Gestion du risque

REVUE 41 • MARS 2018

SECTION CONJOINTE DE LA GESTION DU RISQUE

Entretien avec un chef de la gestion du risque : entrevue avec Nick Silitch

Page 6

Gestion du risque

Revue 41 • Mars 2018

Publié trois fois par année par le Conseil de la Section conjointe sur la gestion du risque de la Casualty Actuarial Society, de l'Institut canadien des actuaires et de la Society of Actuaries.

475 N. Martingale Road, Suite 600
Schaumburg, Ill 60173-2226
Phone: 847-706-3500 Fax: 847-706-3599
www.soa.org

Ce communiqué est gratuit pour les membres de la section. Les numéros courants sont disponibles sur le site Web de la SOA (www.soa.org).

Pour se joindre à la section, il suffit de mettre la main sur le formulaire d'adhésion affiché dans la page Web de la Section conjointe sur la gestion du risque à http://www.soa.org/jrm.

Dates de publication
Mois de publication : août 2018
Date de tombée : le 24 avril 2018

Le coin du président

par C. Ian Genno

Alors que vous vous apprêtez à parcourir les pages de ce numéro, j'aimerais attirer votre attention sur quelques-unes des initiatives auxquelles travaille la Section conjointe sur la gestion du risque depuis ma dernière mise à jour du numéro de décembre 2017.

Kailan Shang a terminé un document de recherche portant sur l'engagement efficace des parties prenantes à la gestion du risque d'entreprise (GRE), un projet supervisé et financé par la Section. Lorsque l'on interroge des professionnels de la gestion du risque au sujet de leur expérience pour ce qui est de susciter l'engagement des parties prenantes de la GRE (membres du conseil d'administration, hauts dirigeants et titulaires de fonctions sur les trois lignes de défense), on découvre plusieurs choses intéressantes. On y découvre notamment des perspectives quant aux besoins des parties prenantes, aux stratégies de communication en matière de GRE, à la quantification des avantages d'investir dans la GRE, à la mise en place des mécanismes de reddition de comptes afin d'assurer le respect des politiques en matière de risque ainsi qu'à l'évaluation et l'amélioration de la culture du risque au sein des organisations. On illustre par des exemples la façon d'appliquer ces concepts de façon efficace dans la pratique.

Parmi les autres travaux, mentionnons notre enquête périodique sur les risques émergents et notre collaboration à l'Indice actuariel climatique, qui contribuent à répondre aux besoins des actuaires en ce qui concerne la modélisation et la tarification de la couverture des risques de catastrophe. Ces deux concepts de recherche suscitent de plus en plus d'attention dans le monde des affaires et sur la place publique. Pour en savoir plus au sujet de la recherche en matière de gestion du risque, consultez le www.soa.org/jrm.

Le travail de planification et de coordination se poursuit en ce qui a trait aux séances sur la gestion du risque qui seront offertes à l'occasion de plusieurs conférences actuarielles à venir. Les membres du conseil de section présentent leur point de vue et offrent leurs suggestions au sujet des thèmes, des sujets pertinents et des conférenciers. Dans certains cas, la Section offre également un soutien sous forme de commandite afin d'assurer la viabilité financière des conférences et de réduire les frais d'inscription imposés aux participants.

Nous travaillons à l'élaboration de notre série de webémissions pour 2018, laquelle offre aux membres un moyen rapide et économique d'accéder à des activités de perfectionnement professionnel continu (PPC) portant sur des questions de l'heure tout en évitant les déplacements et les coûts connexes. Les membres ont également accès gratuitement aux webémissions de 2015 et 2016 commanditées par la section (datant d'un an ou plus). Les enregistrements offerts seront mis à jour chaque trimestre. Pour accéder aux enregistrements gratuits, les membres doivent ouvrir une session dans la communauté de la Section conjointe sur la gestion du risque à https://engage.soa.org.

Le Symposium sur la GRE, qui se tiendra à Miami les 19 et 20 avril, approche à grands pas. Si vous êtes libres et que vous n'êtes pas encore inscrits, je vous invite à consulter la liste des sujets et des conférenciers. Offrant un vaste contenu et une panoplie de points de vue, le symposium constitue également une occasion précieuse de discuter et de faire du réseautage avec bon nombre de collègues du domaine de la gestion du risque. Vous trouverez de plus amples renseignements à www.ermsymposium.org.

En plus de planifier diverses façons d'offrir du contenu de PPC en personne et en ligne, nous envisageons des façons de faciliter encore davantage les activités de réseautage pour les membres de la Section, que ce soit au moyen de commandites ou en prenant part à la coordination des conférences sur la gestion du risque dans le cadre d'événements locaux.

Comme toujours, nous continuons de consacrer notre temps et notre attention au présent bulletin d'information. Je tiens à souligner l'initiative importante prise par les rédacteurs et le personnel pour trouver des articles intéressants et pertinents; sans leurs efforts incessants, ce bulletin ne pourrait exister. J'espère que cette lecture vous plaira.

C. Ian Genno, FSA, FICA, CERA, est directeur et chef du groupe chargé de l'assurance hypothèques au Bureau du surintendant des institutions financières du Canada. On peut le joindre à *ian.genno@osfi-bsif.gc.ca*.

Lettre de la rédactrice

par Baoyan Liu (Cheryl)

L'industrie des assurances moderne est née au 17e siècle, lorsque fut officiellement établie la première compagnie d'assurance contre les incendies. L'industrie a ensuite intégré les assurances sur les biens, l'assurance-vie, l'assurance accident et l'assurance maladie et a raffiné son modèle d'affaires au cours des 400 dernières années afin de s'adapter aux exigences imposées par les risques associés au développement social. En 2018, le secteur des assurances est aux prises avec de nouvelles perturbations attribuables à l'évolution technologique. En effet, les nouveaux agents perturbateurs et la transformation numérique ont pour effet de redéfinir le marché.

Les perturbations technologiques touchant la tarification des produits, la souscription, les opérations, la conduite des affaires et les attentes de la clientèle en matière d'assurances figurent au sommet de la liste des préoccupations de l'industrie. Dans la foulée de la transformation de la plateforme numérique, le contexte cybernétique est également au cœur des discussions portant sur la gestion des risques. Dans ce premier numéro de *Gestion du risque* en 2018, j'aimerais vous parler de certains articles axés sur les risques les plus importants au sein de notre industrie.

Tout d'abord, la Section conjointe sur la gestion du risque est ravie d'annoncer la création d'une nouvelle rubrique intitulée *Entretien* avec un chef de la gestion des risques, dans laquelle nos actuaires partenaires chevronnés s'entretiennent avec les plus grands gestionnaires de risques de l'industrie des assurances, qui se prononcent sur les grands enjeux auxquels fait face l'industrie. Notre premier entretien met en vedette Nick Silitch, de la Prudential Financial. Il partage avec Tony Dardis et Awa Kone son point de vue sur la culture du risque, le recours au capital économique et le rôle des actuaires en gestion du risque.

Pour assurer une gestion des risques efficace, il convient d'atteindre un bon équilibre entre la connaissance du marché et son propre jugement. Dave Ingram, de Willis Towers Watson, présente un sommaire des *risques les plus dangereux pour les assureurs en 2018* selon l'enquête menée par le cabinet. Alors que les sociétés d'assurances adoptent de plus en plus la numérisation, la cybersécurité et la cybercriminalité sont constamment classées parmi les risques les plus importants, une situation qui n'a certainement pas fini d'évoluer. Les risques classiques tels que la déviation de l'orientation stratégique, les réclamations attribuables aux catastrophes naturelles, la concurrence et les risques associés à la tarification et aux produits figurent également dans la liste des dix risques les plus importants.

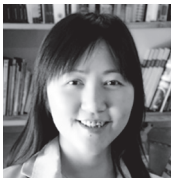
Depuis plusieurs années, l'enquête d'EY auprès des chefs de la gestion des risques (CGR) en assurances assure le suivi du développement de la gestion des risques et de l'évolution des priorités de ces CGR. Dans ce numéro, Chad Runchey et David Paul présentent les principales observations issues de l'enquête d'EY intitulée *EY Insurance CRO Survey—Shifting from Defense to Offense* (Sondage d'EY sur les chefs de la gestion des risques : de la défensive à l'offensive).

Les cyberrisques et la cybersécurité figurent au premier rang des risques les plus dangereux selon un sondage mené par Willis Towers Watson et constituent la préoccupation première selon l'enquête menée par EY auprès des CGR de l'industrie des assurances. Vu la plus grande susceptibilité des assureurs d'être visés par la cybercriminalité, il convient pour ceux-ci d'investir dans des systèmes de technologie de l'information plus efficaces. À l'échelle mondiale, les entreprises ont dépensé des milliards de dollars pour perfectionner leur système de défense interne contre la cybercriminalité. À l'occasion de l'Actuarial Research Conference de 2017, le professeur Shaun Wang, de la Nanyang Technological University, a présenté sa recherche intitulée *Modeling Optimal Level and Allocation of Cybersecurity Spending*. Nous sommes ravis de l'inviter à présenter à nos lecteurs, dans ce numéro de *Gestion du risque*, un sommaire de son exposé.

La gestion efficace du risque d'entreprise peut faire l'objet de longs débats. Dave Ingram nous le démontre dans un article en deux volets intitulé *La GRE en cinq mots*. La première partie a été publiée dans notre numéro de décembre dernier. Elle parle de résilience, de transparence et de discipline. Publiée dans ce numéro, la suite illustre l'importance de l'harmonisation et de la capacité d'adaptation.

Comme à l'habitude, nous présentons une liste des récents articles et documents de recherche susceptibles d'intéresser nos membres. Vous pourrez y trouver de plus amples renseignements sur un vaste éventail de sujets.

J'aimerais remercier tout particulièrement David Schraub et Kathryn Baker pour leur collaboration à la réalisation de ce numéro de mars de *Gestion du risque*. Bonne lecture! ▯



Baoyan Liu (Cheryl), FSA, CFA, est directrice principale, gestion des risques financiers à la société FWD Life Insurance Company (Bermudes) Limited à Hong Kong. On peut la joindre à *cheryl.by.liu@fwd.com*.

Le coin du personnel

par David Schraub

Le Symposium sur la GRE est le « bébé » de la Section conjointe sur la gestion du risque. Et de même qu'il s'écoule neuf mois de la conception à l'accouchement, de même il nous a fallu ce temps pour créer et développer le Symposium pour nos participants. Cette année, le Symposium aura lieu le 19 avril et tous y sont invités à vivre une expérience agréable.

Environ neuf mois avant la rencontre, un comité de bénévoles dévoués est mis sur pied. Pour ce faire, nous cherchons à réunir des gens d'horizons divers – des membres vivant aux États-Unis ou au Canada, qui possèdent de l'expérience en assurances IARD, en assurance-vie, ainsi que des membres de longue date et de nouvelles recrues. Le lieu de la réunion est fixé. Les premières discussions portent sur la philosophie de la réunion, soit le message particulier que nous véhiculerons tout au long du Symposium et qui incitera les participants à vouloir revivre cette expérience. Cette année, nous cherchons du nouveau contenu qui n'a jamais été présenté ailleurs et nous prévoyons consacrer beaucoup de temps à répondre à des questions, afin d'accroître la participation de l'assemblée.

Environ sept mois avant le Symposium, le comité détermine le nombre de séances nécessaires pour chaque grand thème et lance un appel à propositions afin de pouvoir tirer parti des excellentes idées potentielles des personnes externes au comité. De quatre à cinq mois avant la date prévue, les séances ou les propositions sont choisies. Les présentateurs sont informés. Le recrutement commence à prendre de l'ampleur, on commence à exploiter les propositions, mais aussi le savoir collectif des membres du comité. Les thèmes semblables sont regroupés et les contrepoints nécessaires sont fournis. On met la dernière main aux documents de commandite.

Environ trois mois avant la date prévue, l'ébauche du Symposium prend forme, c'est-à-dire que le personnel rassemble les titres et les descriptions (presque) définitifs de la totalité des séances générales et des séances en ateliers, et finalise l'organisation des séances afin que chaque créneau horaire offre une variété de séances pour tous les types de participants, depuis l'actuaire technique spécialisé en assurance-vie jusqu'au cadre supérieur chargé de la gestion des risques IARD, et tous ceux qui se situent entre ces deux extrêmes. Nous veillons également à ce qu'il n'y ait pas en même temps deux séances en ateliers qui plaisent au même public. Nous entrons en contact avec des commanditaires potentiels et nous leur exposons les avantages d'être mis en valeur au Symposium sur la GRE.

Certains membres du personnel se rendent sur place pour mieux visualiser l'espace réservé aux commanditaires, de même que la signalisation et les autres particularités des salles.

Environ deux mois avant la date prévue, les derniers créneaux ouverts sont attribués à des conférenciers. Les courriels d'invitation à s'inscrire sont envoyés. Les contrats avec les commanditaires sont finalisés et nous suivons de près le nombre d'inscriptions afin d'estimer le nombre de participants à chaque séance en ateliers. Est-ce que cinq tables rondes tiennent dans cette salle? Avons-nous assez d'espace pour les bras des fauteuils et le podium en prévision du panel sur les chefs de la gestion du risque?

Le dernier mois est habituellement beaucoup plus tranquille, car les principales tâches du personnel consistent à contrôler les inscriptions et les textes des présentations qui entrent…sauf lorsqu'il y a des questions urgentes à régler, et qu'une séance doit être organisée en suivant notre plan de rechange.

Il faut beaucoup de planification de la part du comité et du personnel pour que tout se déroule bien et que nos membres vivent une expérience enrichissante. Le comité se compose de 15 bénévoles et de nombreux membres du personnel de la Casualty Actuarial Society (CAS) et de la Society of Actuaries (SOA) travaillent ensemble au projet. La SOA a dirigé le Symposium en 2017 et le fera encore cette année, avant de passer le bâton à la CAS en 2019 et 2020 en ce qui concerne la plus grande partie des tâches. Cette alternance se passe assez bien, ce qui prouve une fois de plus la solidité des liens qui unissent nos associations et qui nous permettent d'offrir de l'excellent contenu à notre commun avantage. Voilà à quoi sert la Section conjointe sur la gestion du risque!

Nous comptons sur votre présence au Symposium cette année!

David Schraub, FSA, CERA, MAAA, AQ, est Fellow permanent, gestion du risque à la Society of Actuaries. On peut le joindre à *dschraub@soa.org*.

Entretien avec un chef de la gestion du risque : entrevue avec Nick Silitch

Nick Silitch, chef de la gestion du risque, Prudential Financial

La Section conjointe sur la gestion du risque est heureuse d'annoncer le lancement d'une nouvelle série d'articles intitulée « Entretien avec un chef de la gestion du risque ». Dorénavant, chaque numéro de *Gestion du risque* comportera une série de questions-réponses communiquées dans un esprit de franchise et d'ouverture et faisant intervenir un spécialiste du risque de premier plan qui œuvre dans le secteur de l'assurance. Ces entretiens relateront les grands enjeux auxquels le secteur est confronté et la façon dont les chefs de file du secteur y réagissent.

Dans ce premier article de la nouvelle série, *Gestion du risque* a le plaisir de s'entretenir avec Nick Silitch, chef de la gestion du risque (CGR) chez Prudential Financial. Comme Nick s'exprime sans détour et qu'il est toujours prêt à aviver le débat, l'idée d'avoir un entretien avec lui nous avait suscité de fortes attentes et nous n'avons pas été déçus.

L'entretien a été réalisé le 23 octobre 2017, au bureau de Nick, par Tony Dardis et Awa Koné, de la société Milliman.

Nick Silitch est l'un des spécialistes du risque les plus respectés et les mieux connus du secteur des services financiers. En sa qualité de CGR chez Prudential Financial, Nick supervise le processus décisionnel de gestion du risque et le profil de risque de Prudential à l'échelle mondiale. Nick assume la présidence du comité de gestion du risque d'entreprise de Prudential, qui est chargé d'évaluer les risques présents ou nouveaux pour la société, en plus d'être membre du comité de direction de Prudential. Nick est entré au service de Prudential en 2010 après avoir passé de nombreuses années dans le secteur bancaire, dont près de 30 ans auprès de la Banque de New York Mellon, et il est le seul à cet égard à avoir occupé un poste de cadre supérieur dans le secteur de l'assurance et le secteur bancaire.

Pour cet entretien de grande envergure avec Nick, nous avions une profonde envie d'avoir son point de vue sur des sujets tels que la culture du risque, l'utilisation du capital économique et le rôle de l'actuaire dans la gestion du risque, sujets sur lesquels Nick avait beaucoup de choses intéressantes à dire.

Q : Que faut-il faire pour réussir à instaurer une « culture du risque » dans une société d'assurances? Que peuvent faire les CGR pour intégrer la gestion du risque dans le processus décisionnel de leur société?

R : Je ne crois pas en l'existence d'une culture du risque. Ce que les sociétés doivent faire, c'est de commencer par jeter les bases *à la grandeur de la compagnie d'une culture distinctive de la société, qui inscrit l'importance de la gestion du risque dans les gènes de la société*. Il s'ensuit que toutes les décisions stratégiques sont le fruit d'un compromis entre, d'une part, le profil de risque et le coût d'opportunité des décisions et, d'autre part, le rendement potentiel. Si votre culture accorde de l'importance à la gestion du risque, vous aurez la possibilité de bâtir une société solide qui tiendra dûment compte du risque et du rendement, ce qui constitue un bon cadre pour une entreprise financière.

Considérons par exemple le concept de l'appétence au risque chez Prudential, auquel toute la société a souscrit, si bien que nous avons tous pour objectif commun de décider des meilleures stratégies en fonction de plusieurs optiques financières – qu'elle soit légale, économique ou de liquidité –, au profit des actionnaires et des autres parties prenantes. Bien que ce soit la fonction de gestion du risque qui quantifie et trace les grandes lignes de l'appétence au risque, celle-ci est la responsabilité de l'ensemble de la société : les secteurs d'activité, les fonctions administratives et le conseil d'administration. Résultat? La fonction de gestion du risque fait partie intégrante des discussions stratégiques et intervient d'entrée de jeu. Par exemple, dès que Prudential songe à faire une nouvelle acquisition ou lancer un nouveau produit, nous nous demandons si cette stratégie s'inscrit dans notre appétence générale au risque.

Q : Comment faites-vous donc pour savoir si vous possédez la bonne culture?

R : J'en prends conscience chaque jour. Ici, chez Prudential, nous avons vraiment adopté la politique de la porte ouverte, où tout le monde est encouragé à parler franchement. C'est un privilège remarquable de pouvoir y travailler et continuer à cultiver un environnement aussi sain.

Une chose est sûre : pour savoir si vous avez la bonne culture, il ne suffit pas de cocher des cases. Ce n'est pas quelque chose que vous pouvez tester ou gérer. Vous pourriez trouver cinq ou six attributs caractérisant une culture réussie qui tient compte du risque, mais le danger en ce sens est de gérer en fonction de ces attributs et de perdre ensuite l'essence de votre culture. Vous savez que vous possédez une excellente culture si, chaque fois que vous êtes confrontés à des décisions difficiles, vous prenez la bonne décision. Si vous avez la chance d'avoir ce type de culture, la crainte est que les choses puissent changer. Par conséquent, les conseils d'administration, les cadres supérieurs et les autres acteurs doivent veiller de près afin que le cœur de la culture soit axé sur l'ouverture des échanges et la prise en considération efficace du risque et du rendement.

Q : Quel rôle le capital économique (ou le capital interne) est-il à même de jouer? Quels sont les obstacles pouvant s'opposer à la réussite d'un programme de capital économique, et comment les assureurs peuvent-ils les surmonter?

R : Le concept de capital économique est l'une des idées les plus mal utilisées en finances au cours des 20 dernières années. La notion selon laquelle la modélisation de vos risques en fonction d'un certain intervalle de confiance vous permettra de mettre en équation un dollar de risque relié au marché par rapport à un dollar de risque d'investissement, d'assurance ou de risque opérationnel est certes attrayante, quoique difficilement réalisable et somme toute peu utile même lorsqu'on y parvient. La quantité de données que nous avons relativement à bon nombre de risques que nous prenons ne nous permet pas de faire des mesures précises au niveau de l'extrémité de l'aile de la distribution, du type 5 pour 10 000, sans devoir poser des hypothèses très audacieuses et souvent erronées. Qui plus est, les liens historiques existant entre ces risques peuvent disparaître à mesure que nous étudions les résultats au niveau de l'extrémité de l'aile de la distribution.

L'utilité de modéliser vos risques est de vous aider à mieux comprendre la forme de la distribution et le rôle que chaque élément peut jouer dans le développement de cette extrémité de l'aile. Il est essentiel qu'il y ait compréhension et entente générales (de la part des secteurs d'activité, du conseil d'administration et des fonctions administratives) quant à la nature des risques que vous prenez, avant d'engager un débat ouvert et transparent sur la gestion du risque et de permettre à la société d'assurer collectivement la gestion du risque et du rendement. C'est pourquoi les modèles de capital économique sont des outils importants du gestionnaire du risque, mais ils doivent être complétés par des simulations de crise déterministes et une compréhension des implications sur le capital réglementaire et les liquidités, si l'on veut que le cadre de gestion du risque soit efficace.

C'est seulement lorsque la société aura un portrait complet qu'elle pourra chercher à obtenir les meilleurs résultats pour l'ensemble des parties prenantes.

L'utilité réelle du capital économique est de servir d'outil de tarification des risques et de faciliter la mise en équilibre des profils de risque économique et de rendement dans le contexte d'optimisation sous des contraintes réglementaires de capital qui sont nettement plus prudentes.

Q : Avez-vous établi des priorités dans les limites d'appétence au risque?

R : Nous avons produit une déclaration de l'appétence au risque, mais nous n'avons pas défini de limites relatives à cette appétence. Il s'agit d'une idée générale de la façon dont nous voulons exploiter la société en période de crise. Ensuite, nous élaborons des indicateurs financiers qui traduisent ces idées générales et nous fixons des limites par type de risque afin de respecter les paramètres voulus. Nous avons en place des limites d'exploitation et des limites fixées par le conseil d'administration. Les limites d'exploitation laissent suffisamment de place, de sorte que nous risquons peu d'enfreindre celles fixées par le conseil.

Vous savez que vous possédez une excellente culture si, chaque fois que vous êtes confrontés à des décisions difficiles, vous prenez la bonne décision.

Q : Les actuaires jouent déjà un rôle dans la gestion du risque, mais ils pourraient sans doute en faire davantage. Comment voyez-vous le rôle des actuaires en la matière?

R : Bien entendu, les actuaires jouent un rôle immense dans le secteur de l'assurance et je ne crois pas qu'ils puissent faire mieux que ce qu'ils ont fait jusqu'ici dans leurs domaines de spécialité. Le titre d'actuaire s'accompagne de compétences très spécialisées et, bien que leurs compétences de base leur confèrent une grande valeur, cela ne signifie pas pour autant qu'ils soient qualifiés pour exercer en tant que spécialistes du risque. Par exemple, un professionnel de l'investissement très qualifié n'équivaut pas à un professionnel du risque d'investissement, de même qu'un professionnel des marchés n'équivaut pas à un professionnel du risque de marché et qu'un actuaire n'est pas assimilable à un professionnel du risque d'assurance. Chacune de ces compétences constitue une qualité essentielle d'un excellent professionnel du risque, mais celui-ci doit en posséder d'autres. Et cela est dû au fait que la gestion du

risque exige, pour l'essentiel, que l'on regarde les choses un peu différemment. De fait, un bon gestionnaire du risque doit :

- remettre en cause le statu quo;
- comprendre les résultats au niveau de l'extrémité de l'aile de la distribution, de même que la meilleure estimation;
- gérer la complexité découlant de l'existence de plusieurs priorités concernant une diversité d'enjeux;
- comprendre les cadres analytiques quantitatifs et qualitatifs du risque ainsi que les points forts et les points faibles des deux.

Il serait plus utile de se demander ici dans quelle mesure les professionnels du risque et de l'actuariat communiquent entre eux et collaborent. J'entretiens une relation très suivie avec notre actuaire en chef et nous échangeons ouvertement, et nous avons un immense respect réciproque. L'existence d'un dialogue fructueux entre les actuaires et l'équipe de gestion des risques est essentielle à la bonne gestion globale d'une société d'assurances.

Q : Ces dernières années, l'industrie a fait grand cas du développement des capacités de gestion du risque de modélisation. Selon vous, quelle est la clé de la réussite d'un programme de gestion du risque de modélisation?

R : Dans le secteur bancaire, le risque de modélisation comporte une forte composante humaine et prédictive, ce qui est différent du secteur de l'assurance. Toutefois, en assurance, la rigueur des modèles actuariels est testée régulièrement et assez rigoureusement. Chaque année, il y a validation des modèles par les auditeurs et des tests de sensibilité reliés aux hypothèses. Par conséquent, pour l'essentiel, les principes de base de SR 11-7 sont présents depuis des années dans les cadres de comptabilité, d'actuariat et d'information financière des sociétés d'assurances. Les sociétés doivent donc prendre soin de construire des programmes du risque de modélisation qui tiennent compte des forces existantes et qui permettent d'améliorer la documentation et la rigueur.

Comme c'est le cas pour les autres risques, il est essentiel, en ce qui concerne le risque de modélisation, de maintenir un dialogue ouvert et transparent sur l'élaboration et l'utilisation des modèles et sur l'intégration des modèles dans le plan d'affaires. Une gouvernance solide, transparente des hypothèses et des composantes clés du modèle est aussi essentielle.

Q : Le cyberrisque est un autre « risque opérationnel » qui attire de plus en plus l'attention ces dernières années. Selon vous, quels sont les plus grands problèmes liés au cyberrisque, et quelle est la meilleure façon de les gérer?

R : Le cyberrisque est en constante évolution et retient l'attention de toutes les parties.

De nos jours, il faut supposer que tout le monde peut avoir des renseignements personnels sur d'autres personnes, ce qui complique la vérification de l'identité des clients.

Chaque année, les banques perdent beaucoup d'argent en raison de la cybercriminalité. De plus, la cybermenace a évolué au fil du temps. Auparavant, la cybercriminalité était centrée sur des personnes. Mais, au cours de la dernière décennie, voire plus, les pirates informatiques ont gagné en sophistication et s'intéressent davantage aux entreprises. Notre industrie investit beaucoup de ressources dans la gestion de ce risque. Mais, le stratagème évolue constamment et la barre est sans cesse plus haute. C'est pourquoi nous – et l'industrie dans son ensemble – continuons de surveiller l'évolution de la cybermenace. Si cette escalade se poursuit sans arrêt, les entreprises devront à un moment ou un autre songer ensemble à modifier la façon dont elles communiquent avec leurs clients.

Q : Puisqu'il est question de menaces, à votre avis, quelles sont les principales tendances en matière de risque auxquelles les sociétés d'assurances seront confrontées au cours des trois à cinq prochaines années?

R : L'évolution dans l'utilisation des données et des plateformes numériques et technologiques changera les modèles d'affaires – la façon dont nous apprécions les risques, dont nous servons les clients – et, pendant ce temps, il y aura des risques opérationnels et des risques reliés aux produits.

Les percées dans la génétique et la gestion des maladies pourraient changer le monde – influant sur la mortalité et la longévité aux âges extrêmes, en plus de soulever des questions morales et juridiques complexes et d'entraîner éventuellement une distribution inégale de l'information sur les données personnelles.

De plus, il y a le changement climatique qui menace les assureurs IARD. Une hausse d'un degré des températures océaniques change les modèles de catastrophes de façon exponentielle.

Du côté de l'actif, l'industrie doit être consciente du fait que les entreprises dans lesquelles nous investissons sont confrontées aux mêmes enjeux économiques, politiques et technologiques que nous, dans le secteur de l'assurance, ce qui a pour effet de changer et de faire évoluer les modèles d'affaires. Par conséquent, du point de vue de l'investissement, nous devons garder un esprit d'ouverture. ▯

Awa Koné, FSA, CERA, MAAA, est experte-conseil chez Milliman. On peut la joindre à *Awa.Kone@milliman.com*.

Anthony Dardis, FSA, FIA, CERA, MAAA, est expert-conseil chez Milliman. On peut le joindre à *Anthony.Dardis@milliman.com*.

CERA

Chartered Enterprise Risk Analyst

CREDENTIAL

Meeting the Global Needs of Risk Management—the CERA

The way they think, the skills they bring, the roles they play. The Chartered Enterprise Risk Analyst (CERA) is a unique blend of the quantitative and the qualitative, combining actuarial discipline with the ability to think critically and creatively about risk, enterprise wide.

It's a level of expertise that can only come from the CERA credential from the Society of Actuaries—the most comprehensive and rigorous available. With a deep understanding of enterprise risk management and ethical standards that are beyond compare, the CERA is the risk professional that organizations trust to take them into the future—turning data into decisions to the benefit of their business.

The ERM Experts—the CERA

CERAnalyst.org

SOCIETY OF ACTUARIES®

Les risques les plus dangereux pour les sociétés d'assurances en 2018

par Dave Ingram

Note de la rédaction : Une version antérieure de cet article a été publiée dans le blogue Willis Towers Watson Wire.

Pour bien gérer les risques, il est impératif de trouver l'équilibre entre suivre l'opinion répandue du marché et se fier à ses propres idées. Chaque année, vous devez décider si l'un ou l'autre des risques que votre société prend est plus dangereux qu'il ne l'était l'an dernier. En outre, si de nouveaux risques se présentent pendant la période visée, il ne faut plus les classer comme étant « émergents », mais bien les inscrire à la liste des risques « présents ».

Voici une version de la démarche à cette fin. Nous avons remis à des professionnels du secteur des assurances une liste d'environ 70 risques que nous avons relevés dans les registres des assureurs en 2017. Plus de 230 personnes ont participé à l'exercice et ont classé plus de 8 000 éléments de risques. Plus de 20 % des participants étaient des actuaires et plus de la moitié œuvraient dans le secteur américain des assurances IARD. C'était la deuxième fois que nous faisions ce sondage et nous avons donc pu voir l'évolution des priorités depuis l'an dernier. Les résultats du sondage de l'an dernier peuvent être consultés à l'adresse : https://blog.willis.com/2017/01/2017-most-dangerous-risks-for-insurers/.

Nous avons constaté que les préoccupations des assureurs ont changé. En 2017, outre le risque numéro un, celui de la cybersécurité et du cybercrime, les préoccupations des assureurs sont en grande partie les risques auxquels ils ont toujours été confrontés soit la tarification, les technologies de l'information (TI), la concurrence, la souscription, la réglementation, les placements et les catastrophes.

En 2018, les répondants laissent entendre que bien des gestionnaires de sociétés d'assurances (ceux qui ont participé) craignent que l'industrie ne soit aujourd'hui en voie de devenir la prochaine victime de la vague de la modernité qui a eu pour effet de vider les centres commerciaux et d'obliger un nombre incalculable de librairies à fermer leurs portes. Parmi les 10 risques en tête de liste, on retrouve la technologie perturbatrice et l'incapacité à combler les besoins des consommateurs au moyen des approches conventionnelles. Plus particulièrement, la confiance à l'égard de la capacité de la direction à se frayer un chemin à travers ces problèmes a diminué; le risque de manque d'orientation stratégique et d'occasions ratées s'est hissé, passant du 8e au 3e rang.

Voici donc les 10 risques en tête de liste relevés dans le sondage. Vous pouvez comparer les principaux risques auxquels vous êtes vous-mêmes confrontés avec cette liste et le classement qui y figure.

1. **Cybersécurité et cybercrime** (1er en 2017)
   L'an dernier, le cyberrisque était en tête de liste tant dans les risques émergents que dans les risques présents. Les gestionnaires des risques estiment que le cyberrisque est un risque présent important et qu'il n'a absolument pas fini d'évoluer. Les assureurs élargissent leurs activités opérationnelles pour se numériser davantage et, du coup, deviennent aussi plus susceptibles au cybercrime et ont besoin d'intensifier leur cybersécurité. En outre, ce risque opérationnel pourrait se trouver au haut de la liste puisque les médias font grand état d'un nombre relativement limité d'incidents majeurs.

2. **TI/systèmes et lacunes technologiques** (3e en 2017)
   La plupart des assureurs avec lesquels nous nous sommes entretenus viennent tout juste de terminer ou ont entamé un important exercice de révision de leurs systèmes ou prévoient de le faire. On craint toutefois que toute cette mise à niveau des TI ne requière un grand effort constant et onéreux pour tenir le rythme. Cependant, si les systèmes de technologie de l'information ne tiennent pas la route, les assureurs courent le risque de ne pas être en mesure de satisfaire aux attentes en matière de service à la clientèle. Il s'agit d'un risque à la fois opérationnel et stratégique : le risque stratégique est l'importance des investissements dans les systèmes informatiques et le bon fonctionnement de ces systèmes relève du risque opérationnel.

3. **Orientation stratégique et occasions ratées** (8e en 2017)
   Les répondants sont peu confiants que la direction puisse bien faire les choses. Ils craignent que la haute direction entraîne rapidement la société, mais dans la mauvaise direction, en laissant des options valables sur les tablettes. Il s'agit, bien entendu, d'un risque stratégique dont le rang indique que pour les répondants, la haute direction pourrait trop s'attarder aux détails quotidiens et ne pas avoir assez de recul.

4. **Tarification et bénéfices des gammes de produits** (2e en 2017)
   Depuis toujours, le secteur des assurances est un secteur où les ventes se font et les prix sont fixés avant de connaître le coût des biens vendus (coûts des sinistres). La révolution en analyse des données établit un lien solide entre ce risque et les enjeux technologiques. C'est un risque d'assurance et si jamais il ne figure plus dans la liste des 10 plus importants risques d'un assureur, c'est un signe de catastrophe imminente qui ne ment pas.

5. **Fréquence ou gravité incontrôlées des sinistres** (19e en 2017)
   Il n'y a rien comme une année record de sinistres découlant de catastrophes naturelles pour que ce risque d'assurance fasse un bond de géant. Même si les prix et la souscription sont parfaits, la malchance peut entraîner un nombre plus élevé de réclamations ou des réclamations plus élevées que prévu.

6. **Technologie perturbatrice** (14e en 2017)
   Personne ne sait la forme que cela prendra, mais bien des répondants sont persuadés que quelqu'un, Alphabet ou Amazon peut-être, met tranquillement au point une application pour tuer les sociétés d'assurances. Ce risque stratégique est une crainte étroitement liée au risque suivant.

7. **Incapacité de combler les besoins de la clientèle en se servant des approches conventionnelles** (nouveauté en 2018)
   On peut peut-être parler de l'endos du risque précédent. Pour bien des sociétés, l'âge moyen de leurs assurés et agents/courtiers augmente de près d'un an chaque année. Elles craignent que la génération plus jeune ne voie pas beaucoup d'utilité dans les produits d'assurances qui sont vendus depuis 50 ans ou qu'elle ne soit nullement intéressée par un processus de vente ou de réclamation qui ne peut se régler en quelques clics sur les téléphones intelligents. Un autre risque stratégique qu'on peut relier au vieillissement des équipes de direction des sociétés d'assurances.

8. **Risques émergents** (10e en 2017)
   Ce risque peut se résumer ainsi : « Nous ne savons pas ce que c'est, mais quelque chose de mauvais se prépare. » Il a gravi les échelons à cause d'un sentiment de plus en plus présent de pessimisme mal défini ou le contraire, les risques émergents peuvent avoir grimpé en raison de la confiance accrue dans la capacité de la direction de s'occuper des risques relevés.

9. **Concurrence** (4e en 2017)
   Cette année, il semble que les assureurs craignent plus la prise de contrôle par un concurrent technologique que par celle d'un concurrent traditionnel. Or, le risque qui est au 9e rang dans ce sondage est tout de même en avance de 65 autres risques. La concurrence est toujours un risque important pour les assureurs en raison de la grande sensibilité de la plupart des consommateurs aux prix et du peu d'obstacles à l'entrée de nouvelles institutions. Les assureurs cherchent à se diversifier en élargissant leur empreinte géographique traditionnelle, ce qui intensifie la concurrence traditionnelle. La concurrence est le risque stratégique classique d'un système capitaliste.

10. **Souscription** (5e en 2017)
    Un autre risque classique des sociétés d'assurances qui perd du terrain. Les risques d'assurance comprennent ceux de la tarification, de la souscription, des sinistres et de l'établissement de provisions. Trois de ces risques s'inscrivent toujours dans les 10 principaux. L'établissement de provisions techniques qui se classe au 32e rang n'en fait pas partie. Les répondants estiment donc encore qu'il est de toute première importance d'exécuter les activités d'assurance de base. Le risque lié à l'établissement de provisions peut être considéré faible à cause d'une période relativement longue de libération des provisions techniques. C'est l'un des volets cycliques des activités d'assurance et étonnamment, les assureurs ne semblent pas penser que les récentes baisses dans les libérations des provisions techniques n'annoncent pas que le potentiel futur de renforcement des réserves se rapproche.

SORTANT DES 10 PRINCIPAUX RISQUES

Trois risques ne font plus partie des 10 risques en tête de liste en 2018.

- **Risque législatif et réglementaire** (6e en 2017, 11e en 2018)
  Les récentes mesures fiscales fédérales et l'activité insuffisante de l'ACA (Affordable Care Act) pourraient expliquer la préoccupation moindre manifestée à l'égard de ce risque.

- **Catastrophe naturelle** (9e en 2017 et 17e en 2018)
  Le rang de ce risque en 2018 peut être un exemple de bluff du joueur. Les pertes élevées attribuables aux catastrophes naturelles en 2017 ne réduisent pas la probabilité de pertes importantes en 2018.

- **Risque lié au marché des placements** (7e en 2017, 22e en 2018)
  Ce changement de priorité pour le risque lié aux placements semble cadrer avec la situation sur les marchés où le cours des titres s'enflamme et où la protection contre la volatilité laisse à désirer. Ce n'est pas toujours un bon signe, mais comme l'a dit J.M. Keynes [traduction] « Les marchés peuvent se comporter de façon irrationnelle beaucoup plus longtemps que nous pouvons demeurer solvables. »

QUE FAIRE AVEC CETTE INFORMATION?

Comment cette liste et les changements par rapport à l'an dernier se comparent-ils par rapport à la philosophie de votre société? Réfléchissez-y. Y a-t-il des risques classés supérieurs ici qui ne figurent même pas dans votre registre des risques ou qui sont classés moins graves? Êtes-vous à l'aise avec cela? ▯

David Ingram, FSA, MAAA, CERA, est premier vice-président chez Willis Re. On peut le joindre à *dave. ingram@willistowerswatson.com.*

Sondage 2017 d'EY auprès des chefs de la gestion des risques : de la défensive à l'offensive

par Chad Runchey et David Paul

Selon un sondage effectué par EY auprès des chefs de la gestion des risques en Amérique du Nord, on constate que leurs responsabilités s'éloignent du domaine de la réglementation. Chad Runchey et David Paul nous montrent comment ces derniers s'occupent plutôt du phénomène de perturbation et s'emploient à lutter contre les cybermenaces et à mener le bal de l'innovation.

Depuis plusieurs années, le sondage qu'EY réalise auprès des chefs de la gestion des risques (CGR) du secteur des assurances permet de suivre le développement de la gestion des risques ainsi que l'évolution des priorités du CGR. Le sondage de 2017 est celui qui a la plus grande envergure, puisque les répondants représentent plus d'une quarantaine de sociétés.

Les rapports de sondage précédents décrivaient les progrès réalisés par les entreprises et les CGR en matière de développement et de maturité des capacités de gestion du risque d'entreprise (GRE). Surtout depuis la crise financière de 2007, les sociétés sont aujourd'hui plus nombreuses à mettre en place des programmes de GRE en bonne et due forme, à consolider leur équipe de gestion des risques et, dans bien des cas, à créer un bureau du CGR (ou bien ce bureau a gagné en importance pour occuper une place distincte au sein de l'équipe de direction).

NOUVEAUX THÈMES ÉMERGENTS

Toutefois, en 2017, lorsque nous avons interrogé les participants, nous avons pris connaissance d'autres types de difficultés et de nouveaux facteurs déterminants susceptibles de modifier leur rôle.

Il est toujours vrai que les CGR cherchent à intégrer la GRE aux opérations et à mettre en place des processus efficients, exacts, fondés sur des données fiables et qu'ils veulent éviter le travail en double ou devoir refaire le travail. Mais une chose est claire : les choses sont en train de changer.

Selon les entrevues réalisées dans le cadre du sondage de 2017, il ne fait aucun doute que les CGR consacrent nettement moins de temps qu'avant aux questions réglementaires. Par exemple, les CGR nous ont dit que la mise en œuvre du dispositif ORSA de la National Association of Insurance Commissioners, prévue pour 2017, était maintenant chose faite pour les assureurs soumis à la réglementation des départements d'assurances des États. Certains CGR considèrent leur cadre de GRE comme étant évolué ou mature.

Compte tenu du nouveau climat, le rapport de 2017 est axé sur le recentrage du rôle des CGR et des fonctions de gestion des risques. Le rapport regroupe les observations suivant quatre évolutions majeures, que certains CGR considèrent comme étant les prochaines étapes essentielles. Dans certains cas, ces évolutions sont déjà en cours, tandis que dans d'autres entreprises, on a du mal à se mettre en branle.

1. Évoluer de la stabilité relative à l'ère de la perturbation
2. Évoluer des menaces claires et bien comprises à des risques émergents et inconnus
3. Évoluer d'une fonction de contrôle à une qui fait équipe avec les fonctions d'affaires
4. Évoluer des risques d'action aux risques d'inaction dans la promotion de l'innovation

En outre, le rapport de 2017 présente une analyse approfondie des CGR et de la cybersécurité, qui a été un sujet important de nos discussions en 2017 et qui figurait en tête des plus grands risques selon de nombreux CGR.

SAVOIR S'ADAPTER EN CETTE ÈRE DE PERTURBATION

Nous avons aussi abordé le thème de la perturbation lors de nos entretiens avec les CGR, lesquels considèrent que la perturbation découle à la fois des changements rapides sur leur marché et du monde qui les entoure. Ils craignent que leur activité soit celle qui « subit la perturbation » si leur société ne parvient pas à s'adapter assez rapidement. Les questions qu'il

faut se poser, c'est : « Comment une société peut-elle être l'« élément perturbateur »? » et « Quel est le rôle du CGR dans la promotion de ce type de perturbation afin de protéger l'activité et d'assurer sa croissance? »

En matière de perturbation, les CGR s'attachent aussi à :

- Savoir si l'envergure des simulations de crise et des analyses de scénarios est assez grande pour anticiper les événements
- Demander si les modèles stochastiques tiennent compte de la véritable étendue du risque, surtout en ce qui concerne les extrémités de l'aile des distributions et les corrélations entre les types de risques
- Vérifier si la société a des plans d'intervention suffisamment détaillés et des moyens suffisamment robustes de scruter l'horizon
- Entreprendre l'évaluation de voies révolutionnaires, pas seulement le développement évolutionnaire (p. ex., lancer des scénarios qui prévoient l'abandon de certains marchés et la pénétration de nouveaux marchés). Si un marché est fermé, comment le CGR s'assure-t-il que la société cherchera de nouveaux marchés et trouvera d'autres sources de croissance?

ÉVOLUER DES MENACES CLAIRES ET BIEN COMPRISES À DES RISQUES EMERGENTS ET INCONNUS

Nous avons demandé aux CGR comment leur société s'y prenait pour être « bien positionnée face aux nouvelles tendances ». Ils ont été nombreux à souligner l'importance et la dépendance à l'égard de leur processus de gestion des risques émergents. Le rapport rend compte de ce que nous avons entendu – la façon dont ce processus fonctionne, les parties concernées, le rôle des équipes de gestion des risques et du CGR, et les utilisations faites des résultats du processus. Il montre également la grande diversité des risques émergents sur l'écran radar des CGR en 2017.

La plupart des CGR considèrent le processus de gestion des risques émergents comme étant absolument nécessaire, quoique certains admettent l'existence de lacunes, surtout lorsque le processus est entièrement entre les mains des gestionnaires du premier niveau de la ligne d'affaires. Certains CGR à qui nous avons parlé – surtout ceux qui exercent une grande influence dans leur société – ont décidé de relever le défi eux-mêmes avec leur équipe pour vérifier si la scrutation de l'horizon s'effectue avec rigueur et imagination.

LES CGR ET LA CYBERSÉCURITÉ

Au vu des récentes manchettes et de la gravité des cybermenaces, il ne faut pas s'étonner que les CGR du secteur des assurances les considèrent parmi les premières préoccupations. Ce qui surprend, toutefois, c'est le nombre de répondants du sondage qui ont déclaré que leurs efforts en matière de cybersécurité étaient en perpétuel changement.

Nombreuses sont les sociétés qui n'ont pas encore adopté en bonne et due forme l'approche des « trois lignes de défense » en matière de cybersécurité. Résultat? Nous constatons une grande diversité dans le degré de participation et les responsabilités des CGR et dans les méthodes employées pour mesurer le cyberrisque, de même que dans les relations avec le directeur des systèmes d'information et le directeur de la sécurité de l'information.

Certains des CGR interrogés se sont démarqués du fait qu'ils jouaient un rôle dans la cybersécurité, mais ils étaient en minorité. Davantage de CGR ont dit jouer un rôle passif, bien que quelques-uns aient été chefs temporaires de l'équipe d'intervention, prêts à dépanner dans les situations urgentes et à la tête de la gestion du changement et des efforts de correction, suivant les besoins.

En ce qui a trait à l'activité de mesure, les sociétés comptabilisent au moins les violations, et certaines d'entre elles ont commencé à évaluer l'étendue des dommages financiers, bien qu'elles soient conscientes que l'impact opérationnel et les dommages à la réputation peuvent être plus graves que les pertes financières. Si quelques sociétés notent le cyberrisque ou ont recours à des tiers pour qu'ils l'évaluent, l'activité de mesure demeure, dans l'ensemble, rudimentaire, au vu des résultats de notre sondage.

L'augmentation de l'activité de réglementation influence la façon dont certaines sociétés réagissent face à la cybersécurité. Par exemple, ils peuvent concevoir des structures de gouvernance pour s'aligner sur la réglementation future qu'édicteront les États. Les CGR sont très conscients du processus entrepris par la NAIC pour préparer la loi type sur la cybersécurité, même si ce processus n'est pas achevé et qu'il devra être adopté et promulgué par les législatures des États américains. Toutefois, les dommages potentiels – et même la menace existentielle – d'un cyberincident sont un élément bien plus déterminant que la conformité à la réglementation.

Le bilan de la cybersécurité

La gravité croissante des cyberrisques a été au cœur des discussions sur la gestion des risques au cours des cinq dernières années. Certains des CGR participants ont mentionné que leur société en était encore à réorganiser et mettre à niveau leur plan d'intervention en cas d'urgence. Certains assureurs ont revu les attributions et ont décidé de confier les principales responsabilités en matière de cyberrisque au CGR et à son équipe.

SUITE À LA PAGE 14

Un CGR a fait remarquer que les unités commerciales pouvaient être en mesure de détecter les risques locaux et réagir au fur et à mesure des changements externes, mais qu'elles ne seraient peut-être pas capables de détecter les « macrochangements » soudains qui ont une incidence sur l'ensemble de la société, ni d'y faire face.

En fait, certains CGR estiment qu'ils doivent être proactifs et s'assurer que la société innove et évalue les changements potentiels dans la bonne direction. Ce groupe voit cette activité facilitante non pas comme une responsabilité « ajoutée » ou « facultative », mais plutôt comme étant une de leurs fonctions principales.

> . . . les risques les plus graves pour une société découlent de l'inaction, de l'inflexibilité, de l'absence d'innovation et de la lenteur de la mise en marché.

ÉVOLUER D'UNE FONCTION DE CONTRÔLE À UNE QUI FAIT ÉQUIPE AVEC LES FONCTIONS D'AFFAIRES

- Des CGR qui occupent des postes de haute direction (et, dans certains cas, qui dirigent la fonction stratégique)
- Une fonction GRE qui a pour philosophie d'encourager l'innovation et la transparence dans les échanges entre la fonction de gestion des risques et les fonctions en première ligne, plutôt que de chercher à les contraindre
- Un CGR qui insiste sur la communication entre les secteurs d'activité, de manière transversale dans le cas des cadres supérieurs et en amont pour ce qui est du conseil d'administration

Plusieurs CGR se considèrent comme étant les mieux placés pour définir la stratégie de la société. Ils sont indépendants et, du fait de leur position en deuxième ligne, ils peuvent adopter une vision large et holistique de la société.

ÉVOLUER DES RISQUES D'ACTION AU RISQUE D'INACTION

Tandis que les CGR traditionnels analysent et contrôlent les mesures actuelles ou proposées relativement aux expositions actuelles de leur société, d'autres CGR craignent que les risques qu'entraîne l'inaction ne soient graves. De fait, les risques les plus graves pour une société découlent de l'inaction, de l'inflexibilité, de l'absence d'innovation et de la lenteur de la mise en marché. Il est particulièrement difficile pour les CGR de jouer simultanément plusieurs rôles :

- Prévenir la prise de risque excessive
- Encourager l'innovation
- Vérifier si la répartition des capitaux propres de la société s'effectue sagement entre les activités actuelles plus ou moins capitalistiques et entre les nouveaux investissements plus ou moins spéculatifs

Encourager l'« action » en ces temps nouveaux pose éventuellement plusieurs défis, notamment :

- Le rôle des CGR et de leur équipe dans le développement des produits
- La méthode de lancement de produits avec peu de données
- Les possibilités et les difficultés que fait naître l'existence de capitaux propres excédentaires

Tandis que la question de la perturbation gagne en importance dans un grand nombre de secteurs de l'entreprise, le CGR cherche à vérifier si la société a suffisamment de moyens de défense et de protection contre les menaces extérieures de perturbation. Mais les résultats du sondage de 2017 montrent clairement que certains CGR vont encore plus loin – ils se lancent à l'offensive et poussent leur société à innover et à être l'agent perturbateur pour leur propre avantage.

Chad Runchey et David Paul, qui ont préparé les entrevues du sondage 2017 d'EY, tiennent à exprimer leur gratitude et leurs remerciements à toutes les sociétés et les CGR qui ont participé et fait connaître leurs points de vue exprimés dans le rapport. Cet article a déjà été publié dans Insurance – ERM *et est reproduit avec autorisation.*

Chad Runchey, FSA, MAAA, est associé chez Ernst & Young. On peut le joindre à *chad.runchey@ey.com*.

David Paul, FCAS, MAAA, est directeur général chez Ernst & Young. On peut le joindre à *david.paul1@ey.com*.

ERM Enterprise Risk Management Symposium

April 19–20, 2018
Miami, FL

Insight Into The Future

The ERM Symposium provides a dynamic environment for thought leadership, best practices and networking opportunities. Join us for this unparalleled opportunity to learn from leading enterprise risk management professionals.

CAS · Canadian Institute of Actuaries / Institut canadien des actuaires · SOCIETY OF ACTUARIES

ERMSymposium.org

Niveau et allocation optimaux des dépenses en cybersécurité

par Shaun S. Wang

Note de l'éditeur : C'est sur le thème « Actuarial Research at the Crossroads: Transcending Disciplines » qu'a eu lieu la 52e Actuarial Research Conference à Atlanta, en Géorgie, en juillet 2017. Professeurs, professionnels et chercheurs s'y étaient réunis pour parler des derniers développements et échanger des idées. Dans ce numéro de Gestion du risque, *nous avons le plaisir d'accueillir M. Wang (Ph.D.), qui fait ici un résumé de l'exposé qu'il a donné lors de la conférence et qui portait sur la modélisation du niveau et de l'allocation optimaux des dépenses en cybersécurité.*

INTRODUCTION

Le nombre croissant de violations de sécurité a fait grimper les dépenses en cybersécurité des entreprises. On estime (p. ex., Gartner, 2017)[1] qu'à l'échelle mondiale, le secteur privé investira 93 milliards de dollars en 2018 pour renforcer la protection de ses systèmes internes contre les cybermenaces. Les entreprises veulent donc savoir quels sont le niveau et l'allocation optimaux des investissements en sécurité. Ces questions ont fait l'objet de nombreuses études par les chercheurs (p. ex., Gordon et Loeb, 2002)[2]; (Tanaka et coll., 2005)[3]. Lors de la 52e conférence, j'ai présenté un modèle mathématique qui exprime la probabilité de violation en fonction de la dépense engagée pour la protection du système de technologies de l'information et de la communication (TIC) d'une entreprise et qui calcule le niveau optimal d'investissement en sécurité en pourcentage de la valeur à risque. Le présent article comporte également une synthèse de la première partie du modèle mathématique de Wang (2017)[4].

En règle générale, le système TIC d'une entreprise a une surface d'attaque exposée à divers types de cyberattaques. Cette surface peut comprendre des ports ouverts sur le Web et des appareils mobiles, des services informatiques à l'intérieur du pare-feu d'entreprise, et des employés ayant accès à des renseignements sensibles pouvant faire l'objet d'ingénierie sociale (art d'exploiter les comportements humains afin d'obtenir des informations et des données confidentielles ou des codes d'accès[5], voir la figure 1). Le système TIC d'une entreprise est vulnérable à divers types de cyberattaques, dont les logiciels malveillants, les attaques par déni de service distribué (attaques très évoluées visant à faire planter ou à rendre muette une machine en la submergeant de trafic inutile, aussi appelées DDoS[6]), les intrusions aux points de vente, l'hameçonnage et l'ingénierie sociale, les attaques persistantes avancées, les attaques de l'intérieur et la mauvaise utilisation des privilèges d'accès.

Normalement, les entreprises ont déjà investi dans certaines mesures de cybersécurité pour protéger leur système TIC. Un investissement en sécurité de valeur positive, $B>0$, est choisi comme *dépense de référence* appropriée compte tenu de la superficie de la surface d'attaque. Tout montant de dépense en sécurité Z peut être décrit par le *ratio de dépense*, $z=Z/B$. Pour la dépense en sécurité $Z=zB$, nous désignons la probabilité de violation du système TIC par $v(z)$. Lorsque la dépense de référence est B, nous avons z=1 et la probabilité que le système TIC de l'entreprise soit l'objet d'une violation est donnée par $v(1)$.

Nous pouvons spécifier les conditions de régularité suivantes pour la fonction de probabilité de violation v(z) :

1. $v(0)=1$. Lorsque la dépense en sécurité est nulle, la probabilité d'une violation est de 1.

2. $v'(z) < 0$, pour $z>0$. À mesure qu'augmente l'investissement en sécurité z, la probabilité de violation $v(z)$ diminue. En d'autres termes, chaque dollar supplémentaire dépensé donne proportionnellement moins d'avantages du point de vue de la réduction de vulnérabilité. Idéalement, une entreprise devrait investir dans les outils dont le rendement est le plus élevé. Ce rendement est le taux auquel la probabilité de violation résiduelle diminue avec l'augmentation marginale de l'investissement z. Ce taux n'augmente pas si l'investissement actuel est optimal, car la meilleure protection est acquise en premier. Cette hypothèse intuitive est étayée empiriquement par des données d'entreprise transversales (p. ex., Tanaka et coll., 2005).

Wang (2017) a examiné plusieurs classes de fonctions de probabilité de violation de sécurité :

a. La classe des fonctions exponentielles :

$$v_{EP}(z) = v(1)^{z^{\alpha}}, \text{ où } \alpha > 0 \qquad \text{(éq-3)}$$

b. La classe de modèles à risques proportionnels :

$$v_{PH}(z) = 1 - [1 - v(1)]^{z^{\alpha}}, \text{ où } \alpha > 0 \qquad \text{(éq-4)}$$

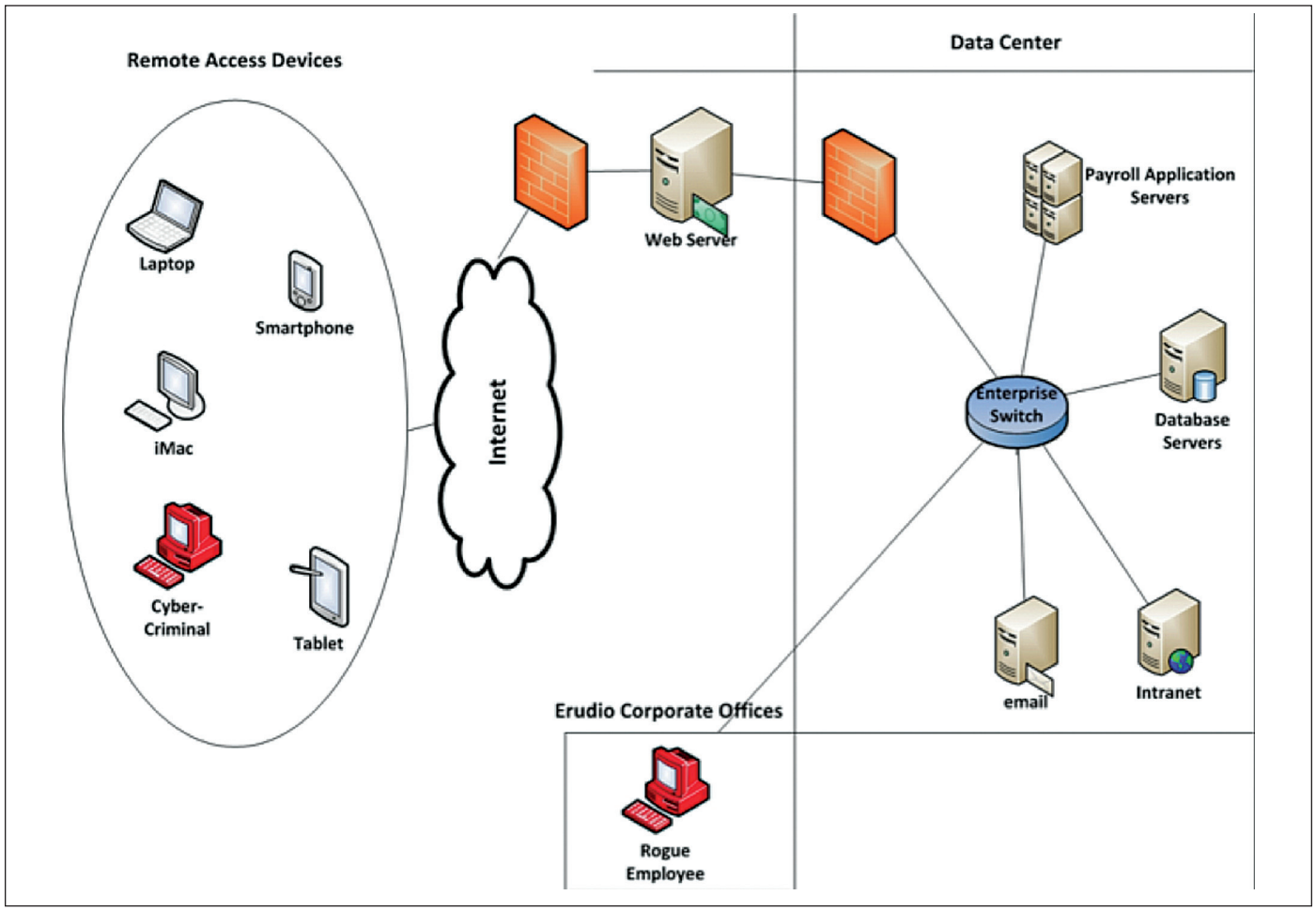
c. La classe des transformées de Wang :

$$v_{WT}(z) = \Phi\left[\Phi^{-1}(v(1)) - \alpha \cdot \ln(z)\right] \qquad \text{(éq-5)}$$

où $\alpha > 0$ et Φ est la fonction de répartition de la loi normale centrée réduite (voir Wang, 2000)[7].

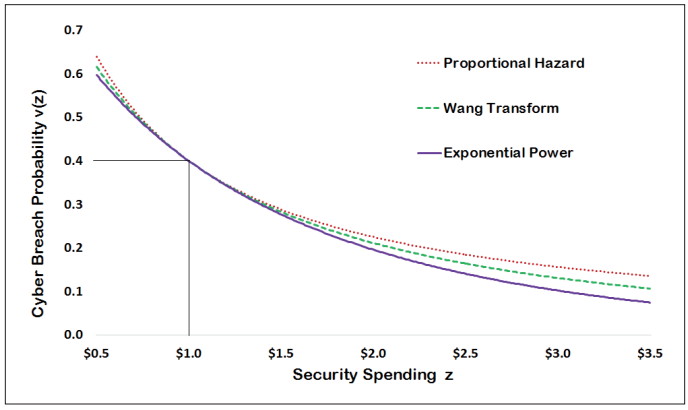
La fonction de probabilité de violation $v(z)$ est dite **invariante** si elle conserve la même forme après un changement de la valeur de référence : $\tilde{B} = \tau \cdot B$, pour tout $\tau > 0$. Il est possible de démontrer que les classes de fonctions exponentielles, de modèles à risques proportionnels et de transformées de Wang sont toutes invariantes, car leur forme fonctionnelle et le paramètre α restent les mêmes quel que soit le choix de la valeur de référence B.

Figure 1
Illustration d'une surface d'attaque



Source : *http://www.infosecinstitute.com*

Figure 2
Comparaison des fonctions de probabilité de violation



NIVEAU OPTIMAL DES DÉPENSES EN SÉCURITÉ

Considérons le système TIC d'une entreprise. Soit R la valeur à risque potentielle ou les dépenses et les pertes monétaires en raison d'une violation de données. En correspondance avec la dépense en sécurité $Z = z \cdot B$, l'entreprise a une probabilité de violation de sécurité, $v(z)$, et une espérance de perte annuelle de of $v(z) \cdot R$. Le total des coûts de la cybercriminalité pour l'entreprise est égal à la somme de la dépense en sécurité et de l'espérance de perte annuelle :

$$\text{Coût}(z) = z \cdot B + v(z) \cdot R$$

Le ratio de dépense optimal z^* est défini de façon à minimiser le coût de la cybercriminalité selon une dépense en sécurité $Z^* = z^* \cdot B$. Le niveau optimal de la dépense en sécurité $Z^* = z^* \cdot B$ vérifie l'équation :

$$-v'(z^*) = B/R$$

Dans le cas particulier de la classe des fonctions exponentielles avec $\alpha = 1$, le ratio de dépense optimal s'exprime par une formule analytique :

$$z^* = \frac{\ln(R) - \ln(B) + \ln(-\ln v(1))}{-\ln v(1)}$$

N.B. La dérivée $-v'(1)$ indique l'efficacité de la dépense marginale dans la réduction de la vulnérabilité, selon une dépense de référence B.

Il est possible de démontrer que l'investissement optimal en sécurité $Z^* = z^* \cdot B$ est borné supérieurement comme suit :

1. Classe des fonctions exponentielles : $Z^* \le \frac{\alpha}{e} \cdot R$
2. Classe des modèles à risques proportionnels : $Z^* \le \frac{\alpha}{e} \cdot R$
3. Classe des transformées de Wang : $Z^* \le \frac{\alpha}{\sqrt{2\pi}} \cdot R$

ALLOCATION OPTIMALE DE L'INVESTISSEMENT EN SÉCURITÉ POUR COLMATER PLUSIEURS POINTS DE VULNÉRABILITÉ

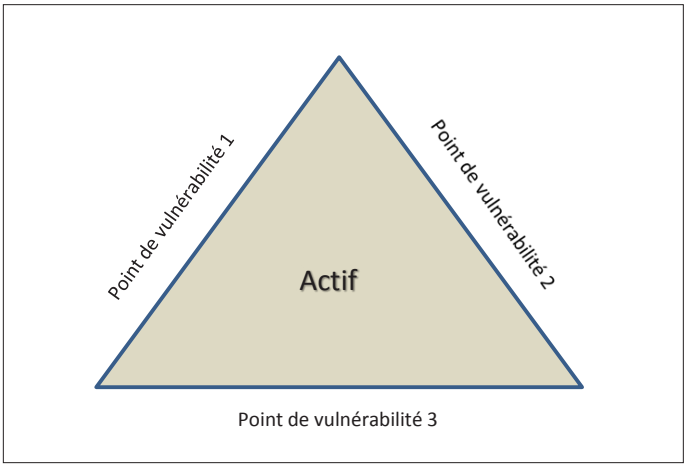
Nous considérons qu'un système TIC comporte plusieurs points de vulnérabilité et qu'une violation de sécurité se produit lorsqu'un pirate exploite avec succès un point de vulnérabilité (voir la figure 3). Nous fixons à trois le nombre de ces points, bien que l'analyse soit valide pour tout nombre de points de vulnérabilité. Pour chaque point j de vulnérabilité ($j = 1, 2, 3$), la dépense de référence est B_j, avec une probabilité de violation correspondante, $v_j(1)$. On suppose que la dépense en sécurité $\boldsymbol{Z}$ de l'entreprise est répartie entre chaque point de vulnérabilité :

$$\boldsymbol{Z}^* = z_1 \cdot B_1 + z_2 \cdot B_2 + z_3 \cdot B_3$$

Nous avons un modèle de risque concurrent :

$$v(\boldsymbol{z}) = 1 - (1 - v_1(z_1)) \cdot (1 - v_2(z_2)) \cdot (1 - v_3(z_3))$$

Figure 3
Routes parallèles ou plusieurs points de vulnérabilité



Notre modèle et notre analyse soulignent l'importance que les dépenses en sécurité couvrent la totalité des points de vulnérabilité; le fait de négliger un seul point peut rendre l'investissement inefficace et inutile. De plus, on obtient une plus grande valeur économique en accordant un traitement différencié aux actifs de données de grande valeur. Les entreprises doivent protéger en premier lieu leurs actifs les plus précieux, par exemple, en réduisant les points de connexion inutiles ou en exigeant une authentification multifactorielle.

Le modèle de référence dans le présent document a des implications pratiques. Il est conseillé aux entreprises de rattacher leur dépense en sécurité à un point de référence et de contrôler empiriquement l'efficacité des dépenses en sécurité pour ce qui est de réduire la vulnérabilité. Pour les entreprises, l'évaluation de la vulnérabilité du système TIC nécessite des connaissances et du savoir-faire; et pour savoir lesquels des actifs de données sont les plus importants, il faut connaître le modèle d'affaires de l'entreprise. Il doit donc y avoir coordination entre les spécialistes de l'informatique et les gestionnaires du risque de l'entreprise. ▯

Shaun S. Wang, FCAS, CERA, Ph.D., est professeur et directeur de l'Insurance Risk and Finance Research Centre, de l'École d'administration de l'Université de technologie de Nanyang, à Singapour. On peut le joindre *shaun.wang@ntu.edu.sg*

NOTES

[1] Gartner. « Gartner Predicts Information Security Spending To Reach $93 Billion In 2018 », Forbes, 2017. https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/#22a572db3e7f

[2] Gordon, Lawrence A. et Martin P. Loeb. « The Economics of Cybersecurity Investment », revue de l'ACM sur la sécurité des systèmes d'information, 2002, vol. 5, p. 438-457.

[3] Tanaka, H., Matsuura, K., Sudoh, O. « Vulnerability and information security investment: An empirical analysis of e-local government in Japan », *Journal of Accounting and Public Policy*, 2005, vol. 24, p. 37-59.

[4] Wang, Shaun. *Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain*, 3 novembre 2017. Disponible auprès de SSRN : https://ssrn.com/abstract=3064533

[5] N.d.t. : Gouvernement du Canada. *Termium Plus. La banque de données terminologiques et linguistiques du gouvernement du Canada. 15 juin 2016.* Récupéré le 7 avril 2018 de http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&srchtxt=SOCIAL+ENGINEering&index=alt&codom2nd_wet=1

[6] N.d.t. : Gouvernement du Canada. *Termium Plus. La banque de données terminologiques et linguistiques du gouvernement du Canada. 8 février 2008.* Récupéré le 7 avril 2018 de http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&srchtxt=DDOS&index=alt&codom2nd_wet=1

[7] Wang, Shaun. « A Class of Distortion Operators for Pricing Financial and Insurance Risks », *Journal of Risk and Insurance*, mars 2000, vol. 67, p. 15-36.

La GRE en cinq mots

Partie 2 : Harmonisation, capacité d'adaptation et résilience

par Dave Ingram

Note de l'éditeur : « La GRE en cinq mots » est une série de deux articles. La première partie, intitulée Résilience, transparence et discipline, *a été publiée dans le numéro de décembre de* Gestion du risque.

En première partie, nous avions expliqué comment la transparence et la discipline renforçaient la gestion du risque d'entreprise (GRE). Mais la solidité du programme de GRE n'est pas toujours une bonne chose pour une entreprise. Nous avons eu vent de confrontations entre des responsables de programme de GRE et des gestionnaires de l'entreprise qui ont été remportées par les premiers. Ces choses ne doivent se produire que lorsque le programme de GRE est bien aligné sur les objectifs et les stratégies de l'entreprise. Autrement, les « victoires » remportées par les partisans de la GRE pourraient se traduire par des « défaites » pour l'entreprise.

De plus, la solidité apparente d'un programme de GRE peut aussi cacher sa fragilité, c'est-à-dire qu'il pourrait échouer en situation de crise imprévue. La GRE doit donc aussi être adaptable si nous voulons en réduire la fragilité. Dans cette deuxième partie, nous traitons de deux autres des cinq mots associés à la GRE, à savoir l'harmonisation et la capacité d'adaptation, et de la façon dont la combinaison des quatre conduit à la résilience.

HARMONISATION

La question du risque a traditionnellement été peu évoquée dans les discussions stratégiques auxquelles les entreprises prennent part.

Souvent, les planificateurs écartent d'entrée de jeu la question du risque lorsqu'ils traitent des forces, des faiblesses, des opportunités et des menaces. Puis, aussi vite que possible, ils passent à l'étude des opportunités. C'est d'ailleurs pour cette raison qu'ils sont là : étudier les opportunités.

La gestion du risque fait partie intégrante des pratiques commerciales depuis des temps immémoriaux. La GRE est une nouvelle approche de la gestion du risque, qui, poussée à l'extrême, peut accroître sensiblement le coût des activités et détourner l'attention des dirigeants de la conduite de leur entreprise. Mais, si la GRE est harmonisée avec le plan d'affaires, elle procurera des avantages qui seront nettement supérieurs à ce coût.

L'harmonisation de la GRE et de la stratégie d'affaires s'opère à deux niveaux : tout d'abord, dans le cadre de la stratégie susmentionnée et de l'exercice de planification, et deuxièmement, pendant les discussions d'ordre opérationnel qui découlent de la stratégie et du plan.

Appétence au risque et stratégie

L'idée selon laquelle l'harmonisation de la gestion du risque et de la stratégie est très importante représente peut-être une avancée pour certaines entreprises, mais, pour les assureurs, le risque représente leur matière première. Il semble donc très naturel que la gestion du risque s'inscrive dans les discussions stratégiques de la société d'assurances.

La pièce maîtresse de la discussion stratégique sur le risque et la gestion du risque est la déclaration de l'appétence au risque. Dans le document intitulé *NAIC Own Risk and Solvency Assessment (ORSA) Guidance Manual*, la notion d'appétence au risque est définie comme suit :

> [Traduction]
>
> Décrire les principes généraux que l'entreprise doit suivre dans la prise de risque, compte tenu de sa stratégie commerciale, de sa santé financière et de ses ressources en capital. Souvent exprimée en termes qualitatifs, l'appétence au risque définit comment l'entreprise prend des décisions stratégiques et communique sa stratégie de prise de risque aux principales parties prenantes. Elle a pour but d'améliorer la capacité de la direction à prendre de bonnes décisions en toute connaissance de cause, tout en prenant des risques dans des limites acceptables.

Outils de GRE

Outre l'appétence au risque, plusieurs outils de GRE peuvent faciliter les discussions stratégiques au sujet du risque.

Profil de risque

Une partie de la documentation relatant l'impact du plan sur l'entreprise devrait être constituée d'un profil de risque antérieur et postérieur au plan. Cela montrerait comment le plan a augmenté ou diversifié les plus importants risques de l'entreprise. Le risque ne peut être entièrement décrit par un seul chiffre; par conséquent, on ne peut représenter le profil de risque de l'entreprise avec un seul graphique circulaire.

Le profil de risque devrait être présenté de façon à exposer clairement les principaux aspects du risque qui sont les conséquences du plan – voulues ou non. Par exemple, il pourrait contenir :

- le profil de risque géographique;
- le profil de risque produit par produit;
- le profil de risque par réseau de distribution;
- le profil de risque par type de risque.

En examinant ces différents profils de risque, les planificateurs jetteront naturellement un coup d'œil aux forces et aux faiblesses des aspects risqués du plan. Ils verront les facettes du risque qui augmentent rapidement et qui nécessitent donc une attention accrue du point de vue du contrôle.

Et même s'il n'y a aucune de ces réactions, la lecture de cette information sur le risque conduira à une meilleure compréhension du risque et à une planification qui tient mieux compte du risque.

Mise en visibilité des gains et pertes par les gestionnaires du risque

La planification commence habituellement par l'examen de l'expérience récente. Les gestionnaires du risque préparent l'analyse de l'exercice précédent en décrivant les résultats pour chaque risque en fonction de la probabilité de dépassement obtenue avec les modèles de risque. Cet exercice peut mener à une discussion sur l'étalonnage du modèle et peut-être à une plus grande confiance dans le modèle de risque ou à un étalonnage différent qui est plus crédible.

Examen des systèmes de contrôle des risques

Chaque risque est géré à l'intérieur d'un système de contrôle. L'examen de l'expérience récente devrait permettre de savoir si les systèmes de contrôle fonctionnent comme prévu.

Tarification ajustée en fonction des risques

L'examen des gains et pertes peut aussi s'effectuer par l'analyse des marges de risque par rapport aux risques pour chaque activité ou produit important ou chaque type de risque. La comparaison avec un indice neutre pourrait aussi être effectuée. Avec cet examen, on devrait pouvoir savoir si les rendements de l'entreprise étaient attribuables à la prise plus importante de risque ou à une meilleure sélection et gestion des risques.

Les comités de direction pourraient être beaucoup plus intéressés par un ou plusieurs de ces outils. Le gestionnaire du risque doit rechercher l'approche à adopter pour discuter des risques qui répond aux intérêts de la direction, afin que la question du risque fasse partie intégrante de la planification et de la stratégie. Faute de quoi, toute discussion sur les risques ayant lieu pour répondre aux pressions des organismes de réglementation ou des agences de notation sera faite pour la forme.

Des études récentes[1] ont révélé que les assureurs qui mettaient en relation GRE et stratégie étaient beaucoup plus satisfaits que les autres de leur programme de GRE. Plus de la moitié des assureurs qui ont répondu à un récent sondage sur l'appétence au risque ont dit que l'établissement de liens entre la GRE et la stratégie était un objectif explicite de leur déclaration d'appétence au risque.

Tolérance au risque et planification de l'entreprise

La tolérance au risque est l'expression consacrée pour désigner la planification globale de la gestion du risque. Une entreprise peut bien ne pas avoir de planification globale de la gestion du risque, mais si elle en a une, cette planification définit sa tolérance au risque. Il est donc probable que beaucoup d'entreprises aient une tolérance au risque et qu'elles ne le savent pas tout simplement.

La plupart des entreprises qui reconnaissent avoir défini une tolérance au risque[2] l'ont fait pour satisfaire aux exigences des agences de notation et des organismes de réglementation, et cette déclaration de tolérance au risque comprend parfois des indications sur le montant de l'excédent exposé au risque suivant des circonstances prédéfinies. Par conséquent, si les assureurs qui n'emploient pas l'expression « tolérance au risque » ont effectivement défini une cible pour leur ratio de capital pondéré en fonction des risques ou pour leur score BCAR (Best's Capital Adequacy Ratio) d'A.M. Best, ils ont donc une planification globale de la gestion du risque, ce qui signifie qu'ils ont effectivement une tolérance au risque.

Impact de la stratégie et de la planification de la gestion des risques

La GRE devrait laisser la voie libre à l'agrégation des risques que l'assureur planifie exploiter.

Le programme de GRE devra aussi aligner la gestion des risques individuels sur la stratégie et la planification. Au plus haut niveau, il existe quatre stratégies possibles pour contrôler les risques individuels :

- Exploiter
- Gérer
- Minimiser
- Éviter

La stratégie de l'entreprise identifie les risques qui seront exploités et gérés. Le programme de GRE doit être actif afin que la gestion des risques ne serve pas de fonction de prévention de ces risques.

Nous l'avons dit, la GRE doit laisser la voie libre à l'agrégation des risques que l'assureur planifie exploiter et elle doit prêter une attention particulière aux risques qui doivent être gérés. Toutefois, cette attention doit être du type « ni trop chaud » « ni trop froid » qui permet la réussite de l'entreprise.

Le programme de GRE doit aussi pouvoir aider à définir les processus et les procédures dont on a besoin pour minimiser et éviter les risques qui ne font pas directement partie de la formule gagnante de l'assureur. En fin de compte, cela signifie que les plans d'acceptation et d'atténuation des risques et les limites correspondantes doivent être soigneusement examinés par la GRE, et ce pour chacun des risques importants de l'entreprise.

Sans lien avec la stratégie

Si la fonction de gestion du risque s'est bien développée en une fonction solide, efficace, disciplinée, deux résultats sont possibles : soit elle peut aider à atteindre les objectifs stratégiques commerciaux, soit être une force solide qui, à l'occasion, empêchera la réalisation des objectifs stratégiques perçus comme étant trop risqués (voir la figure 1).

Un programme de GRE géré avec transparence et discipline constitue un outil puissant à la disposition de la direction. Pareil programme, s'il est en voie d'harmonisation, se maintiendra assurément dans cette voie et pourra toujours appuyer la stratégie globale et apportera à tous des preuves de cette harmonisation.

ADAPTABILITÉ

Encourager délibérément la capacité d'adaptation : voilà comment la fonction de la gestion du risque réussit à réduire les pertes et les mauvaises surprises. Voici quatre moyens que les programmes de GRE emploient pour y arriver.

Figure 1
Efficacité de la fonction de gestion du risque

Efficacité de la fonction de gestion du risque	Harmonisation entre gestion du risque et stratégie : Moins	Harmonisation entre gestion du risque et stratégie : Plus
Plus	La fonction de gestion du risque vise à empêcher la prise de mesures à l'appui des objectifs stratégiques, **ce qui entraîne des confrontations majeures au sein de la direction.**	**La fonction de gestion du risque est vue comme un partenaire stratégique;** elle peut réussir à empêcher des actions qui pourraient compromettre la réalisation des objectifs stratégiques.
Moins	La fonction de gestion du risque s'oppose en vain aux mesures prises à l'appui des objectifs stratégiques; **par conséquent, elle n'est finalement pas écoutée.**	La fonction de gestion du risque essaiera d'empêcher la prise d'actions qui, selon elle, pourraient nuire à la réalisation des objectifs stratégiques; **elle sera écartée des discussions stratégiques.**

Révision des risques identifiés

Tous les programmes de GRE commencent par l'identification des risques. L'entreprise identifie ses principaux risques – ceux qui constituent une menace à son existence – pendant le processus initial d'identification des risques.

Mais ce processus d'identification et de classement par ordre de priorité des risques perd de sa pertinence à mesure que le temps passe. Selon les activités qu'elle exerce, l'entreprise devra peut-être revoir ce processus tous les deux ans; certaines entreprises trouvent même plus facile d'engager ce processus tous les ans.

Mais il y a danger à engager trop souvent ce processus. S'il n'y a aucun changement notable d'année en année dans les priorités ou les risques identifiés, ce processus, qui ne fait que réaffirmer les choix précédents, semblera être une formalité excessive et inutile.

L'une des façons de donner vie à ce processus est de prendre connaissance des idées des autres acteurs de l'industrie. (Voir les risques les plus dangereux en 2017[3].) Le résultat auquel il faut s'attendre est un changement dans l'ordre de priorité des risques d'une année à l'autre. Mais il doit s'agir d'un changement de priorités qui a suffisamment de crédibilité pour justifier tout ce travail de réflexion et le déplacement des ressources et de l'attention vers les risques qui ont le plus augmenté. Cela signifie un changement en lequel la haute direction croit vraiment.

Risques émergents

La gestion normale du risque s'occupe des risques « présents » – ceux que nous connaissons généralement du fait surtout que nous avons une certaine expérience ou que nous avons vu d'autres entreprises subir des pertes en raison de ces risques. Mais, nous avons également été prévenus de l'existence de cygnes noirs et d'inconnues inconnues sortant de nulle part qui nous feraient subir de grandes pertes. En GRE, nous appelons ces risques inattendus des risques émergents. La GRE comporte des processus nous permettant d'identifier les risques émergents et de nous préparer en conséquence.

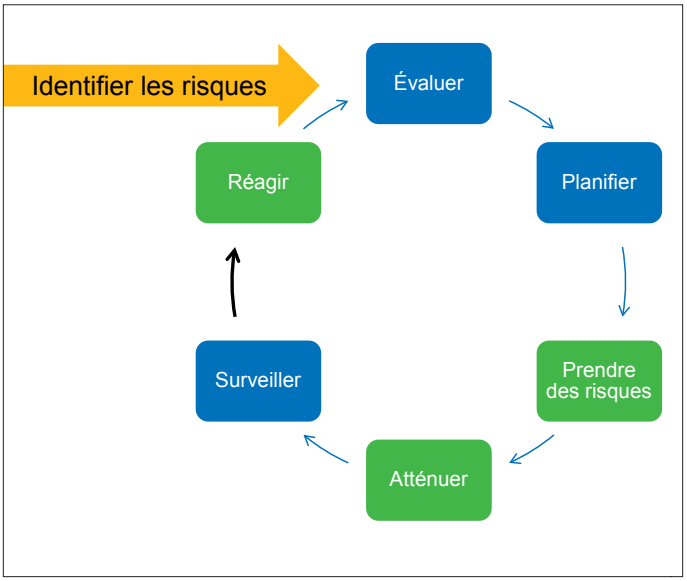
Pendant la mise à jour du registre des risques, les gestionnaires du risque et les dirigeants de l'entreprise doivent déterminer s'il est temps d'inscrire un risque émergent à la liste des risques présents importants. Selon les résultats du sondage sur les risques les plus dangereux en 2017, la cybercriminalité, par exemple, arrive en tête de liste. Il y a plusieurs années, la cybercriminalité aurait été considérée comme un risque émergent.

Cycle de contrôle des risques

La plus grande partie de la GRE s'effectue à l'intérieur d'un cycle de contrôle des risques (voir la figure 2). Ce cycle comporte sept étapes :

- Identifier
- Évaluer
- Planifier
- Prendre des risques
- Atténuer
- Surveiller
- Réagir

Figure 2
Cycle de contrôle des risques



Des sept étapes, la dernière, Réagir, consiste en la possibilité de s'adapter si l'écart par rapport au plan est assez grand. Dans un cycle de contrôle des risques très évolué, l'étape Réagir est planifiée.

Lorsque la situation se produit réellement et qu'il faut réagir, la réponse réellement choisie ne sera pas forcément celle prévue. Toutefois, les entreprises ont constaté qu'une discussion préalable et la planification d'une réponse possible accéléraient la préparation de la réponse réelle lorsque le besoin se faisait sentir.

Une autre caractéristique clé d'un cycle de contrôle des risques est qu'il se répète et qu'à chaque reprise, l'étape Évaluer est effectuée de nouveau. Ce faisant, l'entreprise a l'occasion d'améliorer le processus de gestion des risques. Cela est particulièrement important pour un nouveau système de GRE, dont le développement s'effectue au mieux par un processus détaillé d'essais et d'erreurs.

Processus d'apprentissage des risques

En plus de l'amélioration continue qui accompagne le cycle de contrôle des risques, les entreprises doivent inclure un processus délibéré d'apprentissage des risques dans leur programme de GRE. Par exemple, une entreprise a fait de l'apprentissage des risques un point régulier de l'ordre du jour des réunions du comité de gestion des risques. Les quinze premières minutes de chaque réunion consistent en un exposé d'un des membres du comité choisis à tour de rôle.

La GRE ne produira pas les résultats escomptés à long terme si elle fonctionne comme un système fixe et statique, parce que le risque, en réalité, change constamment et de manière habituellement à rendre inefficaces les processus de GRE existants. Pour ceux qui ont construit le système de GRE, il ne s'agit pas là d'un échec; cela fait simplement partie de la nature du risque.

Amélioration continue de la gestion du risque

Après la fin du projet de développement initial, la GRE doit faire l'objet d'une amélioration continue. De même qu'il y a adaptation constante de l'ordre de priorité des risques d'une entreprise, de même l'efficacité des processus de sélection et d'atténuation des risques évolue constamment. La révision du processus d'identification des risques existants et émergents a pour but d'adapter l'objet de la GRE – à savoir les risques – au contexte présent ou à court terme.

Le cycle de contrôle des risques est conçu comme une boucle de rétroaction qui tient compte de l'efficacité de la gestion des risques de l'année précédente dans la planification de l'année suivante. L'apprentissage des risques est la composante de la GRE qui permet d'intégrer au savoir institutionnel les leçons que l'entreprise a tirées de sa propre expérience et de celles d'autrui. La capacité d'adaptation est encouragée et institutionnalisée au moyen de la GRE.

Si la GRE tire sa force de la transparence et de la discipline et son orientation du processus d'harmonisation, c'est seulement si elle est adaptable qu'elle pourra maintenir son efficacité à long terme.

RÉSILIENCE

Ce qui nous ramène au sujet de la résilience. Et ici, nous ne parlons pas seulement de la résilience dans le contexte de la continuité des activités et de la reprise après sinistre, nous employons le terme résilience dans son sens le plus large. Cette résilience consiste en la capacité d'une entreprise de survivre à tout type d'adversité et de continuer à fonctionner.

Grâce à ce type de résilience, l'assureur est en mesure d'évoluer, de se renouveler et de se réorganiser pour survivre dans un monde et un marché qui eux aussi évoluent, se renouvellent et se réorganisent constamment. C'est à ce moment-là que la définition à double sens du risque redevient unique – la gestion des événements heureux ou malheureux n'est qu'une et seule même chose. En cas de scénario extrêmement défavorable, la vision d'une nouvelle possibilité représente la forme optimale de gestion du risque face à la situation. C'est ce que l'on appelle la capacité d'adaptation.

Et lorsqu'un assureur entrevoit clairement une nouvelle possibilité, si la gestion du risque n'est pas harmonisée avec les efforts déployés pour concrétiser cette possibilité et éviter les échecs, elle sera mise en échec et reléguée à la périphérie. Par contre, lorsque la gestion du risque s'aligne sur la nouvelle stratégie de l'assureur, la discipline et la transparence qui lui donnent toute sa force seront acceptées volontiers.

La fonction de gestion du risque qui ne s'adapte pas ne sera pas alignée et s'opposera aux changements stratégiques qui sont pourtant essentiels à la survie à long terme de l'entreprise. En revanche, la transparence et la discipline constituent les éléments de la force et de la fiabilité de la GRE qui permettront à l'entreprise de maintenir sa stratégie souhaitée dans de nombreuses situations de crise.

La gestion du risque d'entreprise est une question de **transparence,** de **discipline,** d'**harmonisation** et de **capacité d'adaptation**, qui, ensemble, conduisent à la **résilience**. Ces cinq mots sont la clé de la GRE.

David Ingram, FSA, MAAA, CERA, est premier vice-président chez Willis Re. On peut le joindre à *dave.ingram@willistowerswatson.com*.

NOTES

1 *https://www.towerswatson.com/en/Press/2015/04/global-insurers-embrace-risk-management-as-a-strategic-business-partner*

2 *http://blog.willis.com/2015/04/risk-appetite-and-tolerance/*

3 *https://blog.willis.com/2017/01/2017-most-dangerous-risks-for-insurers/*

Publications récentes dans le domaine de la gestion du risque

À titre de rubrique de *Gestion du risque*, nous présentons à nos lecteurs des publications récentes que nous estimons dignes d'intérêt. Veuillez faire parvenir vos suggestions en la matière à *dschraub@soa.org* ou à *cheryl.by.liu@FWD.com*.

Consultation sur la révision des principes de base en assurance (ICP) 8, ICP 15 et ICP 16
AAI
https://www.iaisweb.org/page/consultations/current-consultations/revision-icps-8-15-and-16/

Enhancing the Role of Insurance in Cyber Risk Management
OCDE
http://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf

2017 Insurance CRO Survey (Sondage 2017 d'EY auprès des chefs de la gestion des risques)
Ernst & Young
http://www.ey.com/Publication/vwLUAssets/ey-insurance-cro-survey-2017/$FILE/ey-insurance-cro-survey-2017.pdf

10th Survey of Emerging Risks (10e sondage sur les risques émergents)
Section conjointe sur la gestion du risque (CAS, ICA, SOA)
https://www.soa.org/Files/Research/Projects/10th-survey-emerging-risks.pdf

Big Data & Privacy: Unlocking Value for Consumers
The CRO Forum
https://www.thecroforum.org/2017/12/15/big-data-privacy-unlocking-value-for-consumers/

A Guide to Defining, Embedding and Managing Risk Culture
The CRO Forum
https://www.thecroforum.org/2017/10/06/a-guide-to-defining-embedding-and-managing-risk-culture/

SOCIETY OF ACTUARIES®

475 N. Martingale Road, Suite 600
Schaumburg, Illinois 60173
p: 847.706.3500 f: 847.706.3599
w: www.soa.org

NONPROFIT
ORGANIZATION
U.S. POSTAGE
PAID
SAINT JOSEPH, MI
PERMIT NO. 263