Section conjointe sur la gestion du risque
Institut canadien des actuaires
Casualty Actuarial Society
Society of Actuaries

La cybersécurité : l'incidence sur le domaine et les opérations de l'assurance

Canadian Institute of Actuaries | Institut canadien des actuaires

CAS

SOCIETY OF ACTUARIES

Préambule

La section conjointe sur la gestion du risque regroupant la Society of Actuaries (SOA), la Casualty Actuarial Society (CAS) et l'Institut canadien des actuaires (ICA) est ravie de publier son sixième recueil d'essais intitulé *La cybersécurité : l'incidence sur le domaine et les opérations de l'assurance*.

Ce recueil contient des essais d'actualité exprimant l'opinion et la réflexion de quatre chefs de file en cette matière. Les réflexions et les idées contenues dans le recueil représentent l'opinion des auteurs et ne correspondent pas nécessairement à celle de la SOA, de la CAS et de l'ICA ou des employeurs des auteurs.

L'équipe de rédaction a décerné des prix aux essais suivants :

Gagnants

Premier prix

Le cyberrisque ouvre de nouvelles possibilités
Michael Solomon

Deuxième prix

La cybersécurité et le marché de l'assurance
Laura Maxwell

Point de vue de l'assureur sur l'intégration du cyberrisque dans la gestion des risques
Kailan Shang

Calcul de la probabilité d'une faille de cybersécurité aux fins de la tarification de l'assurance cybercriminalité
Steven Dionisi

Table des matières

Introduction

Les cyberrisques constituent un élément majeur des risques opérationnels et tant les entreprises que les particuliers se tournent vers l'industrie de l'assurance pour obtenir une protection contre ceux-ci. Nous avons donc demandé aux auteurs de partager leurs réflexions sur la façon dont les sociétés d'assurance devraient aborder les cyberrisques dans le contexte de la gestion du risque d'entreprise (GRE) ou encore sur la façon dont elles peuvent répondre à la demande de la société de prendre les mesures nécessaires pour offrir davantage de produits d'assurance contre ces risques. Nous avons reçu plusieurs articles abordant diverses idées portant sur des concepts allant de l'analyse de Markov à la logique floue.

Dans l'essai *Le cyberrisque ouvre de nouvelles possibilités*, Michael Solomon évoque la nécessité pour les actuaires de travailler en collaboration avec d'autres experts de l'industrie de l'assurance afin d'élaborer des solutions novatrices durables à l'intention des principales parties intéressées. Il poursuit en évoquant « les principaux risques liés à la cybersécurité, les raisons qui poussent les entreprises à s'assurer, les motifs pour lesquels les sociétés d'assurances seront tenues d'offrir cette protection... ainsi que les techniques de gestion du risque qui sont à la portée des entreprises. » M. Solomon décrit les caractéristiques d'une éventuelle protection efficace contre les cyberrisques et ajoute que les actuaires sont les mieux placés pour contribuer à la conception de ces produits compte tenu de leurs compétences et de leur expérience. Il conclut en affirmant que le besoin croissant à l'égard d'une telle protection offre un débouché pour les actuaires.

Dans son essai intitulé *La cybersécurité et le marché de l'assurance*, Laura Maxwell se penche sur les façons d'évaluer le prix des cyberrisques et sur certaines sources de données importantes à prendre en considération. Elle suggère que : « De même que les assureurs ont fait figure de pionniers dans la prévention des sinistres dans les branches d'assurance traditionnelles, de même ils occuperont le devant de la scène pour ce qui est de prévenir le cybercrime et d'en réduire les conséquences. »

Dans son essai intitulé *Point de vue de l'assureur sur l'intégration du cyberrisque dans la gestion des risques*, Kailan Shang soutient que : « le cyberrisque doit être intégré au dispositif de gestion des risques, afin de faciliter la cohérence dans la gestion du capital, l'évaluation des risques et la répartition des ressources ». M. Shang se penche ensuite sur une possible définition de la propension au risque en ce qui concerne les cyberrisques et montre comment on peut évaluer l'exposition aux cyberrisques au moyen de modèles de logique floue. Il conclut en soutenant que : « Il importe de prendre des mesures proactives, telles qu'investir dans des technologies, donner de la formation, surveiller le risque ou souscrire une assurance, afin de réduire l'exposition au cyberrisque et de détecter l'évolution de nouvelles formes de cyberrisque. »

Dans son essai intitulé *Calcul de la probabilité d'une faille de cybersécurité aux fins de la tarification de l'assurance cybercriminalité*, Steven Dionisi démontre comment on peut modéliser la cybersécurité comme les produits d'assurance-vie. Il se penche plus précisément sur « l'application de l'analyse de Markov à la Cyber Kill Chain comme moyen de quantifier la probabilité de défaillance d'un système de cybersécurité sur une période donnée ou un nombre d'attaques ».

Nous espérons que ce document saura susciter la réflexion et la discussion. Qu'en retenez-vous?

Afin d'alimenter notre leadership éclairé en cette matière, nous sommes ouverts à d'autres commentaires, articles et réfutations.

Bonne lecture!

Salutations,

Thomas Hartl, Ph.D., FCAS, MAAA—Bryant University

Kevin Olberding, FSA, CERA, MAAA—Unum

David Schraub, FSA, CERA, MAAA, AQ—Society of Actuaries

au nom du Conseil de la Section conjointe sur la gestion du risque regroupant la Society of Actuaries, la Casualty Actuarial Society et l'Institut canadien des actuaires.

Le cyberrisque ouvre de nouvelles possibilités

Michael Solomon

La cybersécurité, c'est ce qui tient nos clients éveillés la nuit. De récents cas d'intrusion, fort médiatisés, préoccupent les administrateurs d'entreprises. Celles-ci se tourneront donc vers leur assureur de responsabilité civile pour obtenir la protection dont elles ont besoin, que ce soit sous forme d'avenant à leur police actuelle ou de police autonome, et elles verront d'un mauvais œil leur assureur si celui-ci refuse de la leur accorder. Tant les journaux spécialisés que les clients rencontrés citent la cybersécurité comme l'un des principaux risques à gérer. Les actuaires doivent collaborer avec d'autres experts du secteur des assurances pour trouver des solutions durables et innovantes qui profiteront aux principaux intervenants. C'est ainsi que leurs clients internes et externes jugeront de la valeur ajoutée de leurs services.

Le présent essai met en lumière les plus importants aspects du rôle de l'actuaire dans la tarification de l'assurance cyberrisque.

Dans la partie 1, nous évoquons les principaux risques liés à la cybersécurité, les raisons qui poussent les entreprises à s'assurer, les motifs pour lesquels les sociétés d'assurances seront tenues d'offrir cette protection même si elles ont de bonnes raisons de s'y opposer, ainsi que les techniques de gestion du risque qui sont à la portée des entreprises.

Dans la partie 2, nous exposons la valeur ajoutée que les actuaires sont en mesure d'offrir.

Dans la partie 3, nous terminons en indiquant que le besoin grandissant de cette protection ouvre de nouvelles possibilités aux actuaires.

Partie 1 : Risque

Les pertes directes découlant de crimes informatiques à but lucratif, telle la prise en otage de données, sont en fait très faibles et s'élèvent à environ deux ou trois milliards de dollars par année; par contre, les coûts directs et indirects engendrés par ces crimes sont très élevés. Les frais de défense engagés pour de tels crimes totalisent près de 19 milliards de dollars par an, tandis que les coûts indirects s'élèvent à 40 milliards de dollars de plus par année[1]. Le coût d'une seule intrusion peut se chiffrer en milliards de dollars (voir tableau 1) :

Tableau 1 : Cas d'atteinte à la protection des données les plus médiatisés et leurs coûts connexes

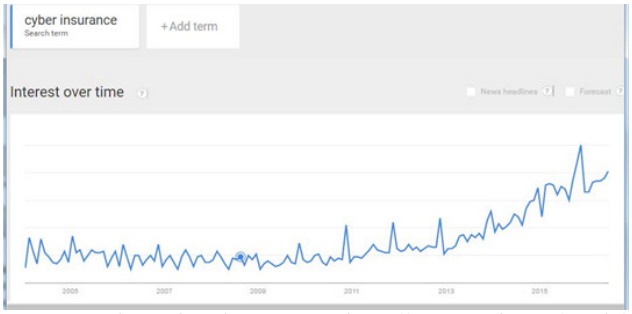
Victime	Cause	Coût total	Coût assuré
Epsilon	Hameçonnage ciblé[2]	Jusqu'à 4 milliards de dollars[3]	Aucune protection en place
Home Depot	Défaillance du système de cybersécurité du fournisseur et du système de sécurité de Microsoft Windows	Milliards $[4]	100 millions $
Wendy's	Inconnue	Milliards $[5]	Inconnu
Administration des anciens combattants	Ordinateurs/Disques durs externes soi-disant volés à la maison de l'employé lors d'un vol avec effraction[6]	500 millions $[7]	Aucune protection en place
Target	Défaillance du système de cybersécurité du fournisseur	252 millions $[8]	90 millions $
Hannaford Bros.	Logiciel malveillant	252 millions $[9]; responsabilité de l'assurance pour vol d'identité et coût de la carte de remplacement[10]	Aucune protection en place
Sony PlayStation	Inconnue	171 millions $[11]	Inconnu; règlement dans l'attente de l'appel après que la cour ait rendu un jugement sommaire à l'encontre de Sony[12]
TJ Maxx	Réseau local sans fil mal sécurisé dans deux magasins[13]	256 millions $[14]	19 millions $[15]
Sony Pictures Entertainment	Corée du Nord	151 millions $ + atteinte à la réputation	151 millions $
Heartland Payment Systems	Attaque par injection SQL[16]	140 millions $[17]	30 millions $[18]
Anthem	Faux nom de domaine/ Hameçonnage	Plus de 100 millions$[19]	100 millions $[20]

Le cybercrime engendre un grand nombre de coûts divers. Les coûts directs comprennent les coûts relatifs aux rançongiciels, à la perte de données et aux poursuites. Ce risque, s'il n'est pas assuré, peut faire perdre leur emploi à des personnes clés, et il se peut même que dans le cadre de nouvelles affaires des conseils d'administration soient poursuivis pour négligence.

Les vulnérabilités informatiques à l'origine de cette situation ne donnent guère de signes d'amélioration au fil des ans. Bon nombre d'entreprises « vivent en deçà du seuil de pauvreté en matière de sécurité ». Les sommes que bon nombre de petites et moyennes entreprises (PME) consacrent à la cybersécurité sont négligeables, ce qui explique pourquoi elles ne possèdent guère de compétences en technologies de l'information, qu'elles ne sont pas en mesure de suivre les recommandations des experts-conseils en informatique et qu'elles ne font par conséquent qu'éteindre les feux plutôt que de gérer les cyberrisques dans une optique à long terme[21]. À l'heure actuelle, on note une absence généralisée de preuve objective que les contrôles particuliers – qu'il s'agisse des politiques, des processus, des technologies ou de quelque autre moyen – ont un impact mesurable et favorable sur la qualité de la gestion du risque[22]. Bien que Singapour figure parmi les pays les plus avancés au monde au plan de la technologie, la solution retenue par son gouvernement en matière de cybersécurité consiste à éliminer l'accès des employés à Internet[23].

Il existe peu de solutions technologiques à même de contrer les cyberrisques. La plupart des options que proposent les fournisseurs n'offrent pas la protection voulue et elles ne semblent pas s'améliorer. Les contrôles techniques sont souvent trop compliqués ou trop coûteux à mettre en place, ou les deux à la fois. Le manque de données disponibles au sujet des cyberrisques les plus probables accentue ces problèmes. À défaut de nouveaux renseignements de sécurité, la plupart des entreprises ne peuvent prendre des décisions éclairées concernant la meilleure façon de répartir leur budget limité en matière de cybersécurité. Cela étant, certaines entreprises peuvent être tentées de souscrire une assurance cybersécurité plutôt que d'investir dans l'achat de solutions technologiques et d'autres moyens de contrôle. Elles peuvent décider de transférer le risque dans son intégralité plutôt que d'investir dans de coûteux efforts d'atténuation du cyberrisque, qui, pour l'essentiel, n'ont pas prouvé leur utilité. Si les assureurs n'imposent pas de critères minimums de sélection des risques, ce phénomène pourrait faire naître un risque subjectif et inciter les entreprises à prendre encore plus de risque au lieu de chercher à améliorer leur culture du risque.

Figure 1 : Tendances de Google



Source : Google Trends, "cyber insurance," https://www.google.com/trends/explore#q=cyber%20insurance.

Certaines sociétés offrent des avenants de cybersécurité à leurs titulaires d'une police d'assurance responsabilité civile, sans bien comprendre ce que leur coûte réellement cette garantie, préférant proposer à la place de faibles montants de garantie. Les assurés ne s'attendent-ils pas à obtenir de l'information sur ce qu'est un montant de garantie adéquat? Lorsqu'un incident survient et que le montant de garantie est faible en regard de la perte subie et que l'assuré doit prendre à sa charge l'écart résiduel, pensez-vous que l'assuré renouvellera sa police avec cette société? Le fait d'offrir de faibles montants de garantie ne saurait remplacer la rigueur dont doit faire preuve l'actuaire. En fait, je suis pour l'offre de montants de garantie élevés.

Partie 2 : Valeur ajoutée

Deux raisons expliquent pourquoi les assureurs offrent une protection contre le cyberrisque. Premièrement, l'assurance responsabilité civile représente, pour de nombreux assureurs, une branche très importante et rentable. Les assurés consulteront d'autres assureurs si celui qu'ils ont actuellement n'est pas en mesure de leur offrir la protection dont ils ont besoin.

Deuxièmement, le cyberrisque est une branche d'assurance qui gagne en importance et qui ouvre de nouvelles possibilités de revenus. Malgré une récente décision de la cour d'appel selon laquelle les polices d'assurance responsabilité civile peuvent couvrir les frais de défense liés à une intrusion informatique[24], l'intérêt manifesté pour l'assurance cybersécurité ne cesse d'augmenter, comme le montre la figure 1[25]. Un grand nombre des cyberrisques ne sont pas nouveaux (p. ex., vol de propriété intellectuelle, perte de profits, bris de confidentialité, atteinte à la réputation), et d'autres professions se tournent vers les actuaires pour qu'ils donnent la voie à suivre. En ce qui concerne la constitution d'un référentiel d'incidents informatiques, un courtier, deux souscripteurs et un réassureur ont soutenu que les actuaires étaient les personnes les mieux qualifiées pour traiter ces données et pour créer de nouveaux produits d'assurance cybersécurité ou améliorer les produits existants.

C'est précisément en raison de l'absence de données que les actuaires sont en mesure de faire preuve de leur utilité. Ils peuvent dresser une liste détaillée des éléments de données à collecter pour permettre une analyse utile, ils peuvent passer au peigne fin

les données disponibles afin d'établir des étalons de fréquence et de gravité, ils peuvent déterminer lesquelles des données sont crédibles et bien soupeser différentes indications. Par ailleurs, les technologues ignorent quelles sont les meilleures protections. Par exemple, dans quelle mesure le chiffrement est-il avantageux? Quel niveau doit-on adopter? Les actuaires sont exceptionnellement bien qualifiés pour trouver dans les données les réponses à ces questions. En procédant à la synthèse des données disponibles, les actuaires peuvent orienter les efforts des assureurs afin qu'ils travaillent avec les assurés à la réduction des pertes et à l'accroissement de la rentabilité.

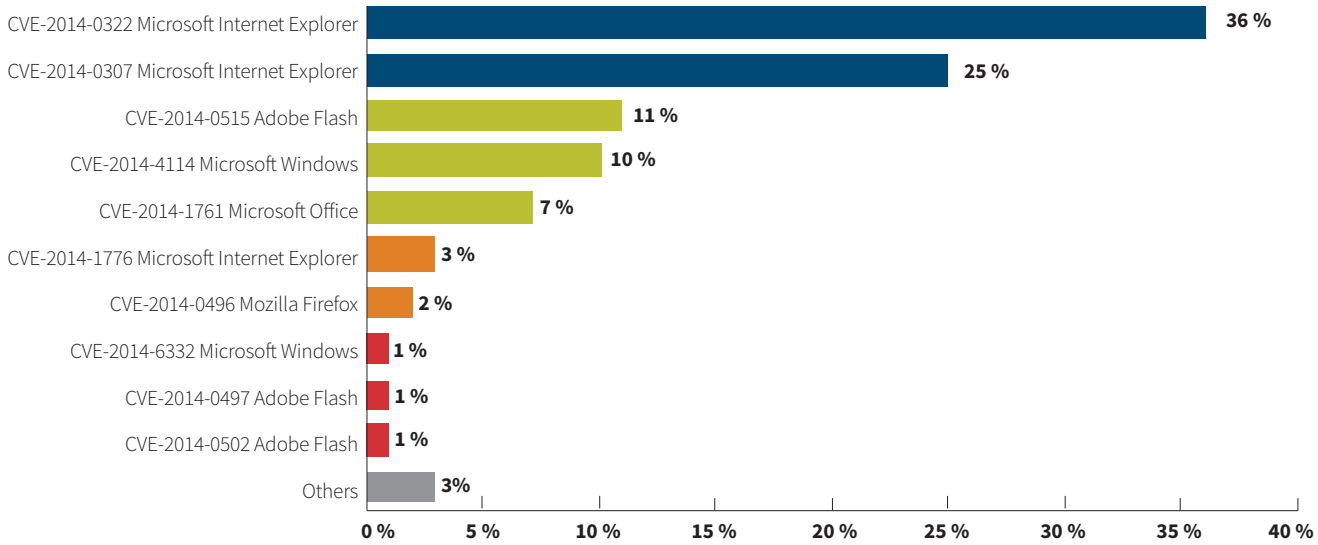
Les polices d'assurance cybersécurité se composent généralement de plusieurs sous-garanties (p. ex., la Beazleys Breach Response en compte huit[26]). Les actuaires peuvent déterminer l'exposition relative de chacune de ces sous-garanties et adapter les conditions particulières des polices aux besoins des assurés.

L'un des grands enjeux de l'assurance cybersécurité est le niveau de cybersécurité que les assureurs doivent exiger des assurés. Si ces niveaux se traduisent par des coûts trop élevés, l'attrait commercial du produit en souffrira. Par contre, l'application de critères trop permissifs encouragera les assurés à lésiner sur les solutions de protection onéreuses. Certains ont fait savoir qu'il était déraisonnable d'exiger de tous les employés qu'ils aient les nouvelles versions corrigées des logiciels. À mon avis, ce ne l'est pas (voir la figure 2). Les assurés sont en mesure de veiller à ce que tous les employés disposent d'une certaine version du logiciel à un moment donné, en procédant à des mises à niveau centralisées. Les assurés sont aussi en mesure d'exiger des employés qu'ils disposent de droits d'administrateur pour effectuer des téléchargements, le chiffrement des disques durs externes, le traitement automatique du langage naturel, et ainsi de suite. Nombre d'entreprises exigent de leurs employés qu'ils suivent une formation tous les ans pour les sensibiliser au harcèlement sexuel, afin d'éviter les poursuites et la perte du personnel clé. Les assureurs auraient donc raison d'exiger une formation annuelle en cybersécurité.

Les causes des pertes sont nombreuses, et l'intrusion des données tient à plusieurs d'entre elles. Bien que toutes ces causes ne puissent être contrôlées par les assurés, le Data Breach Investigations Report de Verizon (2013) révèle que 90 % des cyberattaques survenues au cours de l'année précédente auraient pu être évitées si des systèmes de complexité simple ou moyenne avaient été mis en place. Il y a nettement place à l'amélioration dans la plupart des entreprises en matière de gestion des cyberrisques[27]. Les assureurs ne devraient pas couvrir les risques sur lesquels l'assuré exerce un contrôle; l'assurance a pour but de couvrir uniquement les biens sur lesquels l'assuré ne peut exercer un contrôle. Les assureurs devraient inciter les assurés à faire ce qu'ils peuvent, soit en les obligeant à se protéger, soit par le biais des conditions de la police, comme le précise le présent document.

La fréquence et la gravité des incidents sont au cœur des travaux sur la gestion des cyberrisques. Bien que les entreprises puissent analyser la fréquence des incidents en examinant les quelques données disponibles, l'estimation de leur gravité est une tâche plus ardue. Les divers secteurs sont évalués selon des critères différents. À titre d'exemple, la fréquence élevée des sinistres liés à des crimes

Figure 2 : Les meilleurs exemples de vulnérabilités et expositions communes (VEC) découverts en 2014



Source : HPE Security Research Cyber Risk Report 2015. Hewlett Packard Enterprise Development LP.

informatiques de la part du secteur médical s'explique par les normes strictes de l'HIPAA (*Health Insurance Portability and Accountability Act*) en matière de sécurité et de confidentialité de l'information. Les assureurs demandent aux assurés des primes qui sont fonction de leur zone géographique et de leur secteur. Ils doivent user de leur jugement pour savoir quelles entreprises courent le plus de risque d'être victimes d'une attaque.

La fréquence est faible et, de façon générale, les sociétés constatent rapidement si elles ont été victimes d'intrusion. Cette situation comporte deux répercussions : le risque est plus facile à tarifer et par conséquent, il est plus facilement assurable. En outre, il est rare que plus d'une police soit mise en cause par un événement, et ces rares événements, qui sont généralement le fait de fournisseurs de services infonuagiques, peuvent être spécifiquement exclus d'un contrat. D'aucuns ont suggéré qu'un filet de sécurité fédéral semblable à la TRIA (*Terrorism Risk Insurance Act)* serait nécessaire pour couvrir ces événements.

Les assureurs ne devraient pas couvrir le risque de fréquence. Ce fardeau devrait incomber à l'assuré. Les sociétés d'assurances ajoutent de la valeur aux entreprises en prenant en charge la gestion du risque volatil pour que la direction puisse concentrer le capital dans d'autres éléments. La société est la mieux placée pour gérer les pertes prévisibles au moyen de la gestion des flux monétaires, peut-être par le biais d'une société captive à société mère unique. Les franchises élevées par événement obligent l'assuré à assumer le risque de fréquence et elles ne transfèrent que le risque de gravité volatil à l'assureur. Selon cette logique, il ne serait pas nécessaire d'imposer des franchises globales élevées. Je propose l'application d'une limite par événement dans l'ensemble de la police.

L'application de franchises élevées par événement empêche de percevoir l'assurance comme une solution de remplacement de la cybersécurité en bonne et due forme. Comme il est mentionné ci-haut, certains soutiennent que l'assurance cyberrisque est actuellement moins coûteuse que la cybersécurité; par conséquent, le risque subjectif et le risque moral sont les plus importants obstacles pour les sociétés d'assurances qui souhaitent prendre de l'expansion dans ce secteur. Pour garantir leur viabilité à long terme, les assureurs doivent éliminer l'attrait de leurs polices pour les sociétés qui choisissent l'assurance comme solution pour remplacer l'investissement dans la gestion du cyberrisque.

L'assureur est habituellement davantage en mesure que l'assuré d'assumer le risque de sinistres très graves. Il peut répartir le risque entre plusieurs polices, ce qui lui permet d'absorber plus facilement les événements peu fréquents. Afin d'optimiser la valeur, l'assureur devrait donc offrir des polices à limites élevées. Les polices à limites peu élevées sont utilisées pour abaisser les primes lorsque l'assuré est disposé à assumer des sinistres très graves et qu'il choisit implicitement d'utiliser ses ressources et son capital pour se protéger d'autres risques. Des limites insuffisantes peuvent entraîner la faillite dans les cas les plus graves. D'après mon expérience, les assurés ne sont pas disposés à accepter le risque de sinistres très graves rattachés à la cybersécurité lorsque les risques ne sont pas entièrement connus. Les assureurs sont beaucoup plus à même d'accepter ce risque dans le cadre des mécanismes habituels de mise en commun des risques d'assurance.

Les limites imposées aux polices se justifient également par la conservation des assurés. Comme il est mentionné ci-devant, le risque de gravité dépasse largement le risque de fréquence; ainsi, les franchises par événement sont bien plus efficaces. Les assurés sont davantage en mesure de conserver le risque lorsque les franchises sont élevées que lorsque les limites sont basses.

Partie 3 : Le cyberrisque ouvre de nouvelles possibilités

Pour conclure, je soutiens que les sociétés d'assurances peuvent élargir leur offre de produits d'assurance cybersécurité de la manière suivante :

Les polices doivent prévoir des franchises par événement qui sont élevées, et exiger des assurés qu'ils adoptent des mesures strictes de cybersécurité, ce qui permettra de maintenir les primes à un niveau abordable, tout en encourageant les assurés à réduire leurs risques.

- Les montants de garantie devraient être élevés, que ce soit pour chaque événement ou au total, car les assureurs sont davantage en mesure que les assurés d'assumer le risque de pertes importantes et ces derniers ont peu de possibilités de minimiser ces événements, qui sont peu fréquents.
- Les garanties devraient être flexibles afin de pouvoir répondre aux besoins particuliers des assurés.

Bien que cyberrisque rime avec pertes astronomiques, manque de données et absence de consensus dans le milieu de la technologie quant à la façon de le gérer, c'est précisément pour cette raison que les actuaires, forts de leurs compétences spécialisées et de leur expérience, sont en mesure d'offrir une valeur ajoutée. Au moment d'écrire ces lignes, les plus grandes sociétés d'assurances élargissent leur équipe spécialisée dans la cyberresponsabilité[28], conscientes des énormes possibilités qui s'y rattachent. Les sociétés qui seront en mesure de résoudre les difficultés qui sous-tendent la protection des cyberrisques et de répondre aux besoins de leurs clients s'en verront récompensées. C'est une occasion à ne pas rater!

1 *Cybersecurity Insurance Workshop Readout Report,* National Protection and Programs Directorate, U.S. Department of Homeland Security, Washington, D.C., novembre 2012.

2 Jaikumar Vijayan. « Epsilon a Victim of Spear-phishing Attack, Says Report », *Computerworld*, 7 avril 2011, http://www.computerworld.com/article/2507075/security0/epsilon-a-victim-of-spear-phishing-attack--says- report.html, consulté le 8 juin 2016.

3 Lori Widmer. « The 10 Most Expensive Data Breaches », *Life Health Pro*, 18 juin 2015, http://www.lifehealthpro.com/2015/06/18/the-10-most-expensive-data-breaches?t=practice- management&slreturn=1465402403&page=5, consulté le 8 juin 2016.

4 Greg Masters. « Home Depot Breach Costs Expected to Reach Billions », *SC Media*, 2 octobre 2015, http://www.scmagazine.com/home-depot-breach-costs-expected-to-reach-billions/article/442849/, consulté le 8 juin 2016.

5 « Credit Unions Feeling Pinch in Wendy's Breach », *Krebs on Security*, 2 mars 2016, http://krebsonsecurity.com/2016/03/credit-unions-feeling-pinch-in-wendys-breach/, consulté le 8 juin 2016.

6 « Veterans Affairs Data Theft », *Electronic Privacy Information Center*, n. d., https://epic.org/privacy/vatheft/, consulté le 8 juin 2016.

7 *Ci-dessus, note 4*.

8 Michael Kassner. « Data Breaches may Cost Less Than the Security to Prevent Them », *Tech Republic,* 9 avril 2015, http://www.techrepublic.com/article/data-breaches-may-cost-less-than-the-security-to-prevent-them/, consulté le 8 juin 2016.

9 Widmer. « 10 Most Expensive. »

10 Decision and Order on Plaintiffs' Revised and Supplemented Motion for Class Certification, U.S. District Court, District of Maine (Portland), Civil Docket No.: 2:08-MD-1954-DBH, http://www.med.uscourts.gov/Opinions/Hornby/MDL/MDL1954_2013_03_20_ORDER11.pdf, consulté le 8 juin 2016.

11 *Ci-dessus,* note 3.

12 Young Ha. "Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York ," *Insurance Journal*, 1er mai 2015, http://www.insurancejournal.com/news/east/2015/05/01/366600.htm, consulté le 8 juin 2016.

13 Jaikumar Vijayan. « One Year Later: Five Takeaways from the TJX Breach », *Computerworld*, 7 janvier 2008, http://www.computerworld.com/article/2538711/cybercrime-hacking/one-year-later--five-takeaways-from-the-tjx-breach.html, consulté le 8 juin 2016.

14 Ross Kerber. « Cost of Data Breach at TJX Soars to 256m » *Boston Globe*, 15 août 2007, http://archive.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/, consulté le 8 juin 2016.

15 « Insurance Company Reimburses TJX Almost $19 Million for Data Breach », *Fierce Retail*, 22 février 2008, http://www.fierceretail.com/story/insurance-company-reimburses-tjx-almost-19-million-for-data-breach, consulté le 8 juin 2016.

16 Jeremy Kirk. « Miami Man Indicted for Massive Credit Hack », *CSO Online*, 18 août 2008, http://www.csoonline.com/article/2124294/malware-cybercrime/miami-man-indicted-for-massive-credit- hack.html, consulté le 8 juin 2016.

17 Ci-dessus, note 8.

18 Jaikumar Vijayan. « Heartland Breach Expenses Pegged at $140M—so Far », *Computerworld*, 10 mai 2010, http://www.computerworld.com/article/2518328/cybercrime-hacking/heartland-breach-expenses-pegged-at-- 140m----so-far.html, *consulté le 8 juin 2016.*

19 Ci-dessus, note 8.

20 Mary A. Chaput. « Calculating the Colossal Cost of a Data Breach », *CFO*, 24 mars 2015, http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/, consulté le 8 juin 2016.

21 *Cyber Risk Culture Roundtable Readout Report,* National Protection and Programs Directorate, U.S. Department of Homeland Security, Washington D.C., mai 2013.

22 *Ibid*.

23 « No Internet for Singapore Public Servants », *BBC News*, 8 juin 2016, http://www.bbc.com/news/world-asia-36476422, consulté le 8 juin 2016.

24 John P. Mello Jr. « Insurance Industry Buzzes Over Data Breach Ruling », *Tech News World*, 21 avril 2016, http://www.technewsworld.com/story/83403.html, consulté le 14 juin 2016.

25 Google Trends, « cyber insurance », https://www.google.com/trends/explore#q=cyber%20insurance, consulté le 9 juin 2016.

26 https://www.beazley.com/london_market/specialty_lines/professional_liability/technology_media_and_business_services/beazley_breach_response/understanding_the_coverage.html, consulté le 14 juin 2016. Source des données originales : Breaches handled by Beazley Breach Response Services in 2014.

27 Ci-dessus, note 21.

28 Joyce Famakinwa. « Allianz Expands Cyber Insurance Team », *Business Insurance*, 7 juin 2016, http://www.businessinsurance.com/article/20160607/NEWS06/160609839?tags=58|285|93|137|98|83|76|71|70#utm_medium=email&utm_source=bi-breakingnews&utm_campaign=bi-breakingnews-20160607, consulté le 9 juin 2016 (abonnement obligatoire).

Michael Solomon, FCAS, CERA, MAAA est actuaire-conseil auprès de la firme The Actuarial Advantage, Inc. On peut le joindre à MichaelSolomon613@gmail.com.

La cybersécurité et le marché de l'assurance

Laura A. Maxwell, FCAS, MAAA

La fréquence et la gravité des cyberattaques sont en constante augmentation. Des intrusions pour vol de données ont lieu chaque jour, mais seules les plus importantes font les manchettes. À titre d'exemple digne d'intérêt, citons l'intrusion des systèmes de Premera Blue Cross par des pirates, le 5 mai 2014, qui a affecté 11 millions de personnes. Cette violation n'a été découverte que le 29 janvier 2015[1].

Outre le vol de données personnelles, le crime informatique inclut le vol de la propriété intellectuelle. S'il est difficile d'en déterminer le coût, ses conséquences économiques sont des plus importantes, car il réduit la concurrence et ralentit le progrès technologique[2]. Les entreprises mettent du temps à se rendre compte de ce type de vol et il est rare qu'elles en rendent compte publiquement. Des pirates ont volé les mots de passe des cadres supérieurs de Nortel, y compris celui du chef de la direction, et ont pu ainsi télécharger des articles spécialisés, des rapports de recherche et de développement, des plans d'affaires, des courriels d'employés et d'autres documents recouvrant une période de près de 10 ans[3].

Les rançongiciels, qui sont une autre forme de cyberattaque, gagnent aussi en importance. En l'occurrence, les logiciels malveillants verrouillent les ordinateurs des victimes, qui doivent verser une rançon, généralement en bitcoins, pour pouvoir utiliser à nouveau leur ordinateur. Les ordinateurs de l'hôpital presbytérien d'Hollywood ont été paralysés par un rançongiciel et les administrateurs ont dû verser aux pirates une somme d'environ 17 000 $ pour les débloquer[4]. Au premier trimestre de 2016, le Federal Bureau of Investigation (FBI) a été informé d'attaques de rançongiciels qui se sont traduites par des pertes totalisant plus de 209 millions de dollars[5].

Selon la *2015 Cost of Data Breach Study: Global Analysis*, les coûts du vol de données personnelles se divisent en trois catégories :

1. Coûts directs – le coût de l'activité :

- Notification
- Surveillance du crédit
- Services juridiques
- Relations publiques
- Pertes d'exploitation
- Amendes et pénalités réglementaires

2. Coûts indirects – temps et effort

3. Coûts d'opportunité :

- Roulement de clientèle
- Activités accrues d'acquisition du client
- Atteinte à la réputation
- Dépréciation du fonds de commerce[6]

Selon une étude réalisée conjointement par IBM et Ponemon, le coût moyen de chaque vol ou chaque perte de données personnelles est passé de 145 $, en 2014, à 154 $, en 2015[7]. Les produits d'assurance contre la cybercriminalité aident les entreprises à supporter les coûts des violations de données et des attaques de rançongiciels.

À l'heure actuelle, les primes d'assurance contre la cybercriminalité totalisent 2,5 milliards de dollars et on s'attend à ce qu'elles augmentent considérablement d'ici à 2020. Les projections pour 2020 sont de cinq milliards de dollars selon David Bradford, d'Advisen, de 7,5 milliards de dollars selon PWC ou de 10 milliards de dollars selon ABI[8]. Cette croissance est attestée par le nombre de demandes récentes d'approbation de tarifs, de règlements et de formulaires portant sur l'assurance contre la cybercriminalité. Plusieurs demandes tarifaires faites à partir de mai 2016 concernent l'assurance des entreprises contre les coûts directs que celles-ci subissent du fait de la violation de leurs données. Certaines sociétés d'assurance offrent une protection supplémentaire prévoyant le remboursement des coûts des cyberattaques, y compris l'extorsion. On ne semble pas cependant offrir de garantie contre le vol de la propriété intellectuelle.

Les tarifs varient, certaines entreprises exigeant un taux pour 1 000 $ de ventes brutes, tandis que d'autres demandent un taux de base fixe. Le calcul de la prime est assez simple et prévoit des rajustements pour tenir compte des montants de garantie, des franchises, de l'effet rétroactif de la couverture d'assurance et du type de risque. Deux des compagnies considérées dans notre étude répartissent leurs risques selon l'usage que les entreprises font de leur site Web :

- Risque faible : sites Web qui ne font que donner des informations
- Risque moyen : certaines activités commerciales sont réalisées à même le site Web de l'entreprise, ou celui-ci sert à stocker des numéros de cartes de crédit
- Risque élevé : l'entreprise réalise l'ensemble de ses activités sur son site Web ou y stocke des informations très sensibles telles que des numéros d'assurance sociale[9, 10]

D'autres entreprises répartissent leurs risques entre diverses classes, selon le type d'activité commerciale :

- Entreprises où les principales données personnelles ne concernent que les employés (fabrication, vente en gros)

- Entreprises qui conservent des données financières ou les numéros de compte de leurs clients, mais non pas leur numéro d'assurance sociale (vente au détail, églises)
- Entreprises qui conservent les numéros d'assurance sociale (location d'appartements, soins de santé, services professionnels)[11]
- Établissements d'enseignement
- Administrations municipales
- Hôpitaux et maisons de santé[12]

Les cyberattaques touchent l'ensemble des secteurs, mais leur fréquence et leur gravité varient. En 2015, ce sont les secteurs de la santé, des services financiers, de la vente au détail et de l'éducation qui ont été le plus souvent touchés, tandis que c'est celui de la restauration et de l'hôtellerie qui a enregistré les attaques les plus graves. Les criminels de l'informatique sont passés des supermarchés et des grandes surfaces aux restaurants, hôtels et casinos[13]. L'utilisation du type d'industrie comme critère de classification des risques constitue un bon point de départ pour qui veut mettre un prix au cyberrisque, mais les assureurs doivent aussi prendre en compte le volume de données de l'entreprise, la valeur de celles-ci, le nombre de terminaux à protéger et le nombre de fournisseurs[14].

Les sociétés d'assurance contre la cybercriminalité proposent des tarifs similaires, ce qui peut s'expliquer par l'absence de données d'assurance utiles au calcul des taux de base et des facteurs. Une société a déposé des tarifs qui reposaient sur des données publiées par le Government Accountability Office des États-Unis, le Ponemon Group, Gartner ainsi que la Federal Trade Commission[15]. Les sociétés d'assurance devraient se tourner vers les données externes pour fixer leurs tarifs contre le cyberrisque. Outre les sources précitées, des données sont disponibles auprès de l'Identity Theft Resource Center, du Department of Homeland Security, du Center for Strategic and International Studies et de l'Office des Nations Unies contre la drogue et le crime.

Si le marché de l'assurance des entreprises contre la cybercriminalité gagne en importance, il en va autrement du marché de l'assurance des particuliers. Les assureurs habitation ajoutent des clauses d'exclusion à leurs contrats afin de se dégager de toute responsabilité à l'égard des médias sociaux et de la cyberintimidation. Les garanties se limitent habituellement à l'usurpation d'identité, qui pourrait être le résultat d'un crime informatique. Chubb fait exception à ce chapitre, ayant annoncé dernièrement qu'elle offrirait une protection contre la cyberintimidation dans le cadre de sa police d'assurance habitation Protection familiale. Cette protection couvrira le counseling, la perte de salaires et les relations publiques[16].

Les sociétés d'assurance pourraient aussi venir en aide aux titulaires de polices dans la prévention des crimes. Les assureurs devraient savoir qui est responsable de la violation des données et la manière dont celle-ci s'est produite afin de pouvoir aider leurs titulaires de polices. Ils doivent aussi être mis au courant des récentes menaces afin de pouvoir en informer par avance ces derniers.

Les assureurs peuvent évaluer la qualité de la préparation des entreprises proposantes afin de procéder à une sélection adéquate des risques et proposer des tarifs adéquats et de prévenir les crimes. Dans le cadre de son plan de tarification individuelle sensible aux risques, Chubb passe en revue les mesures de prévention mises en place par l'entreprise et examine les points suivants :

- Coupe-feu et système de détection des intrusions
- Mots de passe et protocole d'authentification
- Utilisation de la cryptographie et méthodes de cryptage
- Tenue à jour du journal de bord du système
- Processus de gestion des correctifs
- Élasticité prévue des ressources informatiques
- Téléphones et appareils informatiques mobiles
- Protocoles écrits prévoyant les critères d'attribution des droits d'accès privilégiés (pour l'administration du système)
- Programme de formation des employés et des utilisateurs autorisés, qui porte sur les questions de sécurité et de confidentialité, y compris les responsabilités légales et les menaces telles que le piratage psychologique (hameçonnage, par exemple), les pourriels et le glanage urbain
- Rapports annuels produits par le service de sécurité informatique à la haute direction
- Plan de réponse aux incidents, y compris la violation de données et la perte d'ordinateurs portables ou d'appareils mobiles
- Procédures de révocation immédiate de la totalité des privilèges et de saisie du matériel informatique
- Sauvegarde journalière
- Plans de continuité des activités et de reprise après sinistre qui tiennent compte des cybermenaces[17]

Les entreprises qui n'obtiennent pas un bon score à ces questions peuvent recevoir de l'aide pour améliorer leurs moyens de défense. La mise en place d'excellents moyens de défense ne permet pas d'éliminer toutes les demandes d'indemnités, mais elle contribue à réduire considérablement les coûts et les temps d'intervention en cas de violation. Les Sœurs de la charité chrétienne du comté de Santa Clara ont pu éviter le paiement d'une

rançon grâce à un appareil qui surveillait les activités inhabituelles sur leur réseau. L'ordinateur qui était en communication avec un serveur en Ukraine a été débranché du réseau avant d'avoir pu provoquer des dommages importants. La détection rapide des rançongiciels permet aux entreprises d'économiser de l'argent .

La formation des titulaires de polices constitue un autre moyen de prévenir le crime. L'erreur humaine est à l'origine d'un grand nombre d'incidents. Selon l'étude de BakerHostetler, l'hameçonnage et le piratage sont responsables de 31 % des cyberincidents et sont souvent dus à l'erreur humaine, les autres causes étant les erreurs des employés (24 %), le vol externe (17 %), les fournisseurs (14 %), le vol interne (8 %) et la perte ou la gestion inadéquate de documents (6 %) .

Après une cyberattaque, la société d'assurance peut être utile en participant à l'analyse criminalistique. Il importe que l'entreprise sache rapidement quelles données sont menacées afin de pouvoir réagir promptement. Les consommateurs sont bien conscients que des intrusions se produisent, et le fait de ne pas reconnaître ou de sous-estimer leur impact peut gravement compromettre la réputation de l'entreprise et la fidélisation de la clientèle.

Les particuliers peuvent avoir besoin d'une vérification de sécurité pour s'assurer que leurs systèmes informatiques ne sont pas menacés. Cela vaut surtout pour les personnes qui stockent des données relatives à leurs placements et d'autres informations sensibles dans leur ordinateur domestique ou leurs appareils mobiles. Pure Insurance offre des vérifications d'une durée d'une journée et des services de détection des intrusions sur réseau domestique. Elle a instauré ce programme en réponse aux demandes d'indemnités reçues suite à des crimes informatiques .

La couverture d'assurance contre la cybercriminalité devrait continuer de s'étendre au fur et à mesure que le cybercrime gagnera en fréquence et en gravité. De même que les assureurs ont fait figure de pionniers dans la prévention des sinistres dans les branches d'assurance traditionnelles, de même ils occuperont le devant de la scène pour ce qui est de prévenir le cybercrime et d'en réduire les conséquences.

---

1 Associated Press, «Data Breach at Premera Blue Cross Could Affect 11 Million People », *SFGATE.com,* 17 mars 2015, http://www.sfgate.com/business/article/Data-breach-at-Premera-Blue-Cross-could-affect-11-6139961.php.
2 Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (Washington, DC: Center for Strategic and International Studies, juin 2014), p. 12, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.
3 Siobhan Gorman, « Chinese Hackers Suspected in Long-Term Nortel Breach », *Wall Street Journal,* 14 février 2012, http://www.wsj.com/articles/SB10001424052970203363504577187502201577054.
4 Sean Sposito, « Locky Ransomware Lives up to its Name, Locking Files », *SFGATE.com*, 19 février 2016, http://www.sfgate.com/business/article/Locky-ransomware-lives-up-to-its-name-locking-6843516.php.
5 Sean Sposito, « Santa Clara Charity Has a Narrow Escape from Ransomware », *San Francisco Chronicle*, 29 avril 2016, http://www.sfchronicle.com/business/article/Santa-Clara-charity-has-a-narrow-escape-from-7384755.php.
6 *2015 Cost of Data Breach Study: Global Analysis*, recherche comparative financée par IBM et réalisée en toute indépendance par Ponemon Institute LLC, mai 2015, p. 25.
7 Caitlin Bronson, « The $2.5 cyber insurance market could be nearly 4 times bigger by 2020 », *IBAMAG.com*, le 5 mai 2016. http://www.ibamag.com/news/cyber/the-2-5-cyber-insurance-market-could-be-nearly-4-times-bigger-by-2020-31531.aspx.
8 Ibid.
9 Pennsylvania National Mutual Casualty Insurance Company, Countrywide Rules, numéro de suivi SERFF PNMC-130250857.
10 Berkley National Insurance Company, Company Rules, numéro de suivi du SERFF BNIC-130409966.
11 American Fire and Casualty Company, Company Exceptions, SERFF Tracking # LBRC-130374617.
12 The Cincinnati Casualty Company, Coverage Rules, numéro de suivi du SERFF CNNA-130319569.
13 Theodore J. Kobus, et al., *Is Your Organization Compromise Ready? 2016 Data Security Incident Response Report* (Atlanta, GA: BakerHostetler, 2016), p. 4, http://www.mass.gov/export/update2016/presentations/2016%20Data%20Security%20Incident%20Response%20Report.pdf.
14 Ibid.
15 The Cincinnati Insurance Companies Rate Filing Memorandum, numéro de suivi du SERFF CNNA-130319569.
16 « Chubb Adds Cyber Bullying Insurance for U.S. Homeowners », *Insurance Journal*, 5 avril 2016, http://www.insurancejournal.com/news/national/2016/04/05/404202.htm.
17 CUSTOMARQ IRSR Plan for Coverage "C" – Cyber Liability and Additional Coverages, numéro de suivi du SERFF CHUB-130359516.
18 Sposito, "Santa Clara Charity."
19 Kobus, et al., *Is Your Organization Compromise Ready?*, p. 6.
20 Priya Anand, « Do Individuals Need Cybersecurity Insurance », *Wall Street Journal*, 20 septembre 2015, http://www.wsj.com/articles/do-individuals-need-cybersecurity-insurance-1442800951.

Laura A. Maxwell, FCAS, MAAA, est actuaire-conseil au sein de Pinnacle Actuarial Resources Inc. Vous pouvez la joindre à LMaxwell@PinnacleActuaries.com.

Point de vue de l'assureur sur l'intégration du cyberrisque dans la gestion des risques

Kailan Shang FSA, CFA, PRM, SCJP

Le cyberrisque est devenu l'un des plus importants risques à surveiller par les gestionnaires du risque en raison de sa fréquence accrue et de son impact. Selon un sondage réalisé en 2014 par la Section conjointe sur la gestion du risque, qui regroupe la CAS, l'ICA et la SOA, la cybersécurité occupe le premier rang des nouveaux risques selon 58 % des répondants[1]. Le cyberrisque se définit comme étant le risque que des personnes ou des défaillances des systèmes ou des processus endommagent le matériel et les logiciels ou compromettent la sécurité du système d'information, ce qui pourrait entraîner des pertes financières ou une interruption des activités ou porter atteinte à la réputation de l'entreprise.

L'industrie de l'assurance adopte depuis un certain temps de nouvelles technologies qui facilitent l'échange d'informations avec les clients et le grand public. Un grand nombre d'entreprises se servent couramment des médias sociaux pour communiquer avec eux. Les assureurs demandent à leurs clients de plus en plus de données personnelles, telles que des données télématiques pour analyser les habitudes de conduite et des données sur l'état de santé ou la condition physique. L'expansion de l'Internet des objets ouvre de nouvelles possibilités, mais entraîne une exposition accrue à un cyberrisque plus complexe. Les assureurs offrent une assurance qui protège l'assuré contre les pertes financières causées par le cyberrisque. Ces assureurs s'exposent à une plus grande variété d'événements porteurs de risques. S'agissant d'un type de risque qui évolue rapidement, le cyberrisque doit être intégré au dispositif de gestion des risques, afin de faciliter la cohérence dans la gestion du capital, l'évaluation des risques et la répartition des ressources.

Propension au cyberrisque

Selon Eling et Wirfs[2], le cyberrisque est moins grave que le risque opérationnel non cybernétique du point de vue du montant des pertes et de leur volatilité. Mais il est plus contagieux que lui. Un seul événement porteur de risques peut toucher plusieurs firmes. En raison de l'application élargie de l'Internet des objets, la fréquence et la gravité du cyberrisque pourraient augmenter de façon importante. Dans le cas d'un assureur particulier, le manque d'investissement dans l'amélioration de la cybersécurité pourrait aussi se traduire par une plus grande exposition au cyberrisque que la moyenne. Pour déterminer la propension au cyberrisque, il faut procéder à une évaluation rigoureuse du système Internet, des pertes qui peuvent découler de la violation de données, des processus internes de contrôle, du personnel compétent en la matière, de l'état de préparation à la gestion des incidents et de la possibilité d'entacher la réputation de l'entreprise.

Une fois les pertes potentielles bien évaluées, qu'elles soient financières ou de nature à nuire à la réputation, la propension au cyberrisque peut être définie en fonction de la volonté et de la capacité de l'entreprise à prendre des risques. Comme c'est le cas des autres types de risques, la tolérance au cyberrisque peut se définir au moyen de mesures quantitatives, telles que le capital exposé au risque et les bénéfices exposés au risque, ou de déclarations qualitatives du type : « Aucun dommage important à la réputation de l'entreprise ni aucune interruption des activités ne sont acceptables du fait du cyberrisque. » Voici un exemple de déclaration de tolérance au cyberrisque :

- L'entreprise ne peut subir une perte de capitaux propres relatifs aux Normes internationales d'information financière (IFRS) supérieure à 10 % du fait d'un seul événement ou d'une seule série d'événements liés porteurs de cyberrisque.
- L'entreprise a une très forte aversion pour le risque d'atteinte à sa réputation pouvant découler de failles de sécurité informatique.
- L'entreprise a mis en place un plan d'urgence prévoyant la continuité des activités en cas de panne Internet ou de cyberattaque.

Dans cet exemple-ci, le chiffre de 10 % devrait s'appuyer sur une analyse quantitative de l'exposition au cyberrisque. Pour pouvoir définir la tolérance au cyberrisque de façon quantitative, il faut des données sur l'expérience, des avis d'experts et un modèle sophistiqué qui tient compte de l'évolution de l'environnement. Le pourcentage peut aussi être estimé grossièrement comme étant le pourcentage attribuable au risque opérationnel non cybernétique multiplié par l'extrémité relative du cyberrisque par rapport au risque opérationnel non cybernétique.

Modèle hybride

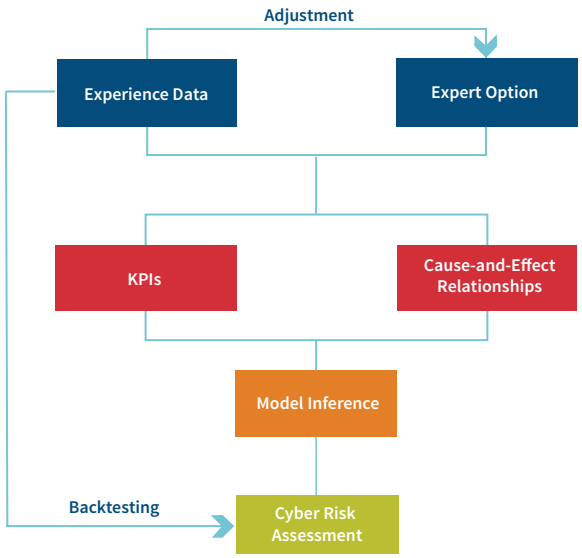
L'incertitude du cyberrisque, l'utilisation accrue de l'Internet des objets pour échanger de l'information et les préoccupations concernant la confidentialité des données sont souvent la cause du manque de données sur l'expérience permettant de mesurer l'exposition au cyberrisque. Même s'il y avait assez de données,

certaines conséquences du cyberrisque, telles que le dommage à la réputation, sont difficiles à quantifier. Un modèle hybride en est un qui utilise les données sur l'expérience limitées et l'avis des experts pour évaluer l'exposition au cyberrisque. En raison de la quantité importante d'information fournie par un éventail d'experts, le modèle doit aussi pouvoir prendre en compte, de façon cohérente, l'information subjective et en tirer des conclusions.

Les modèles hybrides, tels que les modèles de logique floue, peuvent servir à évaluer l'exposition au cyberrisque. Les modèles de logique floue s'appuient sur la théorie des ensembles flous et la logique floue. Ils permettent à un objet d'appartenir à plus d'un ensemble particulier selon divers niveaux de confiance. Ces modèles servent à analyser les risques lorsque les connaissances sont insuffisantes ou que les données sont imprécises. Shang et Hossen (2013) ont étudié l'application des modèles de logique floue à l'évaluation des risques[3]. Les données sur l'expérience disponibles peuvent servir à étalonner la partie quantitative du modèle qui décrit les caractéristiques des principaux indicateurs de risque. Les avis d'experts au sujet de ces indicateurs et de leurs liens avec les expositions au cyberrisque peuvent aussi être intégrés aux modèles de logique floue. La cohérence des règles d'inférence utilisées dans les modèles de logique floue permet de réduire les effets défavorables des biais cognitifs que l'on retrouve habituellement dans les évaluations qualitatives des risques. La figure 1 représente la structure d'un modèle de logique floue.

Puisque les connaissances et l'expérience relatives au cyberrisque évoluent rapidement, les modèles de logique floue rendent l'évaluation du cyberrisque flexible et cohérente. Les experts doivent dresser une liste des principaux indicateurs du cyberrisque qui tient compte de l'infrastructure des technologies de l'information, des activités et des données de l'entreprise. Le tableau 1 montre des exemples de principaux indicateurs de risque pour plusieurs sous-catégories de cyberrisques. La plupart

Figure 1 : Structure d'un modèle de logique floue



[Figure disponible en anglais seulement]

Tableau 1 : Exemples des principaux indicateurs de risque en matière de cybersécurité

Catégorie	Principaux indicateurs de risque
Ressources	Nombre de spécialistes de la cybersécurité
	Caractère suffisant de la formation en matière de cybersécurité
	Niveau de sensibilisation à la cybersécurité
	Caractère suffisant des ressources financières allouées au cadre de la cybersécurité
	Temps de réponse attribué à la gestion de la cybersécurité
Contrôle	Caractère suffisant de l'évaluation du cyberrisque (personnes, processus et technologie)
	Caractère suffisant des vérifications de vulnérabilité du matériel, des logiciels, des réseaux, du télétravail, des appareils mobiles, etc.
	Caractère suffisant de l'évaluation du cyberrisque auprès des fournisseurs de services de TI
	Niveau de la centralisation du contrôle en matière de cyberrisque
	Ponctualité des mises à jour de sécurité et des vérifications
Gouvernance en matière de risque	Portée des politiques en matière de cybersécurité
	Précision des rôles et responsabilités
	Caractère suffisant des vérifications internes et de la surveillance externe
	Soutien des cadres supérieurs
	Analyse de scénarios
Détection	Nombre de droits d'accès incorrects aux données
	Nombre d'accès non autorisés aux données
	Pertes antérieures attribuables à l'atteinte à la protection des données
	Capacité de récupération des données
	Vitesse de mise à jour des technologies relatives à la sécurité des données
Données	Nombre de droits d'accès incorrects aux données
	Nombre d'accès non autorisés aux données
	Pertes antérieures attribuables à l'atteinte à la protection des données
	Capacité de récupération des données
	Vitesse de mise à jour des technologies relatives à la sécurité des données
Gestion des incidents	Temps moyen de réponse en cas d'incident causant des dommages matériels
	Plan de communication
	Récupération du système, du réseau, des données et des activités
	Capacité d'enquête à la suite d'incidents et d'identification des causes
	Base de données chronologiques des incidents (entreprise et industrie)

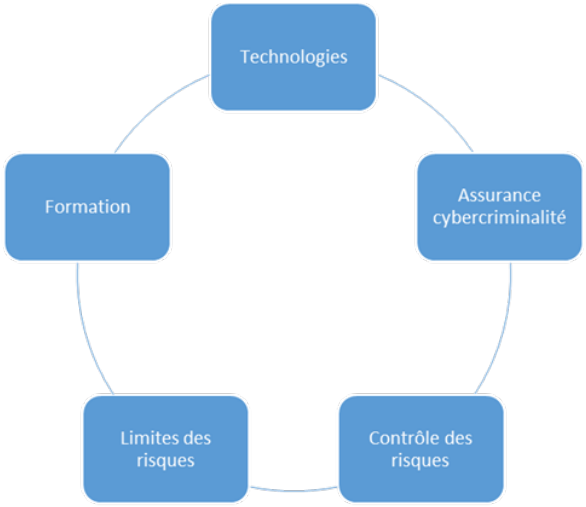
des indicateurs ne sont pas quantifiables et doivent être classés en fonction du niveau de confiance qu'on leur attribue, soit élevé, moyen ou faible.

L'avis des experts concernant la relation entre ces indicateurs et l'évaluation du risque résultant de chacune des catégories du tableau 1 et le niveau global du cyberrisque sera nécessaire. Par exemple, si le nombre d'incidents de sécurité détectés est faible et que le temps moyen de détection des incidents de sécurité est long, le risque lié à la détection d'incidents de sécurité est élevé. En établissant une relation entre les indicateurs et les liens de cause à effet, les modèles de logique floue seront utiles pour calculer le niveau de cyberrisque qui indiquera la fréquence et la gravité. Les nouvelles données sur l'expérience peuvent servir à réaliser un contrôle ex post avant de connaître les résultats de l'évaluation. De plus, les experts peuvent changer d'avis après avoir acquis de nouvelles connaissances et appris de nouvelles choses.

Gestion du cyberrisque

La déclaration de propension au cyberrisque définit la stratégie générale en matière de cybersécurité. Toutefois, comme c'est le cas des autres risques opérationnels, il importe d'assurer une gestion proactive afin de ne jamais dépasser le seuil de tolérance au risque. La plupart des méthodes employées pour gérer les risques opérationnels peuvent être adaptées à la gestion du cyberrisque en vue de leur utilisation.

Figure 2 : Éléments de la gestion active du cyberrisque



Il importe d'investir dans de nouvelles technologies. Celles-ci facilitent l'identification des sources de cyberrisque, préviennent les cyberattaques et préservent la robustesse du système Internet. De nouvelles formes de cyberrisque apparaissent chaque jour et les technologies utilisées pour les combattre évoluent elles aussi rapidement. Bien que les nouvelles technologies puissent être aujourd'hui trop coûteuses, il importe de bien comprendre leurs fonctions et leurs applications afin de pouvoir les adopter lorsqu'il sera économique et nécessaire de le faire.

La formation sur le cyberrisque peut aider les employés à bien comprendre les sources des cyberattaques et les formes qu'elles peuvent prendre, à détecter leur existence, à respecter les procédures de précaution et à pouvoir intervenir rapidement afin d'atténuer l'impact des attaques.

L'établissement des limites pour le cyberrisque ne s'effectue pas de la même manière que pour les autres types de risques. Par exemple, pour déterminer les limites relatives au risque d'assurance, on peut utiliser des mesures quantitatives telles que le capital sous risque net et l'expérience de mortalité, de morbidité et de déchéance. Par contre, pour déterminer la propension au cyberrisque, il faut évaluer le système Internet de l'entreprise, l'attractivité des données auprès des cybercriminels et le niveau de conscientisation des employés, afin de bien apprécier le niveau actuel de cybersécurité. Les indicateurs clés du cyberrisque doivent être conçus en fonction de l'activité particulière de l'entreprise, de ses données et de ses systèmes. Entre autres indicateurs possibles, citons le nombre de pannes de système par mois, le nombre d'utilisateurs qui ont accès aux données sensibles, le degré de sensibilisation des employés au risque, tel qu'il est mesuré par l'ampleur de la formation suivie par les employés, et le temps moyen écoulé avant la détection d'une cyberattaque. Les limites peuvent être fixées en regardant ce que font les pionniers de la gestion du cyberrisque, tout en apportant des ajustements pour tenir compte de la situation de l'entreprise.

Il est difficile de contrôler le cyberrisque en raison de son étendue et de son évolution rapide. Il faut mettre l'accent sur les principales données et la protection des systèmes clés, car le contrôle ne peut être entier et parfait. Étant donné que les événements porteurs de cyberrisque peuvent survenir rapidement, la fréquence du contrôle doit être plus grande que pour les autres types de risques, tels que le risque d'assurance. Le contrôle consiste non seulement à vérifier l'exposition courante au cyberrisque au regard de la limite, mais aussi à surveiller de façon automatique et en temps réel le système Internet, le système de communication (courriel, téléphone, etc.) et les données des médias sociaux, afin de détecter tout indice d'un éventuel événement porteur de cyberrisque, par exemple, une violation des politiques ou des procédures de sécurité d'un système, un logiciel malveillant, des privilèges

d'utilisateur indus, des activités de système irrégulières, des communications avec des systèmes de l'extérieur, tels qu'un ordinateur personnel ou le système d'un tiers, l'accès à des données importantes ou leur transfert.

Le plan d'urgence joue un rôle essentiel dans la gestion des pertes causées par les événements porteurs de cyberrisque, qu'elles soient financières ou de nature à nuire à la réputation. Un plan d'action permet à l'entreprise de réagir rapidement face à un événement porteur de cyberrisque, tel que la violation de données ou la défaillance d'un système. Il peut contribuer à réduire au minimum le risque d'interruption des activités et de faire ainsi la une, ou du moins à montrer que l'entreprise est déterminée et est en mesure de gérer le cyberrisque.

L'assurance cybercriminalité peut être utilisée pour transférer à un tiers la prise en charge du grave impact des événements porteurs de cyberrisque. Malgré de gros investissements dans les technologies, la formation et le contrôle actif du risque, des événements de cyberrisque inattendus peuvent toujours se produire. L'assurance cybercriminalité offre une protection complémentaire contre les pertes inattendues. La gestion proactive du cyberrisque est nécessaire parce que l'assurance cybercriminalité ne couvre pas toutes les pertes, et une bonne gestion du cyberrisque permet de réduire l'exposition à celui-ci et d'obtenir ainsi une prime d'assurance plus basse. Si un tiers assure une part substantielle du risque, sa capacité de payer les indemnités promises doit être évaluée, car les événements porteurs de cyberrisque peuvent toucher simultanément un grand nombre d'entreprises et d'utilisateurs particuliers.

Conclusion

Pour l'industrie de l'assurance, le cyberrisque est devenu l'un des grands risques à surveiller du fait de l'expansion du monde numérique et de l'Internet des objets. Il partage avec les autres risques opérationnels un grand nombre de caractéristiques, mais on considère que son évolution rapide fera en sorte qu'il aura une plus grande incidence dans l'avenir. Comme c'est le cas des autres risques, la déclaration de propension au cyberrisque est utile pour définir le niveau général de tolérance. Toutefois, elle doit s'appuyer sur une modélisation sophistiquée qui est en mesure de tirer parti de façon cohérente des données sur l'expérience limitées et des avis d'experts en la matière. Il importe de prendre des mesures proactives, telles qu'investir dans des technologies, donner de la formation, surveiller le risque ou souscrire une assurance, afin de réduire l'exposition au cyberrisque et de détecter l'évolution de nouvelles formes de cyberrisque.

---

1 Max J. Rudolph, *Emerging Risks Survey* – 2014, Joint Risk Management Section, Institut canadien des actuaires, Casualty Actuarial Society et Society of Actuaries, décembre 2015, p. 7.
2 Martin Eling et Jan Hendrik Wirfs, *Modelling and Management of Cyber Risk*, Association Actuarielle Internationale, 2015, pp. 5–7, http://www.actuaries.org/oslo2015/papers/IAALS-Wirfs&Eling.pdf.
3 Kailan Shang et Zakir Hossen, *Applying Fuzzy Logic to Risk Assessment and Decision-Making*, Joint Risk Management Section, Institut canadien des actuaires, Casualty Actuarial Society et Society of Actuaries, novembre 2013, pp. 32–50.

Kailan Shang, FSA, CFA, PRM, SCJP, est le cofondateur de la société Swin Solutions. Vous pouvez le joindre à kailan.shang@swinsolutions.com

Calcul de la probabilité d'une faille de cybersécurité aux fins de la tarification de l'assurance cybercriminalité

Steven Dionisi, CISSP, CISA, PMP, FFSI, CSSGB

La tarification de l'assurance cybercriminalité s'apparente à celle des assurances IARD ou de l'assurance responsabilité civile. Par exemple, les tarifs d'assurance habitation tiennent compte de l'existence de détecteurs de fumée dans l'habitation, de la construction en béton armé dans les zones de forte sismicité, de la construction en zones inondables ou propices aux tornades, et ainsi de suite. Dans le même ordre d'idées, l'assurance cybercriminalité tient compte de l'existence d'outils permettant de détecter et de prévenir les intrusions dans les réseaux, ainsi que de corrections logicielles, de centres de données sécurisés, et bien d'autres.

Dans ces cas, l'assurance est basée sur la non-survenance d'un événement. Le risque est réparti entre un grand nombre d'habitations pour couvrir celle touchée par une tornade ou une inondation. Les sociétés d'assurance, et leurs actuaires, ne s'attendent pas à ce que chaque habitation soit touchée par une tornade ou une inondation. Ce modèle ne fonctionne pas tout à fait dans le cas de la cybersécurité. Comme l'a fait remarquer John Chambers, chef de la direction de CISCO : « Il existe dans le monde deux types d'entreprise : celles qui ont été piratées et celles qui ne savent pas qu'elles l'ont été[1]. »

Comme la mort et l'impôt, le piratage sera considéré comme une chose inévitable. Cela étant, la protection de cybersécurité pourrait s'inspirer des produits d'assurance-vie. Il ne s'agit plus de se demander si l'entreprise sera piratée, mais plutôt s'il est probable qu'elle le sera au cours d'une certaine période. Pour calculer cette probabilité, il faut prendre en considération les facteurs susceptibles de favoriser l'existence d'un incident, de la même manière que les habitudes de vie (tabagisme) et d'autres facteurs sont pris en compte dans le calcul des probabilités de mortalité au cours d'une période.

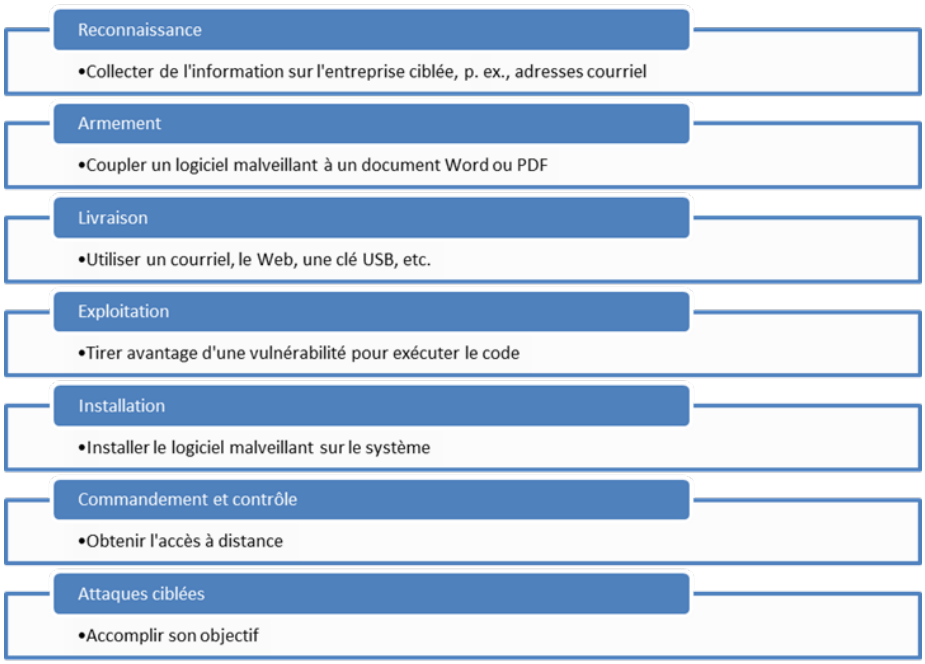
Les facteurs à l'origine d'incidents de cybersécurité sont exposés par Lockheed Martin et sont appelés l'Intrusion Kill Chain ou la Cyber Kill Chain (CKC)[2]. La CKC définit les sept stades d'une cyberattaque, où chacune exige la réussite de la précédente : la reconnaissance, l'armement, la livraison, l'exploitation, l'installation, le commandement et le contrôle, ainsi que les attaques ciblées. Étant donné que chaque étape de la CKC dépend de l'échec de celle qui la précède, les incidents de cybersécurité peuvent être modélisés de façon stochastique par l'analyse de Markov. Nous traiterons ici de l'application de l'analyse de Markov à la CKC comme moyen de quantifier la probabilité de défaillance d'un système de cybersécurité sur une période donnée ou un nombre d'attaques.

Cyber Kill Chain

La CKC de Lockheed Martin expose l'ensemble d'étapes ou de stades que suit l'attaquant pour s'introduire dans un réseau informatique et l'exploiter (voir figure 1). Chaque stade du processus consolide le stade précédent ou en tire avantage. Toute rupture de la chaîne bloque l'attaquant. La CKC s'inspire de la méthode créée par le ministère américain de la Défense pour décrire la structure d'une attaque.

La première étape de la chaîne est la reconnaissance. Les attaquants recherchent, identifient et choisissent des cibles. Durant ce stade, ils collectent les adresses courriel et balaient les ports du réseau de l'entreprise. Forts de cette information, ils se préparent à passer à l'étape suivante : l'armement. L'attaquant couple le logiciel malveillant à d'autres outils, tels qu'un document Word ou du contenu Adobe Flash. Une fois l'arme créée, la livraison peut avoir lieu. Par exemple, on peut procéder à la livraison en laissant des clés USB comportant un logiciel malveillant dans le parc de stationnement de l'entreprise ciblée, dans l'espoir que les employés accéderont aux clés USB à partir de leur ordinateur de travail. Si le logiciel malveillant s'installe dans le réseau informatique de l'entreprise, le code des attaquants est activé et se lance à la poursuite d'une application ou du système d'exploitation, c'est ce que l'on appelle, dans la CKC, l'étape de l'exploitation. Une fois qu'a lieu l'exploitation, les intrus tente d'avoir accès en installant dans le système un cheval de Troie ou une porte dérobée. Après l'étape de l'installation commence le stade du commandement et du contrôle. Le système infecté rappelle l'ordinateur des attaquants en établissant le commandement et le contrôle. Après les six premières étapes, les intrus peuvent partir à la poursuite des données de l'entreprise, ce que Lockheed appelle les attaques ciblées.

Figure 1 : Cyber Kill Chain de Lockheed Martin



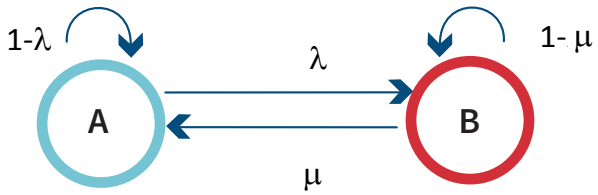
Il existe des outils ou des processus de sécurité de l'information permettant de détecter ou de prévenir les intrusions à chaque stade. Il est possible d'estimer la probabilité de réussite de l'attaquant, ou inversement, la probabilité de défaillance des outils de sécurité. Bien que deux des stades, reconnaissance et armement, aient lieu à l'extérieur du réseau informatique ciblé, la probabilité de réussite ou de défaillance peut être estimée. Par exemple, les systèmes de détection des intrusions peuvent surveiller le balayage de ports durant le stade de la reconnaissance ou utiliser l'analytique Web afin de déterminer si un attaquant collecte de l'information. Les méthodes de contrôle des processus, telles que la désinstallation d'Adobe Flash ou la suppression des droits d'administration locale, peuvent aussi être prises en compte dans les calculs de probabilité au stade de l'armement.

Analyse de Markov

L'analyse de Markov est utilisée pour de nombreux types de calculs de la fiabilité, pour lesquels une suite d'événements dépendants peut entraîner des défaillances du système. Cette analyse sert habituellement à calculer le temps moyen écoulé entre les défaillances des composants d'avion, des réseaux informatiques ou d'autres systèmes. Un type d'analyse de Markov est appelé chaîne de Markov. Il s'agit d'une méthode stochastique permettant de déterminer l'état probable d'un processus basé sur la probabilité d'événements, où chaque événement ne dépend que de celui qui le précède immédiatement. Par exemple, dans la CKC, le stade de l'exploitation n'a lieu que si le stade de la livraison a été réussi.

L'interdépendance des états peut être représentée par un diagramme de transition d'états (voir figure 2). Les états sont désignés par A et B. La probabilité de passer de l'état A à l'état B est désignée par λ et la probabilité de revenir à l'état A à partir de l'état B est notée par μ. La probabilité de rester dans un état particulier est représentée par 1 moins la probabilité de sortir de l'état présent. Dans le cas de l'état A, la probabilité de rester dans cet état est donnée par $1-\lambda$.

Figure 2 : Simple diagramme de transition d'états de la chaîne de Markov



Nous pouvons construire une matrice de transition à partir de ce diagramme (voir figure 3). La probabilité de rester dans l'état A est donnée par 1- λ (c'est-à-dire de passer de l'état A à l'état A). Comme nous l'avons vu, la probabilité de passer de l'état A à l'état B est désignée par λ .

Figure 3 : Simple matrice de transition

$$\begin{bmatrix} 1-\lambda & \lambda \\ \mu & 1-\mu \end{bmatrix}$$

La probabilité d'être dans un certain état après un certain nombre de cycles peut être représentée par l'équation suivante :

$$x_t = x_0 P^t$$

où

x représente le vecteur d'état du système

P désigne la matrice de transition et t le nombre de cycles à partir duquel le vecteur de probabilité sera calculé

x_0 désigne le vecteur d'état initial

Dans le simple exemple qui suit, l'état A est celui dans lequel une machine fonctionne et l'état B est celui dans lequel elle est en panne. La probabilité que la machine soit en panne une journée donnée (λ) est de 0,2 et la probabilité qu'elle soit réparée au cours d'une journée (μ) est de 0,3. L'état initial est représenté $x_0 = [1\ 0]$, ce qui signifie que la machine fonctionne. Les matrices de transition sont données par

$$P = \begin{bmatrix} 0{,}8 & 0{,}2 \\ 0{,}3 & 0{,}7 \end{bmatrix}$$

La probabilité que la machine soit en panne après trois jours est donnée par

$$x_3 = [1\ 0] * \begin{bmatrix} 0{,}8 & 0{,}2 \\ 0{,}3 & 0{,}7 \end{bmatrix}^3$$

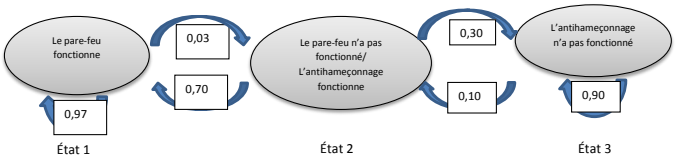
ce qui donne x_3 = [0,650 0,350]. Autrement dit, la probabilité que la machine soit en panne après trois jours est de 35 %.

Application de la chaîne de Markov à la Cyber Kill Chain

La chaîne de Markov peut être appliquée à la CKC pour calculer la probabilité de défaillance d'un système de cybersécurité. Nous utiliserons ici un simple exemple et des probabilités statiques relatives aux composants individuels. La sécurité de l'information est contrôlée par des mécanismes de prévention, de détection et de correction. La probabilité de rester dans un stade de la CKC est liée aux mécanismes de prévention, tandis que les mécanismes de détection et de correction sont regroupés pour calculer la probabilité de revenir à un stade précédent. Par exemple, un mécanisme de correction consisterait à apporter un correctif à un système d'exploitation vulnérable. Pour simplifier l'exemple, nous examinerons seulement deux stades.

La chaîne de Markov de la CKC est définie pour le passage de l'état 1 à l'état 3 en recourant aux deux stades suivants : livraison et exploitation. Dans l'état 1, la prévention de la livraison fonctionne (c'est-à-dire que le pare-feu bloque les pourriels selon un taux de 97 %). Dans l'état 2, la prévention de la livraison a échoué et la prévention de l'exploitation fonctionne (c'est-à-dire que les utilisateurs ont appris à ne pas ouvrir de pièces jointes .exe selon un taux de 70 % et ils rapportent l'existence du courriel). Dans l'état 3, la prévention de l'exploitation a échoué. Pour cet exemple, il y a une faible probabilité que l'exploitation soit détectée par d'autres outils (10 %) et la chaîne revient à l'état 2. La figure 4 illustre la probabilité de ces états à l'aide d'un diagramme de transition.

Figure 4 : Diagramme de transition de la Cyber Kill Chain



Selon ces probabilités, nous obtenons la matrice de transition suivante :

$$P = \begin{bmatrix} 0{,}97 & 0{,}03 & 0{,}0 \\ 0{,}70 & 0{,}0 & 0{,}30 \\ 0{,}0 & 0{,}10 & 0{,}90 \end{bmatrix}$$

Et le vecteur d'état initial est donné par x_0 = [1 0 0]. Après 100 cycles, le vecteur résultant est x_{100} = [0,853 0,036 0,109]. En d'autres termes, la probabilité que le logiciel malveillant soit exécuté est d'environ 11 % (c'est-à-dire que la probabilité d'être dans l'état 3 est de 0,109).

Conclusions

Le modèle CKC nous permet de regrouper en une suite logique les divers outils et processus utilisés en cybersécurité. Une fois établie cette suite logique, l'analyse stochastique de la fiabilité peut être utilisée pour calculer la probabilité de défaillance.

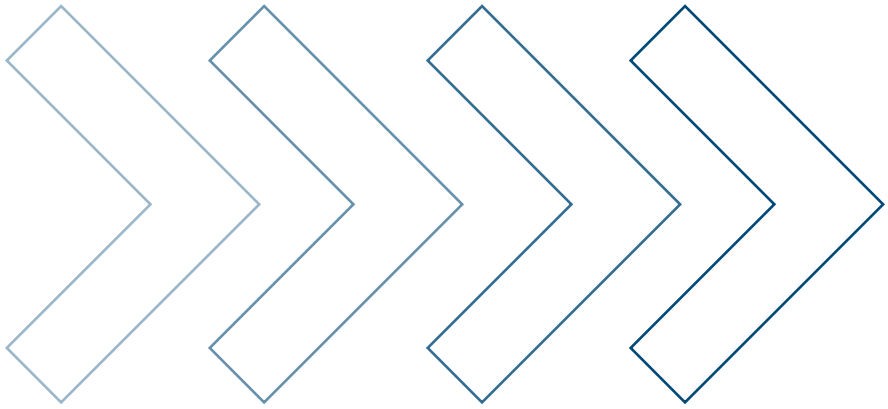
Dans cet exemple, nous avons utilisé un modèle très simple avec des probabilités statiques. Nous utiliserons des probabilités plus complexes et plus rigoureuses, comme celles tirées de la loi de Weibull, lorsque nous aurons mieux compris les taux de fiabilité des divers outils de sécurité. En outre, les entreprises divulguent plus souvent qu'auparavant des données sur les menaces informatiques dont elles sont l'objet. Un meilleur échange de données entre les entreprises sera pour beaucoup dans la compréhension des taux de fiabilité des outils de cyberprotection.

Comme nous l'avons vu, l'application d'une méthode de calcul de la fiabilité aux systèmes de cybersécurité peut faciliter la quantification de la probabilité d'une défaillance d'un système de cyberprotection. Une fois estimée la probabilité de défaillance, l'analyse actuarielle utilisée à l'égard des produits d'assurance pourrait être appliquée aux systèmes informatiques.

Les points de vue exprimés ici sont ceux de l'auteur et ne représentent pas forcément ceux de la Banque de la Réserve fédérale de Boston ni ceux de la Réserve fédérale américaine.

1 « John Chambers' 10 Most Memorable Quotes as Cisco CEO », *Networkworld*, 24 juillet 2015, http://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html.
2 Eric M. Hutchins, Michael J. Cloppert et Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, livre blanc, Lockheed Martin Corporation, n.d., http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

Steven Dionisi, CISSP, CISA, PMP, FFSI, CSSGB, est l'enquêteur des TI mandaté par la Federal Reserve Bank de Boston. Vous pouvez le joindre à steven.dionisi@bos.frb.org.



SOCIETY OF ACTUARIES