CHUBB®

Cyber COPE®

Transformer la souscription de cyberrisques

Russ Cohen et Patrick Thielen

« Combien d'étages y a-t-il dans votre immeuble de bureau? »

« À quelle distance se trouve la borne d'incendie la plus proche? »

« L'immeuble est-il doté d'un système d'alarme? »

« Vous trouvez-vous en zone inondable? »

Les compagnies d'assurance posent des questions simples et objectives comme celles-ci afin de souscrire adéquatement les risques à assurer.

Par contre, les questions posées dans le cadre de la souscription de cyberrisques ne sont pas toujours aussi simples.

Par exemple, savez-vous si votre entreprise chiffre toutes ses données sensibles, dote d'un pare-feu tous ses points d'accès Internet, ou installe les correctifs des vulnérabilités connues sur tous ses systèmes informatiques? Savez-vous au moins à qui le demander?

Les réponses à ces questions et à d'autres liées aux cyberrisques sont souvent complexes et subjectives. Cette absence de simplicité et d'objectivité rend l'évaluation des cyberrisques de votre entreprise plus incertaine pour les assureurs. Par conséquent, il devient plus difficile pour vous d'obtenir l'assurance dont vous avez besoin à un prix raisonnable. Si le nombre d'étages de votre immeuble ou l'âge du système de gicleurs peut servir à l'évaluation des risques pour les biens de votre entreprise, pourquoi le nombre d'ordinateurs que vous utilisez n'influence-t-il pas l'évaluation de vos cyberrisques? En fait, ce nombre peut avoir une influence si l'on applique à la technologie la méthode COPE – un modèle de souscription d'assurance de biens éprouvé – afin d'améliorer la qualité générale des données et de la souscription de cyberrisques.

Unir l'art et la science pour la souscription de cyberrisques

COPE (construction, occupation, protection et expositions) est une méthode simple et efficace d'examiner différents facteurs afin d'aider les souscripteurs à prendre de meilleures décisions quant aux risques portant sur les biens. Comment pouvons-nous donc appliquer COPE à la technologie afin d'améliorer la qualité générale des décisions concernant la souscription de cyberrisques? D'abord, la procédure doit être assez simple pour que n'importe qui puisse l'utiliser, peu importe son niveau de connaissances techniques. Ensuite, elle doit fournir des facteurs objectifs et subjectifs, conformément au modèle COPE initial. Finalement, elle doit favoriser le partage de renseignements afin que les organisations puissent apprendre les unes des autres dans l'optique d'atténuer les sinistres éventuels. Essentiellement, elle doit permettre de déterminer l'origine de ces sinistres.

Le résultat : Cyber COPE®, un nouveau modèle de souscription de cyberrisques visant à simplifier et à améliorer l'évaluation des cyberrisques et des risques liés à la protection de la vie privée.

Transformation de COPE en Cyber COPE

Pour appliquer le modèle COPE à l'exposition aux cyberrisques, nous remplaçons d'abord la catégorie *Construction* par une catégorie *Composants*. Comme la construction d'un immeuble physique, les *composants* représentent les éléments de données objectifs qui fournissent des renseignements sur la cyberstructure d'une entreprise, comme le nombre d'ordinateurs, de comptes d'utilisateur et de connexions Internet.

Ensuite, nous remplaçons la catégorie *Occupation* par une catégorie *Organisation*. Rappelant la composition de l'entreprise, l'*organisation* englobe les éléments de données objectifs liés aux personnes, aux processus, aux renseignements et à la stratégie globale de gestion des risques de l'entreprise. Il peut s'agir, entre autres, du secteur de l'entreprise, du nombre d'employés, du nombre d'entrepreneurs et des allocations budgétaires destinées à la cybersécurité.

Les deux derniers éléments du modèle COPE, *Protection* et *Expositions*, restent tels quels. Cependant, au lieu de biens concrets, le but est de capturer les éléments de données subjectifs qui décrivent la cyberdéfense (*Protection*) d'une entreprise et les faiblesses de sa cybersécurité (*Expositions*). Parmi les exemples d'éléments relevant de la *protection*, citons le chiffrement, l'authentification multifactorielle et la détection d'intrusion. Dans la catégorie *Expositions*, on retrouve les auteurs de menace, les erreurs système et les vulnérabilités logicielles.

Figure 1

Le tableau à droite résume la transformation de COPE à Cyber COPE :

COPE	Cyber COPE	Type de facteur	Exemples d'éléments de données
Construction	**Composants**	Objectif	Nombre de terminaux et de connexions réseau, versions logicielles et emplacements des centres de données
Occupation	**Organisation**	Objectif	Secteur du titulaire de police, qualité des politiques relatives à la technologie de l'information et à la sécurité, et conformité aux normes de l'industrie
Protection	**Protection**	Subjectif	Politiques de conservation des données, authentification multifactorielle, surveillance et politiques d'intervention ou de préparation en cas d'incident
Expositions	**Expositions**	Subjectif	Motif politique ou criminel, types de sous-traitance et type ou quantité de données sensibles

Composants

Quels sont les éléments de données qui composent la cyberstructure d'une entreprise? Lors de l'attribution d'éléments à la catégorie *Composants*, il est important de comprendre que les données doivent être aussi objectives que possible. Par conséquent, l'objectif est d'évaluer chaque élément par rapport à la simplicité de la question « Combien d'étages y a-t-il dans un immeuble? ». Cette question que tout le monde peut comprendre collecte des données objectives. Voici quelques exemples de questions qui fourniraient des éléments de données mesurables pour les *composants* :

- Combien de comptes d'utilisateur ou d'identifiants sont utilisés par vos employés?
- Combien d'applications logicielles votre environnement comporte-t-il?
- De combien de connexions Internet publiques votre entreprise dispose-t-elle?
- À combien de tiers avez-vous recours pour le stockage ou le traitement des données de votre entreprise?
- Combien de terminaux (c.-à-d. ordinateurs de bureau, ordinateurs portables ou appareils mobiles) votre entreprise utilise-t-elle?

L'*accessibilité*, cet autre facteur clé de la souscription d'assurance de biens, est également importante ici. Les entreprises commencent à partager leurs données avec des tiers afin de les faire analyser pour atténuer le niveau de cyberrisque global. L'augmentation de cette tendance et du nombre d'entreprises en mesure d'accéder aux données fera en sorte que tout le secteur sera mieux équipé pour évaluer les risques et réduire les expositions éventuelles.

Organisation

Les éléments de données qui appartiennent à la catégorie *Organisation* sont plus évidents que les *composants* bien qu'ils doivent également être aussi objectifs que possible pour assurer l'efficacité du modèle. Pour l'*organisation*, l'objectif est de recueillir des données qui permettent au souscripteur de déterminer les cybervulnérabilités d'une entreprise du point de vue du conseil d'administration ou de la haute direction. À des fins d'objectivité, les questions qui concernent l'*organisation* s'inspirent également de la question concernant le nombre d'étages d'un immeuble :

- Dans quel secteur votre entreprise exerce-t-elle principalement ses activités?
- Quelles sont les normes de sécurité de l'industrie auxquelles vous vous conformez?
- Vos accords de tiers traitent-ils explicitement de la sécurité?
- À quel niveau de marchand de l'industrie des cartes de paiement (PCI) votre entreprise appartient-elle?
- Quel pourcentage du budget informatique est alloué à la cybersécurité?

Protection

Les éléments de données de la catégorie *Protection* sont axés sur les contrôles de sécurité qui existent au sein d'une entreprise afin de prévenir les cyberincidents. Ils ressemblent à ceux dont traitent les normes de sécurité existantes, comme celles du NIST, de la PCI et ISO 27001. Il serait facile d'insérer des questions provenant de ces normes dans une application de cyberassurance, mais elles sont beaucoup trop longues pour que les organisations, particulièrement les petites entreprises, puissent y répondre. De plus, peu de compagnies d'assurance, de courtiers ou d'agents auront les ressources nécessaires pour évaluer tous les points de données fournis par ces normes.

Par conséquent, les éléments de données sur la *protection* sont basés sur un ensemble de contrôles de sécurité de base. Bien que de nouveaux types d'attaques surviennent sans cesse, les mêmes vulnérabilités sont exploitées d'une année à l'autre. Par exemple, les rançongiciels sont un type de logiciel malveillant qui restreignent l'accès aux fichiers jusqu'à ce qu'une rançon soit versée au cybercriminel.

Par contre, ils ne fonctionnent généralement que si quelqu'un clique sur un lien malveillant dans un courriel, omet de sécuriser un port ouvert accessible par Internet ou ne met pas à jour les logiciels vulnérables. Une entreprise peut atténuer ces risques au moyen d'une formation, d'une sensibilisation et d'une hygiène informatique adéquates.

L'objectif de la *protection* est de déterminer les contrôles de sécurité essentiels aux entreprises tout en permettant un certain niveau de subjectivité. Comme les éléments de données objectifs des catégories *Composants* et *Organisation* sont obtenus en premier, les éléments subjectifs de la catégorie *Protection* sont d'abord définis en termes simples afin que le souscripteur puisse élaborer des questions subjectives visant à obtenir des renseignements supplémentaires. Voici quelques exemples de termes et de questions :

1. **Intervention en cas d'incident :** Avez-vous un plan d'intervention en cas d'incident que vous mettez à l'essai au moins une fois par année?
2. **Gestion des vulnérabilités :** Avez-vous mis en place un processus pour cerner les faiblesses des systèmes informatiques, les évaluer et y remédier?
3. **Gestion des correctifs :** Avez-vous mis en place un processus d'installation des mises à jour de sécurité des applications et des logiciels lorsque le fabricant en fournit?
4. **Authentification multifactorielle :** Avez-vous implémenté l'authentification multifactorielle pour les systèmes de courriel, l'accès réseau à distance et les applications contenant des données sensibles?
5. **Détection et intervention au niveau des terminaux :** Avez-vous mis en œuvre un antimaliciel qui détecte les menaces non détectées par les antivirus traditionnels (p. ex. les exploitations du jour zéro ou les menaces avancées persistantes) et y réagit?
6. **Sécurité périphérique des courriels :** Disposez-vous d'un logiciel qui analyse les courriels et met en quarantaine ceux qui pourraient comporter du contenu malveillant (p. ex. des pièces jointes ou des liens)?

Ces termes sont numérotés, car il est important d'établir un ordre de priorité pour les éléments recueillis dans cette catégorie. Par exemple, les êtres humains représentent statistiquement le maillon faible de la cybersécurité. En augmentant les questions sur les programmes de sensibilisation à la sécurité et l'authentification, vous faites passer en premier votre investissement dans la prévention des sinistres.

Expositions

Lorsque nous pensons aux *expositions* qui concernent les biens, ce sont les catastrophes naturelles, les incendies, les inondations, le vol, etc., qui nous viennent à l'esprit. Afin d'imiter cette méthode dans le cadre du modèle Cyber COPE, nous devons comprendre les caractéristiques sous-jacentes des expositions aux cyberrisques pour déterminer celles qui s'appliquent à une entreprise en particulier.

La principale caractéristique est que ces expositions ne sont généralement pas maîtrisables. Par exemple, dans le domaine de l'assurance de biens, nous pouvons tenter de prédire un ouragan, mais nous n'avons aucune influence sur l'ouragan même. Dans le même ordre d'idée, en cyberassurance, nous pouvons tenter de prédire les entreprises qui pourraient être victimes d'un piratage, mais nous n'avons aucune influence sur la motivation ou la détermination des cybercriminels.

Tout comme les inondations et les tremblements de terre, certains cyberrisques sont susceptibles de devenir des événements généralisés touchant de nombreux titulaires de police. Les cybercatastrophes éventuelles pourraient être pires qu'une catastrophe naturelle, car les cyberévénements ne font pas l'objet de limites géographiques ou temporelles. En conséquence, un souscripteur en cyberassurance doit faire comme un souscripteur en assurance de biens qui évalue les expositions et les protections en fonction des catastrophes naturelles et des structures assurées. De plus, tout comme le gestionnaire d'un portefeuille de polices d'assurance de biens doit s'assurer qu'aucun événement ne pourrait entraîner des sinistres au-delà de la propension au risque d'un assureur, l'assureur doit de son côté quantifier objectivement et contenir les cyberrisques systémiques présents dans son portefeuille.

Le partage de renseignements, l'établissement d'un principe commun de souscription et l'utilisation d'une structure de garanties quantifiable en cas d'événements généralisés permettront au secteur de l'assurance de mieux protéger les organisations contre les expositions aux cyberrisques.

Puisque ces facteurs sont plus subjectifs, les éléments compris dans la catégorie *Expositions* sont définis en termes simples plutôt qu'au moyen de questions suggestives :

- Traitement des données sensibles : données de l'entreprise et de ses clients
- Attaques ciblées : auteurs de menace motivés
- Attaques non ciblées : erreurs humaines
- Ressources tierces : sous-traitance
- Vulnérabilités logicielles courantes : Java, Flash, Windows
- Erreurs des systèmes ou des logiciels : erreur de programmation
- Exigences réglementaires ou de conformité : PCI, LPRPDE
- Événements généralisés : dépendance à l'égard de technologies largement utilisées

À titre d'exemple, examinons le premier composant mentionné : le traitement des données sensibles. Idéalement, une entreprise peut contrôler l'accès à ce type de données. Par contre, si vous stockez et traitez des millions de transactions par carte de crédit, vous externalisez peut-être cette fonction à une entreprise tierce de traitement des paiements. L'exposition existe toujours, mais la protection ne relève plus de vous. Si plusieurs entreprises ont recours au même fournisseur, votre exposition augmente considérablement en raison de l'agrégation des risques. C'est particulièrement vrai pour votre assureur si un grand nombre de ses titulaires de police utilisent ce même fournisseur.

Cyber COPE : la nouvelle ère de la souscription de cyberrisques

Dans les années 1700, le risque d'incendie empêchait de nombreux propriétaires commerciaux de souscrire l'assurance dont ils avaient besoin. Au fil du temps, le secteur a adopté le modèle COPE. De nos jours, ce sont les cyberrisques qui sont en émergence. Les sinistres potentiels sont associés à des coûts élevés et les menaces changent si rapidement que les entreprises ont de nouveau de la difficulté à obtenir l'assurance dont elles ont besoin.

Le modèle COPE est efficace, car il utilise des questions simples et directes pour recueillir des données objectives et subjectives afin d'évaluer les risques avec plus de précision.

Il a résisté à l'épreuve du temps grâce à la collaboration de nombreuses parties au partage et à l'analyse des données recueillies dans le but d'utiliser les résultats pour cerner à l'avance les faiblesses afin que les entreprises puissent mieux protéger leurs investissements à l'avenir.

De même, le modèle Cyber COPE a été conçu dans une optique de convivialité tout en offrant aux souscripteurs un bon équilibre entre objectivité et subjectivité. Il pave également la voie pour que le secteur de l'assurance puisse commencer à éliminer les obstacles historiques qui nuisent au partage de renseignements. En partageant ses renseignements et en établissant un principe commun pour la souscription de cyberrisques en constante évolution, le secteur sera mieux en mesure d'offrir une couverture et des solutions adéquates afin de protéger les organisations contre les expositions aux cyberrisques.

Le modèle Cyber COPE présente d'excellentes occasions d'innover en matière de souscription de cyberrisques, particulièrement en ce qui concerne les catégories *Composants* et *Expositions*. Chez Chubb, nous continuons de collaborer avec des chefs de file du secteur pour mieux définir les facteurs objectifs liés à des expositions aux cyberrisques précises. Ce type de collaboration est essentiel pour déterminer les meilleures mesures qui contribueront à l'atténuation des risques de cyberattaques. Toutes les organisations peuvent bénéficier de cette collaboration dans le cadre de laquelle nous recueillons et analysons les données afin de mieux prédire la fréquence et la gravité des cyberattaques et l'agrégation des risques.

À propos des auteurs

Russ Cohen est vice-président, Cyberrisques, et spécialiste de pratique technologique chez Chubb, où il aide les titulaires de police à analyser leurs expositions aux cyberrisques et à réagir en cas de cyberévénements. Il encourage également l'innovation dans les domaines de la souscription de cyberrisques, des réclamations et de l'actuariat. Fort de plus de 16 ans d'expérience en cybersécurité et en technologie, M. Cohen a occupé différents postes, dont celui de pirate éthique, aussi appelé « chapeau blanc ». Il détient une certification CISSP (*Certified Information Systems Security Professional*; professionnel en sécurité des systèmes d'information) en plus d'être un membre actif de diverses organisations spécialisées en sécurité, notamment InfraGard et (ISC)2.

Patrick Thielen est vice-président principal, Risques financiers, chez Chubb et spécialiste des produits d'assurance erreurs et omissions pour les domaines des cyberrrisques et de la technologie en Amérique du Nord. Il faisait partie des équipes de direction responsables du lancement de la division des assurances pour petites entreprises; des produits Gestion des cyberrisques d'entreprise, DigiTech® et Chef d'œuvreMD; et de la cyberprotection Blink. Fort de 20 années d'expérience en cyberassurance et en assurance des technologies, M. Thielen dirige actuellement les efforts de Chubb pour améliorer et élargir les solutions de cyberassurance et d'atténuation des risques pour les entreprises de toutes tailles ainsi que pour les particuliers et les familles.

Notes de fin

1 Christopher J. BOGGS, *Property and Casualty Insurance Concepts Simplified: The Ultimate "How to" Insurance Guide for Agents, Brokers, Underwriters and Adjusters*, États-Unis, Wells Media Group, Inc., 2010.

2 CyberAcuView (2021) : https://cyberacuview.com/press-release-june-2021/

Chubb. Insured.℠

www.chubb.com/ca-en/business-insurance/cyber-security.html