

Le mot « cyber » a un côté futuriste qui s'avère idéal pour attirer l'attention mais peut faire oublier la teneur du risque, qu'on assimile facilement à une menace lointaine, virtuelle. Or la réalisation du cyber risque, à travers une cyber-attaque, a des répercussions tangibles. Les chiffres de l'année 2015 nous ramènent à la réalité : le cyber-risque est devenu décisif pour nos économies avec un nombre de cyber-attaques reportées en progression de 38% dans le monde, et de 51% en France[3]. Pour se donner un ordre d'idée, il suffit de revenir sur l'attaque de Sony en 2014 (110+ To de données volées, 100% des ordinateurs et 75% des serveurs KO) qui a couté 30 M€, celle de Target en 2013 (vol de données personnelles et bancaires de 110+ millions d'américains) qui a causé une perte de CA de 800 M€ et une perte de capitalisation boursière de 3,4 Mds€, sans parler des 80 procès intentés [4].

Contact : insight@stanwell.fr - 01 55 33 19 80

Par ailleurs, la dernière décennie a vu l'avènement d'attaques d'une échelle inédite, qui laissent présager de cyber-catastrophes à venir. Cet univers gagne en effet en sophistication à mesure que les attaques deviennent de plus en plus structurées et proviennent de bandes criminelles organisées, voire d'entreprises ou d'états. A ce jour, les cyber-attaques les plus dévastatrices sont en effet pilotées par des états. Par exemple, l'armée chinoise dispose de plusieurs milliers de cyber-soldats[5] qui s'emploient chaque jour à s'immiscer dans des systèmes informatiques et à dérober des informations stratégiques de haut niveau. De même, le New York Times a révélé que début 2014, les Etats-Unis ont tenté de compromettre les essais nucléaires nord-coréens à l'aide de cyber-attaques qui auraient réussi à accroître le taux d'échec sur plusieurs tirs[6]… Plus récemment en janvier 2015, près de 20 000 sites ont été la cible d'intrusions organisées par des djihadistes, dans le but d'y afficher de la propagande[7].

À ce titre, les pouvoirs publics prennent la menace très au sérieux. En France, le dernier rapport d'activité de l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) fait état d'une stratégie conjointe avec les pouvoirs publics pour offrir un cadre réglementaire au développement de la cybersécurité. Ainsi, à la suite d'un décret d'état publié en mars 2015, les opérateurs d'importance vitale (OIV) doivent instaurer des systèmes de détection des cyber-attaques, notifier les intrusions et procéder à des audits impliquants notamment l'ANSSI [8]. Les OIV regroupent plus de 200 entreprises dont la cessation l'activité risquerait de diminuer significativement le potentiel militaire ou économique de la nation, ou de mettre en péril l'intégrité de ses ressortissants.

L'élargissement de ces règles à d'autres acteurs permettrait de développer la cybersécurité et de favoriser l'extension des offres de cyber assurance et réassurance. En tout cas, sur ce marché très prometteur, soumis à des contraintes réglementaires croissantes, les assureurs et les courtiers se positionnent.

L'émergence de l'assurance cyber

L'expansion extrêmement rapide des cyber-attaques, dont le nombre a progressé de 140% au cours des trois dernières années [9], a donné lieu à une nouvelle matière assurable. En effet, les compagnies d'assurance se sont adaptées aux nouveaux risques informatiques en deux phases.

La première phase a suivi l'apparition des premières infections virales, les compagnies ont alors proposé à leurs clients des extensions de police d'assurance déjà souscrites. La hausse des primes couvrait les frais d'audit liés à l'installation de firewalls et d'anti-virus. Cependant, les sinistres ont continué à croître en gravité et de nouveaux types de cybercriminalité sont apparus, poussant les compagnies à davantage de prudence à travers de nouvelles exclusions dans les polices.

La seconde phase a commencé dans les années 2000 et a vu émerger des polices axées spécifiquement sur les cyber-risques. Les pionnières du secteur ont été les compagnies d'assurance anglo-saxonnes telles que AIG, Chubb, Lloyd's, ACE, XL. Les assureurs européens ont emboîté le pas récemment. ALLIANZ et AXA se sont ainsi rapprochées, respectivement de Thales et Airbus, afin de proposer deux volets à leurs clients : une police d'assurance couvrant le sinistre, et un accompagnement sur mesure en cyber-ingénierie [10].

Dernièrement, les compagnies de réassurance affichent également de plus en plus d'ambitions. Munich Re, numéro 2 mondial de ce secteur [11], a investi le segment du cyber-risque à la fois en tant que réassureur et assureur direct pour dégager à fin 2015 environ 191 M€ de primes sur son portefeuille cyber, soit +52% depuis 2013[12]. En termes de réassurance, la cession du cyber-risque s'opère généralement via une extension des traités de responsabilité civile professionnelle ou selon un système de quotes-parts pour encourager le développement de cédantes dans ce domaine. Mais à cause d'échelles de portefeuilles limitées, de modélisations inexactes et de statistiques historiques, le marché secondaire de la cyber-assurance, estimé par la SCOR à 450 M€[13], reste à construire.

Bien que les grandes entreprises soient les premières souscriptrices sur du marché de la cyber-assurance estimé à 50 millions d'euros en France - 10 entreprises du CAC 40 sont couvertes et 9 autres en voie de l'être - les PME et les TPE comptent pour 77%, des cibles de cyber-attaques en France, selon un rapport publié en 2016 par Symantec [14]. Cependant, seules 2 à 4% d'entre elles sont aujourd'hui assurées contre ces risques.

Sources

[1] *Lloyd's / Cyence – Rapport risques émergents : « Evaluer les coûts l'exposition au risque cyber décodée » (2017)*

[2] *Gouvernement.fr - Risques Cyber (http://www.gouvernement.fr/risques/risques-cyber)*

[3] *Les Echos « Pourquoi la cyber-assurance peut croire à son essor en France » (janvier 2016)*

[4] *INSA de Lyon, département informatique : Cours de réseaux avancés et sécurité des systèmes d'information répartis (Lionel Brunie 2016/2017)*

[5] *Les Echos - La cyber guerre n'est plus une fiction (Mars 2017)*

[6] *The New York Times - Trump Inherits a Secret Cyberwar Against North Korean Missiles (Mars 2017)*

[7] *Le Monde - Qui sont les « hackeurs pro-islam » qui attaquent des sites français ? (Janvier 2015)*

[8] *Xerfi – Le marché de la cybersécurité pour la banque et l'assurance (juillet 2016)*

[9] *L'Argus de l'Assurance - Cyber risques : Generali France lance une offre dédiée aux TPE-PME (avril 2017)*

[10] *L'Argus de l'Assurance - Axa, Allianz, Aviva : la diversification, mais pas à n'importe quel prix (août 2017)*

[11] *L'Argus de l'Assurance - Réassurance mondiale : découvrez le top 15 (septembre 2017)*

[12] *L'Argus de l'Assurance - Munich Re veut miser sur la cyber réassurance (septembre 2016)*

[13] *SCOR - Cyber risk on the rise: from intangible threat to tangible (re)insurance solutions (avril 2017)*

[14] *Symantec - Rapport annuel sur les cyber-menaces (avril 2016)*

A propos de Stanwell Insight

Créé en 2006, Stanwell Consulting est un cabinet de conseil en stratégie et transformation, historiquement spécialiste de la Banque et de l'Assurance et depuis 2013 du secteur Retail & Luxe.

Son positionnement original associe vision stratégique des modèles métiers de ses clients et capacité à imaginer, concrétiser, et accompagner leurs plans de transformation, qu'ils s'attachent à l'efficacité opérationnelle, l'innovation, l'entreprise digitale ou la croissance de la rentabilité. Assurance, Banque, Retail & Luxe sont les « cœurs de cible » des interventions de Stanwell.

Fort de cette expertise et afin d'accompagner toujours mieux ses clients, Stanwell Consulting est à l'écoute des besoins de leurs propres clients via son équipe Stanwell Insight. Retrouvez sur le site https://insight.stanwell.fr les points de vue des experts Stanwell mais également les études quantitatives et qualitatives conduites par Stanwell Insight.

Stanwell Insight a également créé un partenariat avec Wizville pour construire une offre de service packagée permettant la mise en place d'outil de mesure de la satisfaction client à chaud ou la pérennisation d'observatoires.