

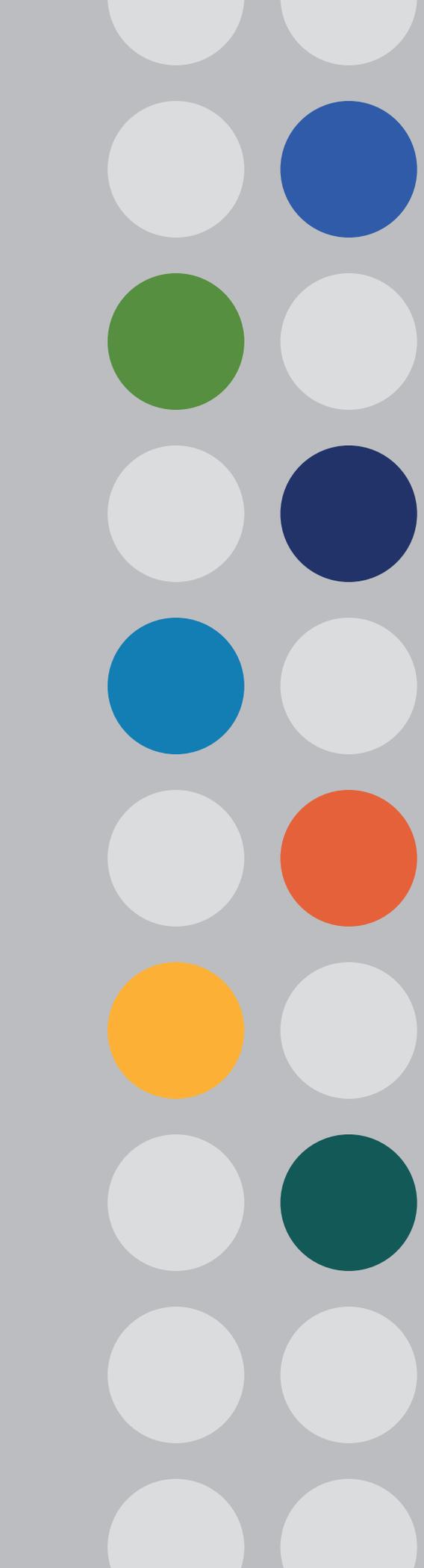
Gestion du risque d'entreprise : La nouvelle vague de risques

Canadian
Institute of
Actuaries



Institut
canadien
des actuaires

cia-ica.ca



À titre d'actuares, nous œuvrons dans le domaine du risque et de l'incertitude – nous l'estimons, le modélisons, l'analysons et l'évaluons. Selon notre appétit pour le risque, nous l'acceptons, le gérons, l'atténuons ou essayons de l'éliminer totalement. L'ignorer n'est généralement pas une option.

L'univers des risques n'a pas de limite. L'évolution des produits, des processus et de l'environnement, ainsi que le contexte mondial, réglementaire et numérique, engendrent de nouveaux risques et de potentielles opportunités.

Ce recueil d'articles sur la gestion du risque d'entreprise (GRE) de l'Institut canadien des actuares (ICA) met en évidence des sujets nouveaux et émergents d'actualité dans le monde actuel de la gestion des risques. Ces articles sont rédigés par des experts en la matière, actuares et non-actuares, qui nous donnent leurs propres opinions et nous font part de leurs expériences professionnelles.

Parmi les sujets abordés, mentionnons la maturité de la GRE, les changements climatiques, la GRE appliquée aux régimes de retraite, la légalisation du cannabis, le risque lié aux algorithmes, le cyberrisque et la culture du risque. Les spécialistes du risque doivent évaluer la façon d'intervenir et de s'adapter à ces nouveaux risques, qui peuvent influencer sur les modèles d'affaires, les ressources, les processus et les systèmes de leurs entreprises. Les organisations pourraient devoir rehausser leurs capacités de GRE à la lumière de ces risques.

La Commission de pratique sur la gestion du risque d'entreprise (CPGRE) de l'ICA tient à remercier les auteurs qui nous ont remis ces articles suscitant la réflexion. De plus, il n'aurait pas été possible de préparer cette publication sans les efforts de nos bénévoles dévoués et du personnel du siège social de l'ICA.

Contenu

- 4** La légalisation du cannabis et ses effets sur l'industrie de l'assurance-vie au Canada
- 8** Algorithmes fous
- 11** Les changements climatiques et l'industrie de l'assurance de dommages au Canada
- 14** « Où en sommes-nous? »
Faire passer la capacité de l'organisation au chapitre de la GRE à un autre niveau de maturité
- 18** Comment la GRE crée-t-elle de la valeur dans un régime de retraite interentreprises?
- 21** Cybersécurité : Le paysage de la menace financière et d'assurance
- 24** Bâtir une solide culture du risque
- 28** Sources

La légalisation du cannabis et ses effets sur l'industrie de l'assurance-vie au Canada

LLOYD MILANI, FICA, FSA, MAAA

Vice-président principal et chef de la gestion des risques, assurance-vie et santé – Amérique du Nord, Munich Re

Le 17 octobre 2018 est maintenant chose du passé et il semble que le monde, ou du moins la petite partie que nous occupons, ne s'est pas encore effondré. La seule chose que j'ai remarquée par une froide journée de janvier, alors que je me promenais dans le PATH à Toronto, c'était l'odeur âcre de pelouse brûlée qui provenait de l'extérieur. C'était pendant l'heure du lunch, après tout.

Sur une note plus sérieuse, devrions-nous nous inquiéter de la légalisation du cannabis au Canada? La consommation de cannabis est-elle différente de la consommation d'alcool? L'industrie de l'assurance est-elle

à l'autre, mentionnons une perception sensorielle accrue, des rires, une perception modifiée du temps et l'accroissement de l'appétit (mais je ne crois pas avoir besoin d'expliquer cela à qui que ce soit!).

La consommation de cannabis au Canada

Selon une étude récente de Statistique Canada, la consommation de cannabis n'a pas augmenté depuis sa légalisation (Statistique Canada, 2019a). Cette situation pourrait s'expliquer, entre autres choses, par le fait que la légalisation est assez récente et qu'il faudra du temps

indique le pourcentage de la population canadienne qui consomme du cannabis, de 1960 à 2015. Comme vous le constaterez, il y a eu une tendance à la hausse de la consommation du cannabis à compter de 2010. Cette situation était principalement attribuable au groupe des 25 à 44 ans (voir le graphique 2). Cette tendance à la hausse s'est produite bien avant que le cannabis ne devienne légal.

La consommation de cannabis à des fins récréatives peut-elle entraîner une dépendance?

Comme toute substance que vous consommez ou mangez, pour atteindre un certain degré de satisfaction, vous devrez peut-être en consommer davantage chaque fois, et l'utilisation peut mener à des abus. L'alcool, la nicotine, le cannabis, la caféine et même le sucre peuvent créer une dépendance. Selon le National Institute on Drug Abuse, il semblerait que le cannabis puisse créer une dépendance psychologique, mais pas physique (Association canadienne de santé publique, 2018). Les symptômes du sevrage du cannabis peuvent comprendre les sautes d'humeur, l'insomnie, la diminution de l'appétit et l'anxiété... ça me ressemble sans mon café du matin. De plus, une personne qui cesse de consommer cette drogue peut connaître des malaises physiques, comme des douleurs abdominales, des tremblements, des sueurs, de la fièvre, des frissons et des maux de tête pouvant durer jusqu'à deux semaines.

Impact de la légalisation de la consommation du cannabis sur l'industrie de l'assurance

Les consommateurs de cannabis affichent-ils la même mortalité que les non-fumeurs?

Selon quelques études, la consommation de cannabis ne mène pas à une mortalité plus élevée que celle d'un non-fumeur.

Dans une étude sur la consommation de cannabis et le risque de cancer du poumon (Zhang et coll., 2015), les consommateurs

Selon une étude récente de Statistique Canada, la consommation de cannabis n'a pas augmenté depuis sa légalisation.

prête à assumer la multitude de souscripteurs éventuels qui reconnaîtront dans leurs demandes d'assurance qu'ils fument un joint à l'occasion? Quels sont les effets à long terme de la consommation de cannabis sur la mortalité? En tant qu'actuaire, comment évaluerons-nous ce nouveau risque?

Comprendre ce qu'est le cannabis

Le cannabis (également appelé « marijuana ») est une plante qui peut croître dans divers climats et qui produit une substance chimique psychoactive appelée tétrahydrocannabinol (THC). Ce produit chimique se trouve dans les bourgeons fleuris de la plante. Le bourgeon lui-même peut être fumé ou l'ingrédient actif peut être extrait comme une huile. Les deux peuvent également être comestibles ou buvables. Le THC, une fois dans votre système sanguin, agit sur certains récepteurs des cellules cérébrales et provoque l'euphorie et un sentiment de relaxation. Parmi les autres effets courants (NIDA, 2018), qui peuvent varier considérablement d'une personne

avant que nous en voyions l'impact. En outre, l'offre et la distribution légales du cannabis sont encore limitées. Il sera intéressant de voir comment ces statistiques se comparent dans un an ou deux.

Le tableau 1 montre la consommation de cannabis en 2018 selon le trimestre au Canada. Les résultats sont fondés sur la consommation autodéclarée. Bien que la documentation ne le mentionne pas explicitement, il faut tenir compte du fait que ces résultats comportent un élément de sous-déclaration. Le tableau indique la consommation de cannabis selon la province, le sexe et les groupes d'âge.

La consommation de cannabis augmentera-t-elle fortement maintenant qu'elle est légale?

À mon avis, il n'y aura pas d'augmentation importante de la consommation. Ceux qui n'en ont jamais consommé pourraient l'essayer une fois par curiosité. Toutefois, la probabilité que ces personnes consomment régulièrement du cannabis à l'avenir sera probablement faible. Le graphique 1

de cannabis dans un groupe de cas souffrant du cancer du poumon ont été comparés à ceux d'un groupe témoin. Les résultats n'ont révélé qu'une faible relation entre la consommation de cannabis et le cancer du poumon.

La seconde étude, intitulée *Associations between Cannabis Use and Physical Health Problems in Early Midlife* (Meier et coll., 2016), portait sur un groupe d'un peu plus de 1 000 personnes nées en Nouvelle Zélande en 1972 et 1973, et qui ont fait l'objet d'un suivi de leur naissance jusqu'à l'âge de 38 ans. L'étude visait à mesurer l'évolution de certains indicateurs de santé entre 18 et 38 ans. Outre la piète santé parodontale des fumeurs de cannabis, aucun effet négatif n'a été observé sur d'autres indicateurs de santé comme la fonction pulmonaire, l'inflammation systémique et la santé métabolique.

Compte tenu de cette information, il semble que l'on s'attend à ce qu'un non-fumeur et un fumeur de cannabis obtiennent la même incidence de mortalité. J'ai été très étonné lorsque notre directeur médical a tenté de l'expliquer à un groupe d'actuaire... quoique j'aimerais voir quelques autres données probantes pour appuyer cet énoncé avant d'être tout à fait convaincu.

Quels sont les effets à long terme de la consommation de cannabis et quelle en sera l'incidence sur l'amélioration de la mortalité et l'état de santé général?

On pourrait soutenir que certains de ces effets peuvent déjà être intégrés à nos données d'expérience, que ce soit dans la population générale ou dans le portefeuille de polices d'un assureur. Bien que l'industrie de l'assurance ait accepté des fumeurs « occasionnels » en santé comme étant non-fumeurs seulement que ces dernières années, il peut exister une certaine consommation non déclarée au sein de la population assurée. Les deux études susmentionnées porteraient à conclure que s'il y avait un impact, celui-ci serait faible.

Enfin, en se reportant au graphique 1, de 1970 à 2010, le pourcentage de la consommation de cannabis est demeuré relativement stable, oscillant entre 10 % et 14 %, sauf pour la période autour de 1992.

L'accès facile au cannabis entraînera-t-il une augmentation du nombre de décès ou de blessures accidentels?

L'une des plus grandes inquiétudes que je ne cesse d'entendre est le danger que représentent les personnes qui conduisent avec les facultés affaiblies. Peu après la légalisation du cannabis dans les États du Colorado et de Washington, des études (Aydelotte et coll., 2017; Tefft et coll., 2016) ont été effectuées au sujet du nombre de décès imputables à la conduite automobile par suite de la consommation de cannabis. La première étude, menée un an après la légalisation, a révélé une hausse du nombre de décès. Cependant, une étude de suivi effectuée quelques années plus tard n'a révélé aucun changement important par rapport à la période précédant la légalisation.

Quels sont quelques-uns des risques que nous devons prendre en compte dans l'industrie de l'assurance-vie?

Le plus grand risque auquel nous sommes confrontés est de tenter de composer avec les inconnus ou les données incertaines. Nous devons nous interroger sur l'usage des données et leur fiabilité. Malgré les études sur la consommation de cannabis et sur la mortalité, en raison du degré de subjectivité, je ne crois pas qu'elles s'apparenteraient à une étude de mortalité normale que nous effectuerions au sein de nos entreprises. Une autre question consiste à savoir si la prévalence augmentera. Juste parce que le cannabis est maintenant légal, est-ce que plus de gens en consommeront?

Par exemple, si nous supposons qu'une tranche supplémentaire de 15 % de la population consomme du cannabis de

façon répétée et que sa mortalité est équivalente à celle d'un fumeur et qu'il n'y a pas de corrélation avec l'usage du tabac, il faudrait ajouter une charge de 25 % aux taux de primes d'assurance-vie des non-fumeurs. Cette règle s'appliquerait aussi aux polices en vigueur.

Pour répondre correctement à ces questions, nous devons d'abord analyser les données que nous recueillons déjà, afin de pouvoir effectuer des études de mortalité plus précises. Nous devons également élaborer des indicateurs précurseurs clés pour les propositions que nous acceptons pour déterminer si des mesures doivent être prises à l'étape de l'évaluation de la souscription ou si des changements doivent être apportés aux hypothèses de mortalité. En tant que praticiens en gestion des risques, nous pouvons commencer par déterminer si nous constatons une augmentation de la consommation de cannabis au moyen de l'information fournie dans les propositions d'assurance et comparer cette information aux données publiques sur la consommation de cannabis.

D'autres indicateurs possibles peuvent être l'évolution des causes de décès et leur fréquence, notamment de demander des renseignements supplémentaires au moment de la réclamation, comme la consommation d'alcool, la consommation de cannabis et l'exercice. À mesure que nous progressons vers une ère de numérisation, je me demande si l'analytique prédictive et l'apprentissage machine peuvent nous aider à prendre de l'avance dans l'analyse du risque de consommation de cannabis, plutôt que d'être coincés dans les « mauvaises herbes ».

Tableau 1 : Consommation de cannabis au Canada (en % de la population)

	2018 T1	2018 T2	2018 T3	2018 T4
Canada	14,0	15,6	15,2	15,4
Terre-Neuve-et-Labrador	16,4	18,1	16,1	19,2
Île-du-Prince-Édouard	14,1	19,2	15,0	17,9
Nouvelle-Écosse	20,0	21,0	23,0	21,6
Nouveau-Brunswick	14,3	17,3	13,8	18,9
Québec	10,4	10,6	10,1	13,6
Ontario	13,5	17,8	15,1	15,4
Manitoba	16,6	15,1	18,9	15,1
Saskatchewan	15,1	9,9	15,7	16,5
Alberta	16,6	15,6	17,0	16,2
Colombie-Britannique	17,1	17,3	20,0	15,3
Selon le sexe				
Hommes	15,8	19,1	17,5	19,4
Femmes	12,2	12,2	12,5	11,3
Selon le groupe d'âge				
15 à 24 ans	23,2	32,7	27,0	27,4
25 à 34 ans	26,1	26,9	24,5	23,2
35 à 44 ans	15,9	14,9	16,5	17,5
45 à 54 ans	8,2	10,6	12,0	12,8
55 à 64 ans	9,4	10,0	9,9	10,4
65 ans et plus	4,0	3,4	4,9	5,2

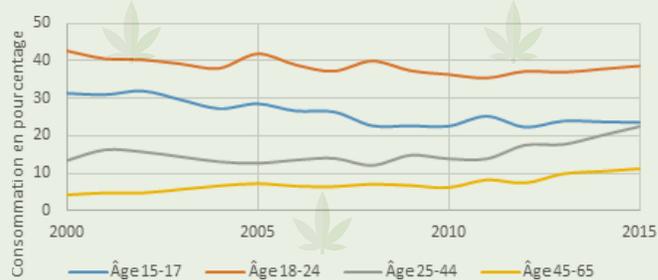
Source : Statistique Canada, 2019b.

Graphique 1 : Consommation de cannabis (en % de la population) 1960 à 2015



Source : Statistique Canada, 2018.

Graphique 2 : Consommation de cannabis (en % de la population) 2000 à 2015 par groupe d'âge

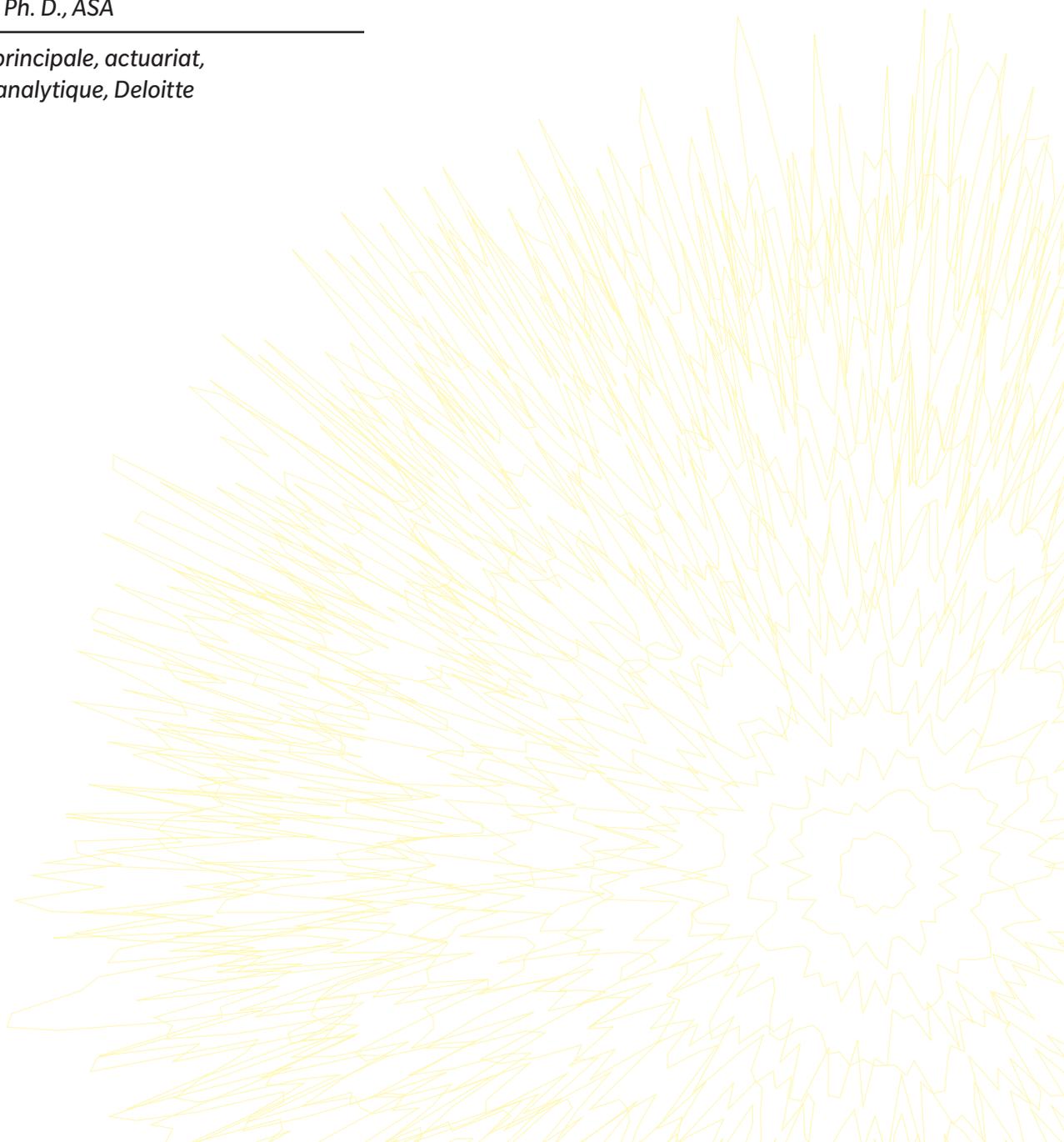


Source : Statistique Canada, 2018.

Algorithmes fous

SAISAI ZHANG, Ph. D., ASA

*Experte-conseil principale, actuariat,
récompenses et analytique, Deloitte*



Pourquoi devrions-nous porter attention au risque lié aux algorithmes?

Les algorithmes sont de plus en plus omniprésents dans notre quotidien. Avec les progrès de l'analytique des données, l'accélération de la puissance de traitement et les capacités grandissantes de l'informatique cognitive, le sens du terme « algorithme » s'est transformé, passant de programmes informatiques fondés sur des règles à des agents intelligents qui informent, voire prennent, des décisions d'une façon semblable au cerveau humain.

Ces décisions entraînent souvent des conséquences sociales ou sociétales, allant de la publicité ciblée et des offres de produits et de crédit à l'embauche, à la conduite automatisée et à la médecine personnalisée. Nous entrons dans une période où les algorithmes détiennent le pouvoir; et c'est pourquoi les retombées des algorithmes fous peuvent entraîner d'astronomiques pertes financières et atteintes réputationnelles.

Au cours de la dernière décennie, des défaillances très médiatisées d'algorithmes ont déjà fait les grands titres à l'échelle internationale. Le krach éclair de 2010, causé par la négociation par algorithme, a entraîné en quelques minutes une baisse de 9 % de l'indice industriel moyen du Dow Jones. Dans la période qui a précédé l'ouragan Irma en 2017, les algorithmes de gestion du rendement de Delta Airlines ont majoré les tarifs aériens à un niveau contraire à l'éthique dans une réaction automatisée à un choc de demande en état de crise. Tout récemment, on a soupçonné le Maneuvering Characteristics Augmentation System (un ensemble de capteurs et d'algorithmes) de l'appareil

Boeing 737 Max d'être responsable de deux écrasements d'avion en 2018 et 2019, tuant au total 346 personnes à bord.

Alors pourquoi le risque lié aux algorithmes existe-t-il?

Les risques liés aux algorithmes peuvent provenir à chaque étape de la prise de décision automatisée ou semi-automatisée : de la saisie des données à la conception de l'algorithme et aux décisions résultantes. À mesure que nous délaissions les solutions fondées sur des règles pour adopter des solutions d'apprentissage automatique, les algorithmes commencent à se libérer des protocoles strictement programmés et à assimiler de nouvelles « règles » fondées sur des données.

Il en découle que ces algorithmes ne sont, au mieux, qu'aussi valables que les données qui les alimentent, lesquelles risquent d'être incomplètes ou superflues, ou inclure des biais sociétaux qui nécessitent une intervention humaine pour compenser les effets négatifs sur les résultats.

Par exemple, des recherches ont révélé qu'en 2015, les algorithmes de Google étaient beaucoup plus susceptibles de montrer des offres d'emplois très rémunérés aux hommes à la recherche d'emploi plutôt qu'aux femmes, laissant supposer que le sexe était un « facteur » ayant influencé les résultats de ses décisions. Bien que le sexe puisse très bien être un facteur prédictif valable d'après les données, le résultat accroissant l'écart salarial entre les sexes serait incompatible avec la mission et les valeurs de l'entreprise.

À l'instar de la modélisation statistique traditionnelle, la conception d'algorithmes d'apprentissage automatique est vulnérable à une variété de risques, comme des techniques, logiques ou hypothèses défectueuses de modélisation/étalonnage. Mais qui plus est, un ensemble unique de risques découle de leur opacité (c.-à-d. leur nature de « boîte noire »). Cette opacité se présente sous trois formes distinctes (Burrell, 2016) :

- La première est le secret d'entreprise intentionnel – si les entreprises adoptent des solutions exclusives, les rouages internes de leurs algorithmes sont considérés comme leurs secrets commerciaux et ne seraient pas apparents aux utilisateurs.
- La deuxième est l'analphabétisme technique – un algorithme peut être entièrement de source ouverte, mais il reste une « boîte noire » puisque le code de lecture et d'écriture constitue un ensemble de compétences spécialisées que seule la minorité possède.
- La troisième réside dans les caractéristiques des algorithmes combinées au volume nécessaire en vue d'une utilisation qui soit pertinente – cette forme d'opacité va au-delà de l'analphabétisme technique, car un technicien peut être en mesure de comprendre le code, mais être incapable de saisir comment les routines fonctionnent dans la réalité ou fournissent des conclusions dans un environnement de production réaliste, en raison de leur niveau élevé de complexité, de leur grand nombre de dimensions et de la complexité des liens entre de nombreuses sous-routines.

Le principal constat est que les entreprises doivent aspirer à comprendre pourquoi l'opacité existe et la placer dans le contexte où les algorithmes sont déployés, plutôt que de considérer l'opacité comme inévitable. Des stratégies ciblées de gestion des risques, comme l'audit des algorithmes ou leur validation, peuvent être élaborées pour atténuer efficacement les pertes éventuelles.

Les décisions provenant des algorithmes sont vulnérables au risque de mauvaise interprétation ou de mauvaise utilisation – ces risques sont particulièrement importants lorsque l'opacité est élevée. L'opacité entraîne également une multitude de risques issus de dilemmes éthiques, quand les algorithmes sont utilisés pour prendre des décisions à conséquences sociales qui ne peuvent être facilement expliquées aux personnes touchées.

Par exemple, les algorithmes de prédiction du cancer du sein peuvent améliorer le pouvoir prédictif de la disposition d'un point de vue mathématique, mais il se peut que les médecins spécialistes ne soient pas en mesure de déterminer pourquoi de telles indications de disposition existent, ce qui laisse le patient dans la position de faire d'importants choix de vie dans le noir.

La cybersécurité est également une préoccupation grandissante à l'ère moderne de la connectivité. Les entreprises doivent également être conscientes des risques liés à la sécurité des TI, car leur vulnérabilité au piratage peut avoir une incidence négative sur leurs données, leurs algorithmes et leurs résultats, pouvant les induire de force à de mauvaises conclusions.

Que pouvons-nous faire pour empêcher les algorithmes de produire des conséquences négatives?

Il est important de comprendre que l'engouement entourant l'« assurtech », ne peut que signifier que nous commençons à voir et à entendre davantage au sujet des algorithmes utilisés et intégrés à des solutions d'assurance modernes.

Il ne fait aucun doute que les algorithmes sont l'avenir pour augmenter l'efficacité et la valeur. Alors que les sociétés d'assurance continuent d'examiner les cas d'utilisation d'algorithmes dans des domaines comme la tarification, l'analyse de la qualité des conducteurs, le traitement des réclamations, la détection de la fraude et l'analyse des sentiments des consommateurs, plusieurs questions urgentes doivent être prises en compte :

- Les entreprises sont-elles au courant de la présence de risques liés aux algorithmes?
- Comment les sociétés élaborent-elles des politiques et entretiennent-elles une culture d'entreprise qui garantit que les risques liés aux algorithmes sont compris dans l'ensemble de leurs fonctions?

- À quoi ressemble un cadre efficace de gestion du risque lié aux algorithmes?
- Quelles sont les considérations éthiques entourant la prise de décision automatisée, y compris la collecte de données et les préoccupations relatives au respect de la vie privée?
- Qui sont les talents appropriés à l'ère des algorithmes?
- Quelles nouvelles compétences les actuaires doivent-ils acquérir?
- Comment pouvons-nous conserver le plein contrôle des technologies qui ont une incidence sur nos vies et qui prennent des décisions pour nous?

Les organismes de réglementation pressent le pas en instaurant des mesures législatives réactives pour régler la prise de décisions issues d'algorithmes. Le Règlement général sur la protection des données (RGPD) de l'Union européenne (Union européenne, 2016), qui est entré en vigueur en 2018, impose des restrictions sur les algorithmes qui prennent des décisions fondées sur des données propres à un utilisateur, en insistant sur le « droit à l'explication » pour une personne qui fait l'objet d'une décision algorithmique qui l'affecte de façon significative. Qui plus est, il énonce explicitement qu'une personne a le droit de ne pas être assujettie à une décision fondée « uniquement » sur un traitement automatisé, y compris le profilage. En France, la loi pour une République numérique de 2016 impose au secteur public des règles plus strictes que le RGPD en étendant ce droit à des décisions simplement « appuyées » par un traitement algorithmique. Plus récemment, en 2019, les législateurs américains reconnaissent l'impact croissant des algorithmes sur les particuliers et ils insistent pour que les algorithmes soient testés afin de détecter les biais avant leur mise en production (Congrès américain, 2019).

Néanmoins, la réglementation sur la prise de décisions fondées sur des algorithmes est passablement à un stade précoce, et est principalement axée sur la transparence (c.-à-d. l'ouverture de la « boîte noire ») afin de promouvoir la responsabilisation. Bien

que la transparence jette les bases d'évaluation de l'équité et de la probité, il manque encore un ensemble clair de normes pour établir une saine gestion des risques et pour s'assurer que les considérations d'ordre éthique sont au premier plan de la conception et du déploiement des algorithmes.

Les cabinets d'audit ont rapidement élargi leurs services pour y inclure des services de vérification et d'assurance des algorithmes. Ils jouent un rôle essentiel dans l'écosystème global de la gestion des risques liés aux algorithmes, car en fin de compte, l'audit des algorithmes exige une vaste expertise interdisciplinaire, y compris l'informatique, l'apprentissage statistique, l'éthique, le droit, le scepticisme professionnel et la communication. Les cabinets d'audit devront modifier leurs normes et lignes directrices en matière d'audit pour tenir compte du risque lié aux algorithmes, et mettre au point des moyens de mesurer la pertinence de la conception des algorithmes et des processus de prise de décisions. Les défis, comme les progrès technologiques rapides dans la conception d'algorithmes, l'évolution réglementaire, le sentiment des consommateurs, la confidentialité des données et les préoccupations en matière de cybersécurité, doivent être pris en compte et surveillés de près pour en assurer le succès.

L'avenir des algorithmes est déjà des nôtres, et les divers intervenants de notre écosystème canadien doivent jouer leur rôle pour être mieux informés de ses risques potentiels et exiger que les algorithmes soient déployés en toute sécurité à des fins commerciales et qu'ils soient examinés sous l'angle de la sécurité publique.

Les changements climatiques et l'industrie de l'assurance de dommages au Canada

PAUL KOVACS

*Directeur général, Institut de prévention des
sinistres catastrophiques, Université Western*

Au cours de la dernière décennie, les sociétés d'assurance se sont adaptées à l'augmentation remarquable des sinistres de nature catastrophique. Néanmoins, les changements climatiques engendreront d'importants nouveaux risques et opportunités pour les sociétés d'assurance de dommages pendant les 10 prochaines années, et au-delà, notamment au chapitre de la souscription, du règlement des sinistres, des opérations, des placements, de l'atteinte à la réputation et de la réglementation.

L'assurance est affaire de gestion des risques. Les assurances IARD comprennent les risques de pertes et de dommages causés par des événements catastrophiques comme les inondations, les feux de forêt, les vents violents, la grêle, la foudre, les tempêtes hivernales et d'autres dangers météorologiques graves.

Les gouvernements se sont penchés sur deux dossiers stratégiques traitant du risque de catastrophe : les changements climatiques et la gestion des catastrophes. Un troisième dossier stratégique – la stabilité financière – émerge en raison de l'incapacité d'atteindre les objectifs de la politique internationale en matière de changements climatiques et de gestion des catastrophes.

La discussion stratégique sur les changements climatiques a été officiellement lancée au Sommet de la Terre en 1992. Établi initialement il y a 27 ans et précisé dans l'Accord de Paris de 2015, l'objectif consiste à réduire les émissions mondiales de gaz à effet de serre afin de stabiliser la température moyenne de la planète. Cependant, les émissions mondiales continuent d'augmenter, pas de chuter, et la température est en hausse, elle ne se stabilise pas.

En 1989, le Canada et la plupart des autres pays ont promulgué la Décennie Internationale de la Prévention des Catastrophes Naturelles. Dans trois accords internationaux ultérieurs, l'objectif stratégique des 30 dernières années a été de réduire les dommages directs causés par les catastrophes. Toutefois, ces dommages ont augmenté de façon alarmante, et les

facteurs sous-jacents nous avertissent que les pertes augmenteront encore davantage.

Plus tôt en 2019, le Forum Économique Mondial a déterminé que le risque croissant de dommages causés par les phénomènes météorologiques extrêmes et l'incapacité d'atteindre les objectifs d'atténuation et d'adaptation liés aux changements climatiques constitueront les deux principaux risques mondiaux au cours des 10 prochaines années.

Mark Carney, gouverneur de la Banque d'Angleterre et ancien président du Forum sur la stabilité financière, a averti qu'un traitement inadéquat des risques liés aux changements climatiques représente une menace émergente pour la stabilité du système financier. Il a abordé trois tendances fondamentales qui présentent des risques et des opportunités pour les sociétés d'assurance, les banques et les investisseurs :

- Le risque croissant de dommages matériels;
- La croissance des litiges liés au climat;
- Le risque de placement lié à la transition vers un avenir à faibles émissions de carbone.

Au cours des 40 dernières années, les prestations versées par des assureurs canadiens en raison de catastrophes ont doublé tous les cinq à 10 ans. De fortes augmentations des dommages matériels ont aussi été constatées dans la plupart des autres pays. En outre, un certain nombre de facteurs laissent planer la menace d'autres augmentations au cours des prochaines années, notamment la croissance des structures dans les régions à risque, le vieillissement des infrastructures et l'expectative d'événements météorologiques extrêmes plus fréquents et plus graves en raison des changements climatiques.

Les litiges reliés aux changements climatiques ont également augmenté au cours de cette période. En particulier, il y a eu une augmentation des contestations judiciaires aux États-Unis au cours des 10 dernières années touchant un éventail croissant



de sujets. Les litiges visant les gouvernements et les émetteurs plus importants introduisent de l'incertitude et présentent des opportunités pour les assureurs, les prêteurs et les investisseurs.

Des investissements massifs sont nécessaires pour appuyer la transition vers une société à faibles émissions de carbone, notamment la construction de maisons et de bâtiments écoénergétiques, le soutien du passage à des véhicules électriques et hybrides, et la mise au point de technologies de captage et de stockage du carbone. La transition reposera sur les changements technologiques, l'évolution des attentes des consommateurs, ainsi que la réglementation et les taxes gouvernementales. La transition présente des opportunités et des risques significatifs, dont le risque de placements pour les sociétés d'assurance.

L'industrie canadienne de l'assurance s'est adaptée à l'augmentation des sinistres de nature catastrophique. Plus particulièrement, elle a déclaré globalement un modeste bénéfice de souscription au cours de 15 des 16 dernières années, malgré l'augmentation remarquable des prestations liées à des catastrophes, notamment les inondations (Calgary, 2013), les ouragans (Juan, 2013), la grêle (Airdrie, 2014), les feux de forêt (Fort McMurray, 2016), les tornades (Ottawa, 2018) et les vents violents (Ontario, 2018) représentant les événements les plus coûteux au Canada. En outre, l'industrie a exprimé sa volonté d'élargir la couverture, pour une prime raisonnable, de risques non assurés ou sous-assurés, ce

qui a mené à l'instauration de la protection résidentielle contre les inondations (2015).

D'ici 2030 et au-delà, les conditions météorologiques extrêmes et les changements climatiques devraient engendrer des risques et des opportunités significatifs pour l'industrie canadienne de l'assurance, notamment dans les domaines de la souscription, du règlement des sinistres, des opérations, des placements, de l'atteinte à la réputation et de la réglementation.

D'abord et avant tout, le risque croissant de dommages matériels offre aux sociétés d'assurance une opportunité de croissance. Cela s'accompagne de la nécessité d'une tarification et d'une couverture de réassurance adéquates. La réglementation des taux de primes perturbe les efforts déployés par les assureurs pour garantir la suffisance des



taux aux États-Unis, mais cette ingérence n'existe pas sur les marchés d'assurance de biens immobiliers canadiens.

On s'attend à ce que de nombreux facteurs contribuent à l'augmentation des demandes d'indemnisation, y compris le vieillissement d'infrastructures de moins en moins capables d'affronter des événements météorologiques violents, l'évolution du comportement des consommateurs, comme la conversion des sous-sols en espaces de vie, et les risques de phénomènes météorologiques extrêmes plus fréquents. Ces préoccupations seront compensées par des ménages et entreprises qui investissent dans la construction

de nouveaux immeubles et la rénovation de bâtiments actuels résistants aux changements climatiques. Il faudra déployer beaucoup d'efforts pour s'assurer que la tarification de l'assurance tienne bien compte du risque de perte.

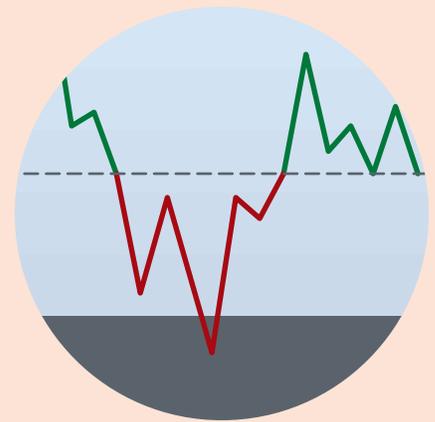
La hausse des demandes de règlement liées aux catastrophes présente des opportunités et des risques accrus pour la gestion des sinistres. Les demandes liées à des catastrophes représentent une part croissante des réclamations en dommages matériels. Les catastrophes sont concentrées dans le temps et géographiquement; plusieurs événements peuvent survenir sur une courte période et le risque de sinistres entraînant des pertes totales peut être accru. La gestion des réclamations liées aux catastrophes continuera d'évoluer, y compris pour la mise sur pied d'équipes d'intervention en cas de catastrophes et le recours à un soutien externe spécialisé.

Les assureurs doivent gérer le risque opérationnel découlant d'événements plus extrêmes. Les employés peuvent subir des dommages personnels qui nuisent à leur capacité de travailler, les entreprises d'assurance peuvent être confrontées à des pertes de courant et des immeubles peuvent être endommagés. Les plans actuels de continuité des activités pourraient être insuffisants pour rencontrer les risques futurs prévus.

La transition vers une économie à faibles émissions de carbone engendra un risque de placements et des opportunités pour les assureurs, les prêteurs et les investisseurs. Des fonds importants seront nécessaires pour aider les entreprises et les propriétaires fonciers à investir dans des mesures de résilience climatique. Les gouvernements cherchent des partenaires pour investir dans le renouvellement des infrastructures, y compris des projets qui réduiront le risque de dommages météorologiques extrêmes. Toutefois, les investisseurs peuvent être exposés à des risques réglementaires et technologiques liés aux changements climatiques, incluant la menace de variations soudaines de la valeur des actifs et d'actifs bloqués.

Les changements climatiques comportent un risque d'atteinte à la réputation pour les entreprises, y compris les sociétés d'assurance, qui ne gèrent pas activement leur impact sur l'environnement.

L'incapacité de composer avec les changements climatiques engendre des risques et opportunités réglementaires pour les sociétés d'assurance. Le Groupe de travail sur l'information financière relative aux changements climatiques élabore des recommandations internationales de divulgation à l'intention des sociétés d'assurance et de sept autres secteurs d'activités. Le Bureau du surintendant des institutions financières, l'Autorité des marchés financiers et le Conseil canadien des responsables de la réglementation d'assurance examinent actuellement la surveillance qu'ils exercent sur les risques climatiques.



En 2019, le Groupe d'experts sur la finance durable a adressé un rapport au ministre fédéral des Finances et la Banque du Canada a lancé un programme de recherche sur le climat. Les préoccupations au sujet de la stabilité financière constituent le fondement de ce nouvel intérêt en matière de réglementation des pratiques de crédit, d'assurance et de placement.

Les sociétés d'assurance canadiennes ont réussi à s'adapter à l'augmentation des réclamations liées à des catastrophes au cours des 20 dernières années et elles seront encore une fois confrontées aux risques et opportunités qui se présenteront au cours des 10 prochaines années, et au-delà.

« Où en sommes-nous? » Faire passer la capacité de l'organisation au chapitre de la GRE à un autre niveau de maturité

DANIELLE HARRISON, FICA

*Ancienne chef de la gestion des risques, Groupe
Co-operators*



La GRE au sein des sociétés d'assurance est à un stade d'évolution critique. Le rôle du chef de la gestion des risques (CGR) reste encore à définir au sein des organisations, et les professionnels de la gestion des risques sont issus de divers milieux. L'attention et les efforts se concentrent sur la réponse aux exigences réglementaires, ce qui peut prendre un certain temps.

Les éléments suivants de votre liste de contrôle sont cochés :

- Nommer un CGR ou un responsable de la fonction de GRE compétent et indépendant.
- Confier des mandats aux comités de gestion des risques et au conseil d'administration.
- Mettre en œuvre le modèle des « trois lignes de défense » ou une autre structure suffisamment robuste.
- Approuver des cadres et politiques de GRE qui énoncent de façon exhaustive la vision et les attentes en matière de GRE, ainsi que la façon dont les risques sont régis.
- Élaborer une taxonomie commune des risques et répertorier les risques clés et les contrôles.
- Formuler l'appétit pour le risque à l'aide d'énoncés définis de façon succincte.
- Sélectionner des indicateurs de risque clés qui soutiennent votre appétit pour le risque par la définition de limites et de niveaux d'alerte préventive qui surveillent périodiquement l'évolution de votre profil de risque réel en le comparant à votre appétit pour le risque.
- Évaluer et quantifier les risques les plus importants auxquels l'organisation est confrontée et effectuer des simulations de crise pour déterminer les exigences de capital.

Il peut s'écouler de nombreuses années avant que le programme de GRE d'une organisation soit au diapason des exigences et des attentes réglementaires. Il n'est pas facile d'atteindre cet objectif.

Tout va bien maintenant... n'est-ce pas?

Bien que l'approche réglementaire d'exécution de la liste de contrôle soit excellente

au départ, il s'agit également, pour bien des organisations, de la fin de l'évolution de la maturité de leur processus de GRE. Un examen plus attentif peut révéler que l'exécution des activités sur la liste n'est pas aussi achevée que vous l'aviez d'abord imaginé.

La complaisance est dangereuse. Vous pouvez travailler indéfiniment les activités de la liste de contrôle. Il ne s'agit pas d'un exercice ponctuel. Ce qui fonctionnait pour vous par le passé ne répond peut-être pas à vos besoins actuels. Des changements constants affecteront la réalisation des activités et vous serez occupé à vous assurer qu'elles sont toujours effectuées adéquatement. Nous œuvrons dans un contexte dynamique où les risques, les stratégies, l'organisation et le paysage de la concurrence évoluent sans cesse. Les risques émergents que posent le cybersécurité, les progrès de l'analytique et de l'intelligence artificielle, la légalisation de la marijuana, l'évolution du profil démographique de la population et les changements climatiques sont tous des exemples

avoir l'impression que leur réalisation est suffisante... mais ce n'est pas le cas. Les exigences réglementaires constituent un bon point de départ puisqu'elles fournissent les outils nécessaires pour mieux faire le travail. Mais ultimement, la GRE a pour but d'éviter que l'organisation ne prenne par inadvertance des risques qui n'étaient pas souhaités et n'attire l'attention sur les possibilités d'assumer stratégiquement plus de risques ou de procéder à leur arbitrage. Il est nécessaire de réaliser les activités de la liste de contrôle, mais ce n'est pas suffisant.

Quelle sera la suite?

Il peut être difficile d'accélérer le rythme et d'accéder au niveau suivant. Comment pouvons-nous contribuer à cette transition? Pour établir véritablement la GRE comme catalyseur stratégique de l'entreprise, le travail difficile doit commencer. La GRE peut devenir plus mature lorsque vous déployez efficacement votre boîte à outils

Vos cadres, politiques et rapports de GRE peuvent être en place, mais les mettez-vous vraiment en pratique?

d'enjeux qui influencent la conception de nos programmes de GRE et la priorisation de nos efforts d'atténuation des risques. Les organismes de réglementation forment également d'autres attentes à l'égard de la GRE, ce qui rallonge la liste de contrôle.

Les lignes directrices réglementaires visant à aider les organisations à faire progresser leurs programmes de GRE et à préciser le rôle de la haute direction et des membres du conseil d'administration sont devenues, dans bien des cas, la raison de l'existence du CGR et des professionnels dédiés à cette fonction au sein des sociétés d'assurance.

Compte tenu de la quantité de travail nécessaire pour intégrer ces éléments à votre programme de GRE, vous pouvez

réglementaire et que vous l'intégrez à votre culture organisationnelle. Deux leviers puissants pour y parvenir sont l'intégration et la critique constructive.

1. De l'identification à l'intégration (sensibilisation, responsabilisation, prise de décisions)

La GRE est plus efficace lorsqu'elle imprègne la culture d'une organisation, de sorte que chaque employé reconnaît qu'il a un rôle à jouer en matière de gestion des risques. La gestion des risques ne se limite pas aux professionnels de la GRE, la haute direction, le CGR ou le conseil d'administration. Il existe quelques questions permettant d'évaluer objectivement votre état actuel d'intégration.

Vos cadres, politiques et rapports de GRE peuvent être en place, mais les mettez-vous vraiment en pratique?

Ils doivent être communiqués, compris et suivis, et ils doivent décrire avec exactitude comment les risques les plus importants sont gérés. En d'autres termes, ils doivent dépasser les simples mots. Pour vraiment mettre en pratique votre gouvernance, les principes et les processus que vous avez définis pour gérer les risques doivent être pris en compte dans la prise de décisions.

Pouvez-vous imaginer une situation où vous vous attendiez à ce qu'un employé soulève une préoccupation liée au risque ou y donne suite, mais ne l'a pas fait?

Même les meilleures directives et la meilleure surveillance des risques ne peuvent tenir compte de toutes les circonstances. Il surviendra toujours des situations de risque inattendues, et une organisation dont les employés ont adopté une solide culture axée sur la sensibilisation et la responsabilisation à l'égard du risque dépassera la lettre de la loi pour s'attarder à son esprit et veiller à ce qu'un signalement opportun soit effectué et que des décisions appropriées fondées sur de l'information adéquate sur le risque soient prises. Vos employés combleront les lacunes et ils s'adapteront adéquatement aux circonstances.

Qui sait qu'il existe un comité de la haute direction chargé de la gestion des risques

au sein de votre entreprise et en quoi consiste son mandat?

Tous vos employés doivent comprendre comment et quand signaler des préoccupations à ce comité; il ne devrait pas s'agir simplement d'un comité auprès duquel le CGR ou l'équipe de la GRE le font. La distinction fondamentale entre les éléments de nature pertinente au risque et les autres se trouve dans la liste de contrôle réglementaire. Souvent, les questions de gestion stratégique font l'objet d'une discussion

créer une nouvelle tribune pour lancer ces conversations globales. Parlez de ce que l'entreprise tente de réaliser, puis intégrez-y les risques.

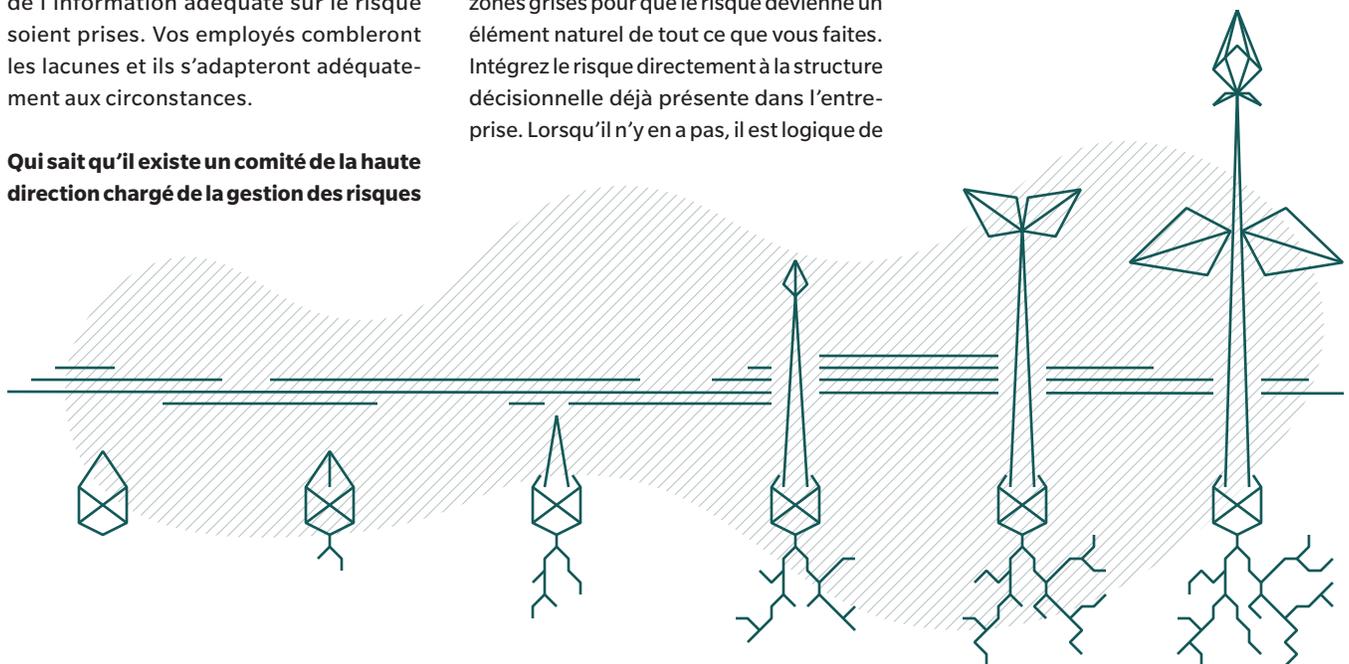
2. De la facilitation à la critique constructive (confiance, sécurité, crédibilité)

L'identification, l'évaluation, l'atténuation, la quantification et la surveillance des risques de manière holistique exigent une connaissance approfondie de l'organisation et de l'in-

Pouvez-vous imaginer une situation où vous vous attendiez à ce qu'un employé soulève une préoccupation liée au risque ou y donne suite, mais ne l'a pas fait?

distincte parmi les membres de la haute direction et elles ne sont pas soumises au comité chargé de la gestion des risques au sein de l'entreprise. L'existence de comités distincts de la haute direction rend nécessaire la distinction artificielle entre le risque et la stratégie. Intégrez harmonieusement les zones grises pour que le risque devienne un élément naturel de tout ce que vous faites. Intégrez le risque directement à la structure décisionnelle déjà présente dans l'entreprise. Lorsqu'il n'y en a pas, il est logique de

dustrie dans laquelle elle exerce son activité. Il n'est pas étonnant que de nombreux professionnels de la GRE assument le rôle de facilitateur, en puisant dans les connaissances spécialisées qui existent dans de nombreux rôles et rassemblant la sagesse collective. Il s'agit d'un exercice très important que



l'organisation doit réaliser de même qu'un ensemble de compétences tout aussi importantes que les professionnels de la GRE doivent perfectionner. Mais on peut faire plus que recueillir la contribution des experts et passer à autre chose. Les professionnels de la GRE ont une position privilégiée pour observer l'ensemble des activités de l'entreprise et ils sont indépendants. En examinant l'ensemble de l'organisation, ils peuvent cerner les incohérences et repérer les opportunités interfonctionnelles. Exerçant une fonction de supervision en tant que deuxième ligne de défense, ils ne sont pas imputables des décisions opérationnelles de l'entreprise, mais ils peuvent influencer ces décisions. Comment pouvez-vous permettre que cette perspective indépendante de l'entreprise soit présentée et qu'elle exerce une réelle influence sur les décisions? Vous pouvez prendre certaines mesures clés pour favoriser la critique constructive.

Faites en sorte que vos leaders de la GRE soient perçus comme des conseillers stratégiques, et non des délateurs. Critiquer pour critiquer n'est pas constructif, pas plus que cela ne permette d'établir des relations de confiance. Les dirigeants de la GRE et les dirigeants de l'entreprise doivent communiquer activement les uns avec les autres et examiner tous les aspects d'un problème pour élaborer les solutions envisageables. Les outils utiles à la GRE peuvent servir de mesures de référence et de points d'ancrage à ces discussions. L'atteinte d'une solution mutuellement acceptable peut ne pas être possible, mais un tel exercice effectué correctement se traduira par un examen plus rigoureux des options, ce qui renforcera la résolution de la décision finale retenue. Si les dirigeants ont confiance qu'ils seront considérés équitablement, il ne devrait y avoir aucune crainte de menace en cas de désaccord.

La critique constructive est une compétence essentielle favorisée par la sécurité qui accompagne l'indépendance et l'envergure, et par la crédibilité provenant de la formation et de l'expérience. Les responsables de la GRE doivent s'exprimer ouvertement, surtout lorsque les membres de l'entreprise estiment qu'ils ne peuvent pas le faire. Ils

disposent d'une plateforme pour mettre en lumière différents points de vue afin de s'assurer que tout a été pris en compte et qu'il n'y a pas d'angles morts ni de « vaches sacrées » interdits de discussion. C'est leur rôle, et l'exercice peut laisser des cicatrices. Un déséquilibre des connaissances et/ou du pouvoir dans n'importe quelle discussion peut intimider et empêcher l'expression d'une critique constructive. De plus, une culture organisationnelle qui évite les conflits productifs peut qualifier les dirigeants de la GRE d'antagonistes. Notre tendance à la conformité peut littéralement changer ce que nous voyons. Les organisations doivent atténuer « la douleur de l'indépendance » pour cultiver des points de vue diversifiés.

[Traduction libre] « Si vous pouvez exprimer ce à quoi ressemblent des tensions saines, productives et souhaitables, vous pouvez empêcher les gens d'interpréter la diversité de la pensée comme une dynamique dysfonctionnelle, explique Liane Davey dans son livre publié récemment, *The Good Fight*. Grâce à une meilleure sensibilisation et à un langage commun, votre équipe commencera à s'apercevoir qu'une grande partie de ce qu'elle a interprété comme des frictions interpersonnelles était en fait une tension parfaitement saine issue de la différence des rôles. » Les divergences d'opinions sont peu pratiques et nous obligent à travailler davantage. Cependant, la création d'un environnement où ces opinions sont prises en compte dès le départ peut prévenir des faux pas dévastateurs.

L'équipe de la GRE doit représenter un terrain d'entraînement pour les meilleurs talents alors qu'ils effectuent une rotation dans l'ensemble de l'organisation et en renforcent la culture.

De nombreux responsables estimés de la GRE ont travaillé directement dans différents secteurs de l'entreprise. Leur expérience leur permet de comprendre ce que sont les risques et les contraintes pratiques permettant de les atténuer; ils possèdent les connaissances et la sagacité nécessaires pour critiquer éloquemment les opinions qui leur sont présentées. De même, de nombreux chefs d'entreprise appréciés

ont travaillé au sein d'une fonction de GRE à un moment ou à un autre de leur carrière. Ils comprennent la difficulté d'exercer une influence lorsque vous ne possédez pas un sens « critique » bien exercé qui inspire de saines décisions.

À quoi ressemble une capacité de GRE mature?

Ma vision de la GRE passe par l'évolution au-delà d'une liste de contrôle réglementaire bien tenue à un déploiement complet des outils de GRE passant par son intégration et la critique constructive. Ce n'est qu'à ce moment que les organisations pourront s'attaquer à ce qui compte vraiment : veiller à prendre des décisions éclairées sur les risques afin de favoriser l'atteinte de résultats fiables.

Les sociétés d'assurance tentent de s'adapter à un taux de changement sans cesse croissant, cherchant à accroître l'efficacité de leurs opérations tout en renforçant simultanément leur résilience financière et opérationnelle. Le dialogue intégrant la stratégie et les risques ainsi que la prise de décision exhaustive, enrichis de perspectives variées, sont les caractéristiques d'une capacité de GRE mature et ils se prêtent bien à ces objectifs communs d'efficacité et de résilience. Nous constituons une main-d'œuvre qui apprend à adopter la philosophie d'« échec rapide », l'application de notre capacité de GRE diminuera la probabilité que nos initiatives échouent dès leur mise en application et se traduisent par des conséquences désastreuses. Nous nous tournons vers de nombreux domaines pour rehausser notre avantage stratégique, à partir de l'expérience client jusqu'à l'analytique et le numérique. J'encourage la haute direction et les conseils d'administration de nos organisations à rehausser leur capacité de GRE comme élément de différenciation stratégique.

Comment la GRE crée-t-elle de la valeur dans un régime de retraite interentreprises?

LEEANNE K. BARNES

Directrice, gestion du risque opérationnel et d'entreprise, stratégie et risque, Régime de retraite des enseignantes et des enseignants de l'Ontario

Pour un régime de retraite interentreprises comme le Régime de retraite des enseignantes et des enseignants de l'Ontario (RREO), la mission consiste à offrir des prestations de retraite viagères à ses participants. On comprend qu'il existe des risques inhérents dans toutes les activités d'un régime de retraite de ce type, du portefeuille de placements et des services aux participants à la prise de décisions stratégiques, opérationnelles ou de gouvernance. Pour composer avec l'éventail des risques auxquels sont exposés les régimes de retraite, les conseils d'administration et les équipes de direction ont instauré des programmes de GRE. En outre, ils reconnaissent qu'une solide culture et une approche rigoureuse de la gestion des risques sont essentielles au respect de la promesse en matière de retraite faite aux participants.

Cela signifie que la GRE d'un régime de retraite dépasse les cinq piliers traditionnels que sont l'identification, l'évaluation, l'atténuation et la gestion, la quantification et la surveillance, ainsi que la production de rapports sur les risques. Lorsque la valeur de la GRE est reconnue et défendue par le conseil d'administration et la direction, elle imprègne l'ensemble de l'organisation et intègre la conscience du risque à la culture. La GRE devient un catalyseur stratégique en fournissant des renseignements utiles aux dirigeants pour appuyer la prise de décisions sur les priorités organisationnelles et l'affectation efficace des ressources afin d'assurer la viabilité à long terme tout en préservant l'équilibre de la relation risque-rendement.

Plusieurs régimes de retraite ont établi un programme de GRE après la crise financière mondiale de 2008. Depuis, bon nombre d'entre eux ont progressé d'un programme de base à une fonction orientée

sur la stratégie où les hypothèses internes et externes existantes sont remises en question, l'information sur les risques est communiquée efficacement et les domaines d'intérêt sont mis en évidence. Un cadre de GRE fournit une approche cohérente et simple pour définir le risque et l'appétit pour le risque entre ses grandes catégories et permet de profiter d'une structure de gouvernance améliorée par la présence de protocoles de signalement favorisant la discussion autour de la gestion des risques existants, nouveaux et émergents.

Selon le RREO, trois catalyseurs clés sont importants pour développer la maturité de la GRE :

- L'appui ferme du conseil d'administration et de l'équipe de direction reconnaissant la valeur que la GRE procure à l'organisation en concentrant l'attention sur les zones de risque ce qui déclenche des discussions approfondies et rigoureuses sur la façon d'atteindre les objectifs.
- Le modèle de partenariat avec l'entreprise est fondé sur la confiance et la transparence. La mobilisation des cadres supérieurs dans l'ensemble de l'organisation, appuyée par les responsables des risques de l'équipe de direction et les partenaires de risque, est essentielle pour soulever les constats importants.
- La méthode d'évaluation des risques doit évoluer continuellement en mettant à profit les pratiques exemplaires de l'industrie et en les ajustant pour répondre aux besoins d'un régime de retraite particulier, car les approches universelles ne conviennent pas à tous.

Par exemple, au sein du RREO, les changements climatiques et la cybersécurité sont deux risques importants devant être abordés maintenant par la direction afin d'éviter des répercussions négatives importantes dans l'avenir. Les risques liés aux changements climatiques pourraient avoir une incidence sur le maintien à long terme du rendement des placements, tandis que les risques relatifs à la cybersécurité pourraient constituer une menace pour nos systèmes et nos données.

L'identification de ces risques est une bonne première étape, mais la valeur n'est réalisée que lorsque les méthodes d'atténuation de ces risques sont ajustées. Le RREO a amélioré ses processus de placements afin de tenir compte systématiquement des répercussions éventuelles des facteurs environnementaux, sociaux et de gouvernance, y compris ceux liés aux changements climatiques, en collaborant avec des sociétés de portefeuille et des gestionnaires externes des placements pour obtenir de l'information pour mieux comprendre comment ils évaluent, gèrent et divulguent les expositions aux risques climatiques. Nous préconisons des politiques et des règlements clairs et stables qui favorisent une transition ordonnée vers une économie à faibles émissions de carbone, et nous appuyons les recommandations du Groupe de travail sur l'information financière relative aux changements climatiques (GIFCC), publiées en 2017 par le Financial Stability Board (Conseil de stabilité financière) visant à promouvoir la divulgation d'informations financières relatives aux changements climatiques cohérentes, comparables, fiables et efficaces, fournissant des

renseignements utiles à la prise de décisions aux prêteurs, aux assureurs et aux investisseurs.

En matière de cybersécurité, nous utilisons un programme exhaustif contribuant à protéger l'organisation contre les fuites de données et autres incidents. Le programme veille à la présence de contrôles appropriés pour protéger les renseignements de l'organisation et s'assurer régulièrement de leur efficacité. Nos plans d'intervention en cas d'incident sont mis à l'essai et en pratique régulièrement, pour qu'ils soient le plus prêts possible à gérer les incidents de cybersécurité ou de menace à la continuité des affaires, et à s'en remettre advenant leur survenance.

Alors que les régimes de retraite interentreprises poursuivent leur parcours dans la GRE, ils doivent garder à l'esprit d'éviter la complaisance à l'égard de leurs programmes actuels, peu importe leur degré de maturité. Il y a toujours place à l'évolution et à l'amélioration. Par exemple, d'autres progrès pourraient porter sur le renforcement des capacités de compréhension de l'interdépendance des risques. Ceci fournirait des renseignements importants sur les thèmes et les tendances significatifs qui pourraient influencer sur la viabilité.

Un autre domaine d'intérêt pourrait consister à élargir l'adhésion à la GRE des interv-

enants de tous les niveaux de l'organisation et de l'extérieur, par divers moyens. On pourrait alors identifier de nouvelles perspectives sur les risques et les opportunités pour améliorer les discussions stratégiques. En renforçant l'importance de la gestion quotidienne des risques et de la prise de décisions de première ligne, la GRE pourrait également avoir un effet positif sur la culture de l'organisation. Étant donné que les risques d'entreprise sont liés à la planification d'entreprise, la communication de la GRE peut être mise à profit pour mieux faire connaître les liens entre les travaux au niveau des équipes et le contexte plus large des objectifs de l'organisation.

Nous nous attendons à ce que les régimes de retraite interentreprises soient actifs pour les générations à venir et à ce que leurs objectifs organisationnels soient définis pour réaliser leur mission. Un programme de GRE peut ajouter de la valeur en faisant en sorte que la direction demeure concentrée sur les risques et les opportunités importants, actuels et potentiels, qui pourraient avoir le plus d'effet sur ces objectifs organisationnels. Cela permettra également de mieux protéger la réputation du régime de retraite tout en

aidant l'entreprise à se concentrer sur des stratégies de croissance novatrices pour continuer à fournir à vie des bénéfices de retraite aux participants.

Le présent article a été rédigé à partir des leçons apprises par les professionnels de la GRE du Régime de retraite des enseignantes et des enseignants de l'Ontario et il ne vise pas d'autres régimes de retraite.

Cybersécurité : Le paysage de la menace financière et d'assurance

JESSE JORDAN

Expert-conseil principal, FireEye Mandiant

Les cyberattaques continuent d'évoluer. Les organisations de toutes tailles sont ciblées par divers cybercriminels qui recourent à une vaste gamme de tactiques et de techniques. Les incidents d'extorsion sont en hausse et les attaques contre les services infonuagiques ont augmenté en raison d'une plus grande utilisation de l'infonuagique par les organisations dans le cadre de stratégies TI globales.

Bien que des cyberattaques contre tous les secteurs d'activité soient signalées, les institutions financières demeurent principalement visées. Parmi les incidents auxquels la division d'expertise-conseil Mandiant de FireEye (une firme de cybersécurité) a répondu en 2018, 23 % ont touché l'industrie des services financiers.

Portrait des menaces visant les industries des services financiers et de l'assurance

Les auteurs de menaces commandités par l'État continuent de poser un risque élevé pour les industries des services financiers et de l'assurance, qui ont toutes deux accès à un éventail de renseignements de nature

de souscription. L'information recueillie, qui comprend des profils complets de vulnérabilité liés à des actifs de grande valeur, peut être utilisée par les auteurs de menaces pour déterminer les failles potentielles. Les auteurs de menaces commandités par l'État peuvent également faire bénéficier les intérêts commerciaux d'une nation en obtenant des renseignements économiques provenant de négociations commerciales avec des entités étrangères.

En 2018, la Corée du Nord, la Russie, la Chine et l'Iran ont été responsables du plus grand nombre d'attaques de cyberespionnage dans le monde. Nous avons constaté une complexité accrue des attaques d'auteurs nord-coréens ciblant des institutions financières par l'exploitation de vulnérabilités non déclarées auparavant (zero-day vulnerabilities), des attaques d'hameçonnage ciblées contre des chefs de la direction et des chefs des services financiers, et des attaques de chaîne d'approvisionnement motivées par un gain financier. Des attaques visant une chaîne d'approvisionnement peuvent survenir lorsque des pirates réussissent à infiltrer une organisation par l'entremise d'un four-

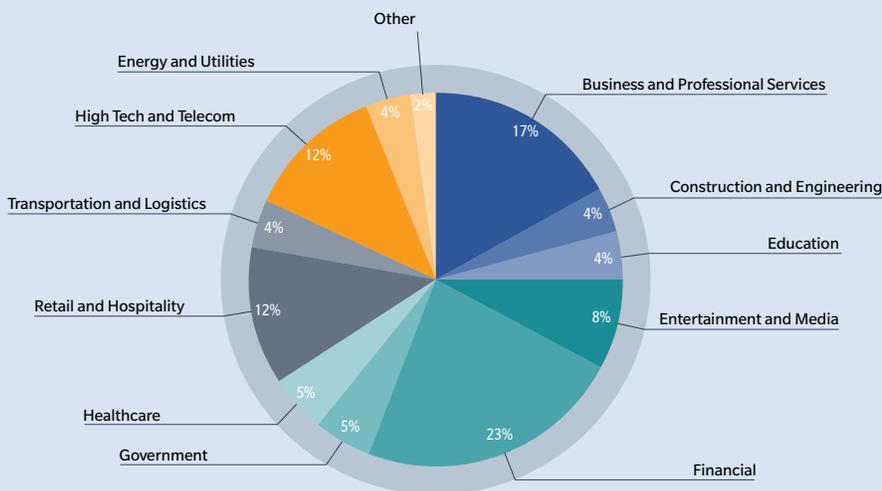
efficaces, car un seul élément compromis dans la chaîne d'approvisionnement peut faire un grand nombre de victimes. Mandiant a relevé des exemples récents où des auteurs de menaces ont été en mesure d'insérer un code malveillant dans des ressources logicielles collaboratives, dans certains cas par l'entremise de personnes malveillantes en interne, ou ont expédié à des clients des dispositifs renfermant un logiciel malveillant préinstallé. Si la rupture de la chaîne d'approvisionnement est suffisamment importante, les auteurs de menaces commandités par l'État passent essentiellement inaperçus.

Les auteurs de menaces considèrent les attaques de la chaîne d'approvisionnement comme un moyen efficace de contourner des années d'investissement dans des moyens de défense périmétriques par des organisations matures en termes de cyberdéfense. Ces dernières années, Mandiant a noté une importante augmentation de ces types d'attaques.

L'augmentation du nombre d'attaques de la chaîne d'approvisionnement à motivation financière par des auteurs de menaces commandités par l'État peut être attribuée en partie à des sanctions accrues contre certains des États-nations cités précédemment, lorsque l'obtention de fonds par tous les moyens est jugée nécessaire. Par exemple, dans le cadre d'opérations menées à l'échelle mondiale, des pirates nord-coréens ont tenté de voler plus de 1,1 milliard de dollars US à des sociétés financières en exploitant des transferts entre banques sur une période de deux années.

Les cybercriminels continuent également de cibler les entreprises dans les industries des services financiers et de l'assurance en tirant parti de l'ingénierie sociale et des attaques d'hameçonnage pour expédier des rançongiciels dans le but d'extorquer des organisations pour en tirer un gain financier. Les cybercriminels utilisent des méthodes semblables pour voler des renseignements de nature délicate à la fois aux assureurs et à leurs clients, en conservant ces renseignements sous la menace d'une divulgation publique si l'organisation ne répond pas à certaines demandes financières. Les cybercriminels tirent également parti des informations échangées dans le cadre de la souscription d'une police d'assurance par un client pour

Graphique 1 : Rapport M-Trends 2019 de FireEye Mandiant – Industries étudiées



Source : FireEye Mandiant, 2019. Reproduit avec permission. Disponible en anglais seulement.

délicate sur leurs clients. En ce qui concerne les assurances, les courtiers examinent les risques potentiels auxquels leurs clients sont exposés dans le cadre du processus

naisseur de produits ou services par le biais d'un code ou d'une infrastructure partagés en recourant à des modes de distribution fiables. Ces attaques sont particulièrement

recueillir des renseignements sensibles et les vendre ensuite sur les marchés clandestins pour le vol d'identité, l'extorsion et la fraude.

Mandiant prévoit que la cybercriminalité, en particulier la cyberfraude, continuera de progresser en 2019. La hausse des attaques contre des sites Web financiers, où des « cloneurs » virtuels sont utilisés pour voler des renseignements personnels, des numéros de cartes de paiement et des codes CVC de cartes de crédit, se pour-

La détection et l'intervention précoces sont essentielles

Les organisations des Amériques détectent plus rapidement les menaces à leur environnement. Le temps d'arrêt médian, qui correspond au temps pendant lequel les auteurs de menaces sont demeurés dans les réseaux de victimes, de la première preuve de compromission à la détection de l'intrusion, a diminué, passant de 99 jours en 2016 à 71 jours deux ans plus

uniforme et exhaustive. Des solutions centralisées de gestion des risques peuvent être mises en œuvre pour faciliter un suivi normalisé des risques de cybersécurité et des processus afférents.

Lors du suivi des risques, il convient de tenir compte des fournisseurs susceptibles d'exposer l'organisation dans les cas où ils seraient victimes d'une attaque. Il convient par le fait même d'implanter des contrôles connexes, comme la gestion d'un nombre réduit de fournisseurs et l'imposition d'exigences strictes de contrôle et d'attestation des fournisseurs, tout en veillant à ce que les changements non autorisés apportés aux logiciels soient décelés au moyen de processus établis.

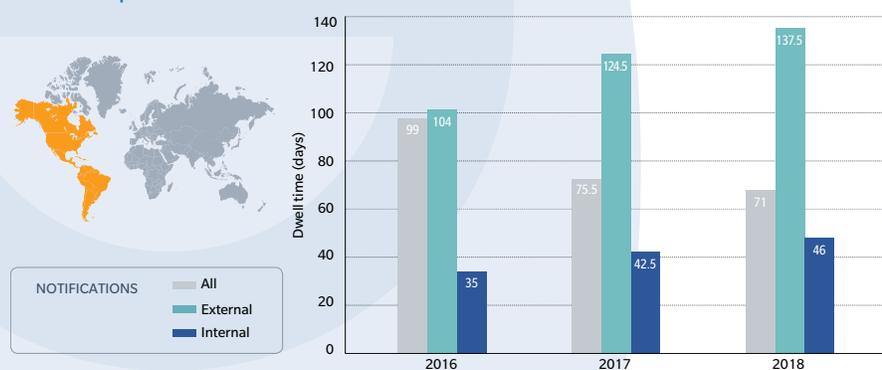
Les organisations doivent également assurer la mise en place d'un cadre et d'une méthodologie cohérents et systématiques de détection des incidents de cybersécurité, en plus de définir un processus d'analyse, de priorisation, de confinement et d'intervention.

Des exercices de simulation pour mesurer l'efficacité des interventions, combinés à des évaluations régulières de l'équipe d'intervention pour évaluer les capacités de détection et d'intervention de l'organisation, peuvent être utilisés pour rationaliser et améliorer davantage les capacités. Les tests de pénétration internes et externes constituent également un moyen efficace de détecter les vulnérabilités et les problèmes de configuration que les auteurs de menaces utilisent pour exploiter les environnements et obtenir davantage d'accès.

La formation du personnel sur la façon de repérer et de signaler un courriel d'hameçonnage, en particulier ceux qui demandent à l'utilisateur de prendre une mesure particulière, est également un facteur important pour empêcher les auteurs de menaces d'accéder initialement à un compte. Les simulations régulières d'hameçonnage représentent un moyen éprouvé de tester les messages de sensibilisation et l'efficacité globale des programmes.

Les atteintes à la sécurité sont inévitables, mais grâce à de solides pratiques de gouvernance de la sécurité et à une approche définie de gestion des incidents combinée à des mesures préventives, les organisations peuvent réduire leur impact global.

Graphique 2 : M-Trends 2019 de FireEye Mandiant – Temps d'arrêt médians dans les Amériques



Source : FireEye Mandiant, 2019. Reproduit avec permission. Disponible en anglais seulement.

suivra. En 2018, les auteurs de menaces financières ont eu recours à des techniques avancées pour contourner les processus d'enregistrement des comptes par l'entremise de portails en ligne afin d'avoir accès aux comptes, de transférer des fonds, de commander des chèques et de modifier les destinations des transactions.

Bien qu'ils posent un risque relativement faible pour les industries des services financiers et de l'assurance, les pirates informatiques activistes continuent de causer des perturbations sous forme d'attaques à motifs idéologiques, dont l'objectif consiste souvent à porter atteinte à la réputation d'une organisation, ce qui entraîne des pertes de parts de marché, soit en exposant des renseignements de nature délicate sur les clients, en volant des renseignements stratégiques ou en tentant de causer des interruptions d'affaires en effectuant des attaques par déni de service contre des sites Web destinés aux clients ou d'autres systèmes critiques.

tard (voir le graphique 2). Cette diminution est en grande partie attribuable aux organisations qui travaillent à améliorer continuellement leur capacité de détecter rapidement les menaces – soit en créant des unités internes de surveillance des menaces, soit en mettant au point une capacité accrue de détection et d'intervention en matière de réseau, de point d'accès et d'infonuagique.

En outre, il importe d'assurer la participation de la sécurité aux pratiques de GRE au moyen d'une stratégie de gestion des risques clairement définie en ce qui a trait aux cybermenaces. Les organisations devraient adopter une vision structurée, incluant la mesure des risques, pour la sécurité et prévoir des stratégies claires d'atténuation et de correction.

Des processus détaillés de quantification, de classement, de propriété, de suivi et d'atténuation devraient être élaborés pour garantir l'application d'une approche

Bâtir une solide culture du risque

MIKE STRAMAGLIA, FICA, FSA, CERA, ICD.D

Directeur en résidence, Global Risk Institute



Cet article fait partie d'une collection d'articles portant sur la gestion du risque d'entreprise (GRE) de l'Institut canadien des actuaires (ICA). Ces articles ont été rédigés par des experts en la matière, actuaires et non-actuaires, qui nous donnent leurs propres opinions et nous font part de leurs expériences professionnelles. Ils mettent ainsi en lumière des questions nouvelles et émergentes dans le monde actuel de la gestion des risques. Lisez tous les articles à cia-ica.ca/gre.

Même l'observateur le moins averti remarquera que les manchettes des journaux continuent d'être alimentées par un flot constant de scandales corporatifs, de méfaits et d'autres « faux pas » variés en matière de conduite et de gestion des risques. Bien qu'aucun secteur ou aucune industrie ou région ne semble à l'abri de ces incidents, l'industrie des services financiers semble avoir acquis un profil particulièrement prédominant à cet égard (p. ex., transactions malhonnêtes, pratiques de vente trompeuses, stratagèmes d'investissement de Ponzi, pratiques comptables douteuses, manipulation du marché/des indices de référence et, bien sûr, la crise financière de la fin des années 2000).

Il n'est donc pas surprenant que ces événements entraînent inévitablement une vaste analyse rétrospective et de nombreux commentaires, alors que les organismes de réglementation, les conseils d'administration, la direction et d'autres intervenants clés s'efforcent d'en comprendre les causes profondes et la façon dont ces connaissances acquises pourraient aider à prévenir de telles débâcles.

Un thème récurrent dans la plupart des récits et des analyses résultants indiquent que ces événements sont souvent directement attribuables à une forme quelconque de « défaillance importante de la culture (du risque) ».

La question évidente que cette révélation pose aux gestionnaires du risque est la suivante : « Quelles sont les pratiques ou les conditions organisationnelles qui minent l'établissement d'une culture du risque efficace, et donc notre capacité à éviter des pertes significatives? » ou, ce qui est équivalent, mais en des termes plus constructifs, « quelles sont les pratiques ou les conditions organisationnelles qui contribuent à favoriser une solide culture du risque et, par conséquent, à accroître notre confiance dans l'atteinte des objectifs organisationnels? »

Pour répondre à ces questions, il faut d'abord définir clairement ce qui constitue une « solide culture du risque » :

Une solide culture du risque peut être attribuée à une organisation qui assume systématiquement les bons risques de la bonne façon.

- Le terme « systématiquement » s'applique à de multiples facettes, y compris au fil du temps (pas seulement périodiquement ou pendant certaines parties du cycle économique/commercial, etc.), à l'échelle de l'organisation (toutes les unités opérationnelles/entités/divisions, le siège social, etc.) et de façon ascendante/descendante à la hiérarchie de la direction (des premières lignes jusqu'à la « salle du conseil », les attentes en matière de gestion des risques étant également appliquées explicitement à tous les fournisseurs tiers/intermédiaires, etc.).
- Les « bons risques » désignent uniquement les risques pris activement et qui sont cohérents avec l'appétit pour le risque de l'organisation ainsi qu'à sa capacité et à ses compétences à les assumer, les risques requis pour faire progresser sa stratégie, sa mission et ses objectifs, les risques pour lesquels elle est adéquatement rémunérée, etc. Il convient également de noter que cette définition reconnaît que les organisations doivent assumer activement et gérer des risques pour atteindre leurs objectifs. Une solide culture du risque ne se caractérise pas par un biais systématique à l'égard d'un évitement perpétuel des risques.
- La « bonne façon » sous-entend que la prise de risques suit des processus robustes d'évaluation et de mesure des risques, qu'elle fait l'objet d'une surveillance et d'un contrôle continu et proportionnels des risques, que la prise de risques est conforme aux valeurs organisationnelles, etc.

En gardant cette définition concrète à l'esprit, il est possible de cerner un certain nombre de saines pratiques et conditions de gestion qui peuvent souvent jouer un rôle essentiel dans l'établissement de la culture du risque d'une organisation. Cela comprend notamment la formulation et l'harmonisation de l'appétit pour le risque de l'organisation, la capacité à envisager des risques de faible probabilité/gravité élevée, les programmes de récompense et de reconnaissance, les pratiques en matière de leadership, à la promotion de l'apprentissage continu et la capacité à susciter une remise en question constructive. Afin d'illustrer en quoi la définition ci-dessus d'une « solide culture du risque » pourrait aider à façonner les pratiques

de gestion dans ces domaines clés, les trois premiers sont explorés plus en détail ci-dessous. Chaque exemple est accompagné d'une brève description et de questions dont les gestionnaires du risque devraient tenir compte pour déterminer si l'état actuel de cette pratique au sein de leur organisation favorise une culture du risque solide ou faible.

Formulation et harmonisation de l'appétit pour le risque

L'harmonisation de l'appétit pour le risque est un déterminant fondamental de ce qui constitue les « bons risques ». Il est donc impossible d'avoir une solide culture du risque sans le niveau requis de compréhension et de consensus à l'échelle de l'organisation au sujet de son appétit pour le risque. Cet appétit fournit également un contexte commun pour faciliter le type de remise en question constructive qui est également essentiel pour bâtir une solide culture du risque, illustrant l'interconnectivité qui est souvent inhérente à ces pratiques et conditions essentielles qui façonnent la culture du risque.

- L'appétit pour le risque correspond-elle à la stratégie, à la mission et aux objectifs de l'organisation, ou l'atteinte de ces objectifs exige-t-elle en fait des niveaux d'appétit pour le risque plus élevés ou plus faibles que ceux qui sont prévus?
- Dans quelle mesure les communications, les programmes de formation, etc., connexes permettent-ils de s'assurer que tous les intervenants internes et externes comprennent l'appétit pour le risque à un niveau proportionnel à leurs activités de gestion des risques?
- Dans quelle mesure l'appétit pour le risque est-elle intégrée efficacement aux décisions courantes en matière de gestion des risques (p. ex., le processus d'approbation des analyses de rentabilisation (*business case*) exige-t-il une démonstration de la cohérence de l'initiative proposée avec l'appétit pour le risque de l'organisation)?
- La formulation de l'appétit pour le risque appuie-t-elle suffisamment la gestion des risques inhabituels, émergents ou non envisagés en fournissant le contexte des principes et de la philosophie de l'organisation sous-jacents à la prise de risques?

Capacité de l'organisation d'envisager des événements à faible probabilité/gravité élevée

Les organisations caractérisées par une faible culture du risque semblent souvent atteintes de myopie systémique, ou du moins d'un manque fondamental d'imagination, autour d'événements peu fréquents mais très graves (« Cela ne pourrait jamais se produire ici... »). Cette situation peut être attribuée à divers facteurs, dont l'incapacité de reconnaître et d'atténuer le type de biais cognitifs qui peut souvent mener à une sous-estimation importante des probabilités sous-jacentes aux événements extrêmes associés aux queues de distribution. Par exemple, par définition, la probabilité d'avoir observé un événement de type 1:200 est très improbable en vertu de l'historique de pertes connues de l'organisation. Toutefois, l'appétit pour le risque est souvent établi en fonction de fréquences très faibles, liées à des événements non observés auparavant. Les organisations doivent donc surmonter la tendance naturelle à se fier presque exclusivement à l'expérience passée, apparemment bénigne, pour formuler ces évaluations des risques.

- L'organisation a-t-elle pris des mesures explicites pour s'assurer qu'elle ne succombera pas au biais causé par un échantillon de trop petite taille ou par des événements récents dans l'évaluation de ses risques liés à des événements à faible probabilité/gravité élevée?
- L'organisation applique-t-elle régulièrement des techniques de simulation de crise inversée pour faciliter la discussion ou l'évaluation de scénarios de risque extrêmes et qui n'aurait pas lieu autrement?
- Les processus d'identification et d'évaluation des risques de l'organisation vont-ils au-delà des conséquences directes des risques pour saisir adéquatement les effets de l'interconnectivité et de contamination (« effet domino »)?
- L'organisation remet-elle régulièrement en question des secteurs d'activité qui semblent particulièrement bien fonctionner, plutôt que de se concentrer uniquement sur les secteurs sous-performants?

Programmes de récompense et de reconnaissance

Il n'est donc pas surprenant que les programmes de récompense et de reconnaissance mal conçus soient souvent cités comme le principal facteur d'un comportement de gestion malsain. La capacité d'un programme d'incitatifs d'influencer la prise de risques (dans ce contexte, prendre les « bons risques » de la « bonne façon ») et, par conséquent, de façonner la culture du risque est bien documentée. Les conséquences imprévues d'un comportement orienté sur la prise de risques sont souvent attribuables à une forme quelconque de biais structurel où les systèmes incitatifs se concentrent exclusivement sur les résultats obtenus, sans suffisamment tenir compte de la façon dont ces résultats sont obtenus.

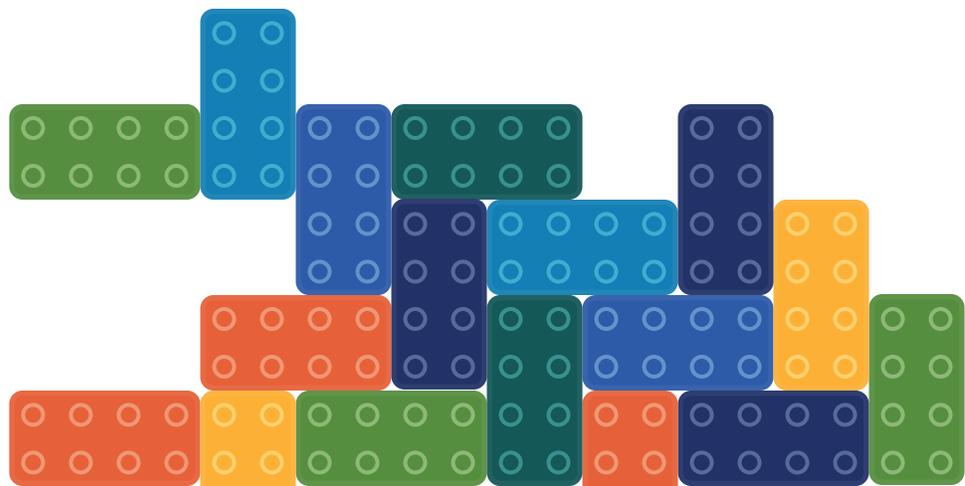
- Les cibles de rendement intégrées aux programmes incitatifs sont-elles raisonnablement réalisables en respectant l'appétit pour le risque prescrit et les pratiques commerciales éthiques?
- Les principales mesures de rendement sont-elles adéquatement ajustées en fonction des risques?
- Dans quelle mesure les objectifs de gestion des risques sont-ils explicitement pris en compte dans les objectifs annuels de gestion du rendement?
- Les programmes d'incitatifs intègrent-ils explicitement des protocoles pour exercer un pouvoir discrétionnaire au besoin afin de tenir compte adéquatement des résultats fondés sur le risque? Les principaux programmes incitatifs comprennent-ils des niveaux appropriés

de report, des dispositions de récupération, etc., afin de faire progresser de manière cohérente cet objectif?

- Le chef de la gestion des risques (« CGR ») participe-t-il à l'examen de la conception des programmes de rémunération incitative et des résultats proforma obtenus afin d'évaluer de façon indépendante l'harmonisation avec l'appétit pour le risque? Le CGR fait-il officiellement rapport de cet examen au conseil d'administration (ou à un comité désigné sur la rémunération)?
- Dans quelle mesure les décisions clés en matière de ressources humaines (embauche, promotion, cessation d'emploi, etc.) intègrent-elles explicitement les évaluations des valeurs avérées d'une personne et de ses comportements généraux en matière de gestion des risques?

En mettant en œuvre la définition pratique d'une solide culture du risque présentée dans cet article, les gestionnaires de risque peuvent développer un catalogue exhaustif de pratiques de gestion qui sont requises pour cultiver les trois principes d'une culture du risque illustrés plus haut, ainsi que les principaux moteurs d'une culture du risque, tels que les pratiques de leadership, la promotion de l'apprentissage continu et la capacité à susciter une remise en question constructive.

Le répertoire de pratiques de gestion qui en résulte peut aider à évaluer l'harmonisation d'une organisation avec les principes de base d'une culture du risque et, par conséquent, permettre d'orienter ses efforts pour établir les principales pratiques de gestion requises pour prendre constamment les bons risques de la bonne façon, ce qui accroît la confiance dans l'atteinte des résultats organisationnels souhaités.



Cette publication a été préparée par la Commission de pratique sur la gestion du risque d'entreprise de l'ICA.

Membres :

Mario Robitaille (président)
Joel Cornberg
Claude Désilets
Maja Dos Santos
Pierre Lepage
Frédéric Matte
Karim Nanji
Phil Rivard
Anandhi Sarvananthan

L'Institut canadien des actuaires (ICA) est l'organisme bilingue national et le porte-parole de la profession actuarielle au Canada. Nos membres se vouent à fournir des services et des conseils actuariels de la plus haute qualité. L'Institut fait passer l'intérêt du public avant les besoins de la profession et de ses membres.

Les actuaires sont des experts en gestion du risque. Ils utilisent leurs connaissances en mathématiques, en statistique et en probabilités afin d'aider à assurer la sécurité financière des Canadiens. Les domaines de pratique traditionnelle comprennent l'assurance-vie et les assurances IARD, les placements, les régimes de retraite et la gestion du risque d'entreprise.

Nous remercions les auteurs qui ont participé à la rédaction de ces articles.

Les opinions exprimées sont celles des auteurs.

Sources

Association canadienne de santé publique. 2018. <https://cpha.ca/sites/default/files/uploads/resources/cannabis/evidence-brief-addictive-e.pdf>

Aydelotte J.D., Brown L.H., Luftman K.M., Mardock A.L., Teixeira P.G.R., Coopwood B. et Brown C.V.R. « Crash fatality rates after recreational marijuana legalization in Washington and Colorado », dans *American Journal of Public Health*, août 2017, vol. 107, n° 8, pp. 1329–1331. <https://www.ncbi.nlm.nih.gov/pubmed/28640679>

Burrell, J. « How the machine “thinks”: Understanding opacity in machine learning algorithms », dans *Big Data & Society*, 2016, vol. 3, n° 1, n.p. <https://doi.org/10.1177/2053951715622512>

Clearfield C. et Tilcsik A. *MELTDOWN: Why Our Systems Fail and What We Can Do About It*, Toronto, Allen Lane, 2018.

Congrès américain. *Algorithmic Accountability Act*, 2019. www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf

Davey, L. *The Good Fight: Use Productive Conflict to Get Your Team and Organization Back on Track*, Vancouver, Page Two Books, 2019.

[Mandiant] FireEye Mandiant Services. *M-Trends 2019: FireEye Mandiant Services|Special Report*, FireEye, Milpitas, 2019. <https://content.fireeye.com/m-trends>

Meier M.H., Caspi A., Cerdá M., Hancox R.J., Harrington H., Houts R., Poulton R., Ramrakha S., Thomson W.M. et Moffitt T.E. « Associations between cannabis use and physical health problems in early midlife: A longitudinal comparison of persistent cannabis vs tobacco users », *JAMA Psychiatry*, 2016, vol. 73, n° 7, pp. 731–740. doi:10.1001/jamapsychiatry.2016.0637.

[NIDA] National Institute on Drug Abuse. « What is marijuana? », 2018. www.drugabuse.gov/publications/drugfacts/marijuana [Consulté en mai 2019.]

Statistique Canada. Centre de statistiques sur le cannabis, 2019a. <https://www150.statcan.gc.ca/n1/pub/13-610-x/cannabis-fra.htm> [Consulté en mai 2019.]

Statistique Canada. Prévalence de la consommation de cannabis au cours des trois derniers mois, auto-déclarée, 2019b, 13-10-0383-01. https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=1310038301&request_locale=fr [Consulté en mai 2019.]

Statistique Canada. Élaboration d’estimations historiques du volume de consommation de cannabis au Canada, 1960 à 2015, 2018, 11-633-X2018015. <https://www150.statcan.gc.ca/n1/fr/catalogue/11-633-X2018015>

Tefft B., Arnold L. et Grabowski J.G. « Prevalence of marijuana involvement in fatal crashes: Washington 2010–2014 », dans *AAA Foundation for Traffic Safety, Washington*, 2016. <https://aaafoundation.org/wp-content/uploads/2017/12/PrevalenceOfMarijuanaInvolvement.pdf>

Union européenne, Parlement et Conseil, *Règlement général sur la protection des données*, *Journal officiel de l’Union européenne*, L 119/1, le 4 mai 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC>

Zhang L.R., Morgenstern H., Greenland S., Chang S.C., Lazarus P., Teare M.D., Woll P.J., Orlov I., Cox B., Cannabis and Respiratory Disease Research Group of New Zealand, Brhane Y., Liu G. et Hung R.J. « Cannabis smoking and lung cancer risk: Pooled analysis in the International Lung Cancer Consortium », *Int J Cancer*, 2015, 136(4):894–903. <https://www.ncbi.nlm.nih.gov/pubmed/24947688>

Canadian
Institute of
Actuaries



Institut
canadien
des actuaires

cia-ica.ca