Quantification du cyberrisque pour les actuaires

Une approche économique fonctionnelle – Résumé

Quantification du cyberrisque pour les actuaires

Une approche économique fonctionnelle – Résumé

Unal Tatar — Université d'Albany – SUNY, Albany (NY), États-Unis

Omer Keskin — Université Old Dominion, Norfolk (VA), États-Unis

Hayretdin Bahsi — Université de technologie de Tallinn, Tallinn, Estonie

C. Ariel Pinto — Université Old Dominion, Norfolk (VA), États-Unis

Projet financé par les organisations suivantes :
Casualty Actuarial Society
Institut canadien des actuaires
Society of Actuaries

Quantification du cyberrisque pour les actuaires

Une approche économique fonctionnelle – Résumé

Section 1 : Introduction et aperçu

En raison de sa complexité, la sécurité du cyberespace est l'un des plus grands défis d'aujourd'hui. Le cyberenvironnement devenant davantage intégré au monde réel, l'impact direct des incidents de cybersécurité sur l'entreprise est également accru. L'analyse du cyberrisque représente le principal outil de gestion des conséquences des cyberévénements.

L'analyse des risques repose sur la réponse à trois questions :

1. Qu'est-ce qui pourrait mal tourner?
2. Quelle est la probabilité que cela se produise?
3. Quelle en serait l'incidence? (Kaplan et Garrick, 1981)

La formule générale d'analyse quantitative du risque, qui s'applique également à l'analyse du cyberrisque, est créée à partir de ces questions. Selon cette formule générale, le risque est un ensemble de triplets, $R = \{< S_i, P_i, X_i, >\}, i = 1,2,..,N$ où S_i est une identification de scénario, P_i est la probabilité de ce scénario, X_i est l'incidence de ce scénario, et N est le nombre de scénarios envisagés (Kaplan et Garrick, 1981).

Le National Institute of Standards and Technology (NIST) définit le cyberrisque comme suit : [traduction libre] « Risque de pertes financières, de perturbations opérationnelles, ou de dommages, découlant de la défaillance des technologies numériques utilisées pour les fonctions informationnelles ou opérationnelles introduites dans un système de fabrication par des moyens électroniques par suite de l'accès, de l'utilisation, de la divulgation, de la perturbation, de la modification ou de la destruction non autorisés du système de fabrication » (Stouffer et coll., 2019).

L'évaluation des répercussions, qui fait partie intégrante de l'analyse des risques, tente d'estimer les dommages possibles d'une cybermenace pour une entreprise ou une mission. Elle donne un aperçu du classement des risques par priorité, car elle intègre les exigences opérationnelles à l'analyse des risques afin de mieux équilibrer la sécurité et la convivialité. De plus, cette évaluation constitue le principal flux d'information entre les techniciens et les dirigeants d'entreprise. Il convient donc d'harmoniser efficacement les aspects technologiques et opérationnels de la cybersécurité (Bahsi et coll.,2018).

1.1 Limites des méthodes actuelles d'analyse du cyberrisque

Les méthodes actuelles d'analyse du cyberrisque présentent plusieurs limites. Le cyberrisque est souvent traité comme un problème de technologie de l'information plutôt qu'un élément essentiel de la gestion du risque d'entreprise (Moore, Dynes et Chang, 2015). Les méthodes existantes d'analyse du cyberrisque évaluent le risque principalement au niveau de la couche d'actifs (c.-à-d. l'évaluation des risques liés aux logiciels, au matériel et aux données par l'assurance de la qualité des logiciels, l'analyse des vulnérabilités, la détection des intrusions et l'analyse des logiciels malveillants), dans une certaine mesure à l'échelle de l'organisation (c.-à-d. les processus opérationnels), et rarement sur le plan des écosystèmes (c.-à-d. les chaînes d'approvisionnement) (U.S. Department of Homeland Security [DHS], 2018).

Une autre lacune a trait à l'insuffisance des mesures utilisées pour appuyer les décisions de placement, y compris la cyberassurance, la sécurité et les contrôles. Des mesures qualitatives et des termes opérationnels sont souvent utilisés comme indicateurs du cyberrisque plutôt qu'à titre de mesures financières quantifiées qui éclairent les décisions de placement. Les mesures qualitatives ou opérationnelles du cyberrisque entraînent, d'une part, un manque de compréhension des dirigeants d'organisations et, d'autre part, une réticence à apprécier l'importance des cyberrisques. Cette question a été énoncée dans le plan stratégique du Programme fédéral de recherche et développement sur la cybersécurité : [traduction libre] « Il n'existe pas de fondement scientifique pour l'analyse du risque de coût, et les décisions opérationnelles sont souvent fondées sur des données non scientifiques ou des arguments de qualité non quantifiés » (National Science and Technology Council, 2011). En outre, l'absence de quantification de la façon dont les placements dans des contrôles particuliers modifient le niveau de risque (c.-à-d. la mesure de l'efficacité des contrôles prévus ou mis en œuvre) constitue une autre limite des méthodes actuelles d'analyse du cyberrisque.

On note une variation du langage utilisé dans la communication du cyberrisque entre les décideurs en cybersécurité à tous les niveaux de gestion et les unités opérationnelles d'une organisation. À l'instar de nombreux autres domaines, la prise de décisions en matière de cybersécurité comporte trois niveaux : tactique, opérationnel et stratégique. La différence entre les paramètres décisionnels des gestionnaires de niveau tactique (p. ex., le nombre de systèmes vulnérables), opérationnel (p. ex., les contraintes juridiques et organisationnelles) et stratégique (p. ex., l'incidence sur l'ensemble des activités) crée une lacune en matière de communication, ce qui empêche l'évaluation exacte du cyberrisque.

L'incidence et la probabilité d'un scénario de risque peuvent varier au fil du temps. Très peu d'études traitent du changement de la vigueur et de la criticité des dépendances dans le temps et de la valeur des risques qui s'y rattachent.

Cette recherche a pour but d'élaborer un modèle d'analyse quantitative probabiliste du cyberrisque sur la façon dont sont reliés le risque rattaché à l'actif et les objectifs de l'organisation. Dans le cadre de cette méthode, nous tiendrons compte des répercussions en cascade au moyen de dépendances internes d'une organisation.

La méthode d'analyse du cyberrisque mise au point utilise des graphiques d'attaque probabiliste, qui reposent sur les vulnérabilités connues des logiciels et des topologies de réseau. Les capacités dynamiques d'évaluation du risque sont accrues dans le graphique d'attaque fondé sur des réseaux bayésiens. Le cadre proposé tirera également parti de la dépendance fonctionnelle. La cyberpropagation de l'incidence est modélisée dans les couches d'une entreprise et entre les différentes entreprises. Parmi les caractéristiques, mentionnons l'expression de l'incidence comme fonction de la perte de confidentialité, d'intégrité et de disponibilité (CID), et de nouvelles relations de dépendance mathématique reflétant la nature des cyberdépendances. Gardons en tête les définitions suivantes :

- La *confidentialité* consiste à [traduction libre] « préserver les restrictions autorisées à l'accès à l'information et à sa divulgation, y compris les moyens de protéger les renseignements privés et exclusifs » (McCallister, Grance et Scarfone, 2010).
- L'*intégrité* représente [traduction libre] « l'objectif de sécurité qui crée l'exigence d'une protection contre les tentatives intentionnelles ou accidentelles de porter atteinte à l'intégrité des données (la propriété selon laquelle les données n'ont pas été modifiées de façon non autorisée) ou l'intégrité des systèmes (la qualité dont dispose un système lorsqu'il remplit sa fonction prévue d'une manière non altérée, sans manipulation non autorisée) » (Stoneburner, 2001).
- La *disponibilité* consiste à [traduction libre] « assurer un accès rapide et fiable à l'information et son utilisation » (Ross, McEvilley et Oren, 2016).

La perte de confidentialité, d'intégrité et de disponibilité est mesurée dans l'étude afin de quantifier les répercussions des cyberattaques sur les systèmes d'entreprise. D'autres analyses quantifient les répercussions économiques au moyen de la perte de confidentialité, d'intégrité et de disponibilité.

Cette étude vise à élaborer un modèle générique qui peut être appliqué par n'importe quelle organisation. Aux fins de la validation de la méthode d'analyse du cyberrisque élaborée, des simulations et une analyse de sensibilité seront effectuées.

1.2 Gestion du cyberrisque du point de vue de l'actuariat

La gestion du cyberrisque du point de vue de l'actuariat pose problème. Dans le cas de l'assurance traditionnelle, les données historiques sur les sinistres sont habituellement privilégiées pour l'utilisation de modèles actuariels. Toutefois, dans le cyberdomaine, les données historiques sont insuffisantes pour deux raisons principales : (1) La cyberassurance est un domaine relativement nouveau et novateur qui ne comporte pas un long historique de plusieurs décennies et (2) les données existantes deviennent vite désuètes, car les menaces, les vulnérabilités et les méthodes d'atténuation évoluent rapidement (Böhme, Laube et Riek, 2017).

Certaines études dans la documentation regroupent les données actuellement disponibles sur les pertes liées à des cyberincidents dans le but d'obtenir une perte totale moyenne (Biener, Eling et Wirfs, 2015; NetDiligence, 2018). Toutefois, les résultats ne sont pas avantageux puisque les méthodes et les contextes des études varient de façon considérable. Même si Biener, Eling et Wirfs (2015) laissent à entendre que le coût moyen par cyberincident est de 40 millions de dollars pour 994 incidents entre 1971 et 2009, l'étude de NetDiligence (2016; 2018) conclut que le coût moyen pour 1 201 sinistres entre 2013 et 2017 s'établit à 0,7 million de dollars. Cette différence s'explique, comme en font foi les deux raisons principales mentionnées précédemment. En raison de ces problèmes, les actuaires craignent d'utiliser ce genre de données dans les analyses. Le contexte éventuellement différent de chaque cyberincident peut s'ajouter aux différences entre les diverses entreprises de secteurs différents.

Les problèmes liés à la modélisation du cyberrisque qui dépend des données ont forcé les actuaires à adopter d'autres approches pour estimer la modélisation des pertes et la quantification du cyberrisque. Le modèle élaboré dans l'étude aide les actuaires à évaluer les cyberrisques que pose un réseau de technologies d'information et de communications (TIC) d'entreprise afin de prendre des décisions bien éclairées au sujet de la garantie des polices, des primes et des franchises. Le modèle élaboré peut être appliqué à tout réseau de TIC d'entreprise en personnalisant les intrants en conséquence.

1.3 Contribution

La contribution du milieu scientifique à cette recherche vise à mieux comprendre et à mieux évaluer l'impact dans le contexte de l'analyse du cyberrisque. L'un des résultats les plus novateurs est l'élaboration d'un modèle probabiliste quantitatif du risque fondé sur un graphique pour déterminer la propagation de l'impact à chaque couche et entre toutes les couches (c.-à-d., les actifs, les services ou les processus opérationnels) d'une organisation.

Cette méthode évalue les étapes des attaques et évalue comment les autres composants sont affectées par la connexion de graphiques d'attaques probabilistes alimentés par le système commun de notation des vulnérabilités (CVSS) et les réseaux de dépendance fonctionnelle. La méthode proposée permet de hiérarchiser les vulnérabilités en fonction de leur impact et de promouvoir de meilleures décisions de placement en fonction des risques.

À l'heure actuelle, ce rapport est disponible en anglais seulement. La version française paraîtra au cours des prochains mois. Une version anglaise du résumé est également disponible.