CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

La cybersécurité, une protection de l'intérieur vers l'extérieur

GUIDE PRATIQUE SUR LA PROTECTION DES DONNÉES ET LA GOUVERNANCE POUR PETITES ET MOYENNES ENTREPRISES (PME)

par Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC

Quel est le problème?
Ces dernières années, les changements économiques se sont accélérés à l'échelle mondiale, le rôle traditionnel du professionnel de la comptabilité évoluant au rythme des besoins nouveaux des organisations. Les entreprises canadiennes et les professionnels en exercice s'adaptent rapidement aux tendances qui découlent de la législation sur les données et la vie privée, des normes de cybersécurité et des transformations technologiques. Le CPA peut désormais saisir l'occasion sans précédent d'aider les entreprises et les organismes sans but lucratif (OSBL) de toutes tailles à tirer parti de ses capacités professionnelles. Ce faisant, le CPA devient un conseiller de confiance et un leader dans un monde constamment aux prises avec la tâche difficile d'évaluer et d'atténuer les risques.

Pourquoi est-ce important?
Tous les jours, on signale des atteintes à la protection des données et des incidents de piratage numérique. Qu'ils travaillent à domicile ou dans un environnement de bureau traditionnel, les utilisateurs professionnels sont maintenant habitués à s'attendre à des demandes frauduleuses, mais ne sont pas toujours en mesure de distinguer celles-ci des demandes légitimes. La situation contribue à sensibiliser les particuliers et les entreprises à l'importance de la protection des données. La réglementation en matière de signalement et de communication de l'information joue un rôle crucial dans la dénonciation de la collecte massive de données et de la négligence dans divers secteurs d'activité.

Que peut-on faire?
Les entreprises et les OSBL de toutes tailles font face à un problème qui constitue à la fois une occasion à saisir : renforcer leurs façons de faire en matière de cybersécurité et faire de la prévention, la détection et la réaction les phases clés d'une stratégie de gestion des risques adaptée aux réalités d'aujourd'hui.

En donnant des conseils sur les techniques d'atténuation des risques ou les mécanismes de transfert du risque, les CPA qui maîtrisent le langage de la gestion des risques liés à l'information peuvent saisir cette occasion pour accroître leur participation stratégique aux efforts de conformité aux normes et fournir une aide aux décisions opérationnelles.

Vue d'ensemble

Étant donné la faiblesse généralisée des investissements en cybersécurité, des maliciels sont utilisés pour voler des données, des utilisateurs sont aux prises avec des rançongiciels et des victimes de tous horizons sont piégées par des techniques de piratage psychologique. Selon Beazley Breach Response, 71 % des rançongiciels visent les PME.

Avec la « nouvelle normalité » amenée par la COVID-19, les organisations anticipent les cyberattaques, et jusqu'à 55 % d'entre elles avouent qu'elles paieraient une rançon si elles en arrivaient là (DarkReading, 2019). Une évolution sans précédent dans le monde des affaires, puisque l'on estime que 73 % des PME paient effectivement des extorqueurs pour récupérer l'accès à leurs données et systèmes tenus en otage par des rançongiciels (Infrascale, 2020).

Hier encore limité à la seule fonction comptable, le rôle du CPA évolue : celui-ci devient un conseiller et collaborateur de confiance ayant une vue directe sur les aspects financiers des entreprises et contribuant au contrôle diligent des fournisseurs et à la protection des actifs. Le risque lié à l'information est désormais une priorité pour les professionnels de la comptabilité. Le CPA est maintenant un pivot qui exerce une influence dans toute l'entreprise, étroitement lié aux rôles de conseillers comme les spécialistes des TI, les ressources humaines et les gestionnaires de projets.

Les lignes directrices qui suivent s'adressent aux CPA et aux professionnels en exercice des PME qui ont besoin d'un stratège en cybersécurité ayant une vision claire des finances et des activités. Elles illustrent la manière dont les PME établissent leur budget de cybersécurité, transfèrent les risques coûteux liés aux données au moyen de polices d'assurance et priorisent les contrôles technologiques clés pour une efficacité opérationnelle maximale.

Compte tenu du fait que les atteintes à la protection des données coûtent aux entreprises en moyenne 4 millions de dollars par incident (IBM, 2020), les organisations doivent revoir leur façon de prendre des décisions relatives à la cybersécurité et adopter une approche descendante, émanant de la direction, qui repose sur de judicieux conseils. Ces lignes directrices présentent donc des concepts qui sont de plus en plus pertinents pour votre profession et celle de vos parties prenantes.

Dans ce contexte, le traitement des risques, sans être compliqué, diffère grandement des approches précédentes – et nécessite donc le leadership et le savoir-faire d'un conseiller de confiance bien au fait des mobiles habituels des cybercriminels.

Incidence des tendances émergentes sur votre organisation

Des organismes faisant autorité s'efforcent de cerner l'évolution de la cybercriminalité, et les organisations en découvrent autant sur leur propre résilience que sur la gestion des risques. Comme, chez la plupart des organisations, la plus grande partie de la valeur se trouve dans leurs actifs incorporels (analyse des données, renseignements personnels, etc.) et puisque de nombreuses entreprises se tournent vers des environnements de travail à distance et décentralisés, nous constatons une confluence sans précédent de facteurs de risque. Les enjeux sont considérables pour les entreprises, grandes et petites, dont les risques existentiels sont liés non seulement à leur propre sécurité, mais à celle de la chaîne d'approvisionnement. Par conséquent, le rôle du CPA englobe maintenant ceux de conseiller, de gardien des finances et de technologue, et la profession continue à s'adapter à un contexte où les conseils d'experts sont de plus en plus demandés.

Il est largement admis que les atteintes liées à la cybersécurité ont une forte incidence économique et constituent une menace pour la sécurité nationale. Notons que 90 % des entreprises canadiennes ont subi au moins une violation de données en 2018 (Cision Canada, 2018). L'augmentation des volumes d'informations et la faible maturité à l'égard de la gestion des risques exposent les PME à des pertes financières, à des poursuites en responsabilité et à des dommages causés à la valeur de leur marque. Qui plus est, la moitié des petites entreprises qui subissent de graves atteintes à la sécurité de leurs données cessent leurs activités dans les six mois qui suivent (Cybercrime Magazine, 2019).

Les professionnels de la comptabilité doivent être conscients des six facteurs de risque fondamentaux suivants, qui ont une incidence sur les activités des entreprises; trois sont externes, et les trois autres, internes :

À l'externe :

- modifications législatives
- innovations technologiques
- nouveaux risques liés à la cybersécurité

À l'interne, la nécessité de développer les éléments suivants :

- résilience (face aux risques d'entreprise et aux cyberrisques)
- adaptabilité (en particulier aux facteurs externes)
- esprit d'innovation (nécessité de demeurer concurrentiel grâce à une transformation et à un progrès continus)

Il existe une forme d'hameçonnage qui a connu une augmentation de 100 % d'année en année depuis 2017 : il s'agit de la « fraude du président ». On estime aujourd'hui que près de la moitié de toutes les fraudes de ce type font intervenir des maliciels (Standard Chartered, 2020) entraînant des fraudes électroniques. Quant aux violations de données et au vol d'appareils, ils représentent encore plus de 70 % des pertes de données (Shred-it et Institut Ponemon, 2020).

À la lumière des changements économiques, sociétaux et culturels importants, les conseillers professionnels et les professionnels en exercice doivent voir à transformer la manière dont les organisations sont soutenues, depuis la définition de politiques et de procédures appropriées jusqu'à la mise en œuvre d'une gouvernance stratégique qui détermine quelles données les organisations doivent recueillir et traiter. À mesure que la protection de la vie privée et la gouvernance des risques deviennent des domaines de pratique bien développés au sein des organisations, il est nécessaire de relever un nouveau défi : équilibrer les risques opérationnels avec les investissements financiers nécessaires pour atténuer ou transférer ces risques.

Les atteintes à la protection des données ne sont pas seulement causées par des attaquants malveillants. Selon le Commissariat à la protection de la vie privée du Canada (2019), près du quart d'entre elles sont accidentelles, dues à une erreur humaine plutôt qu'à la malveillance. Ces statistiques font ressortir le danger évident des menaces actuelles en matière de cybersécurité. Il y a quelques années à peine, le grand public était considéré comme mal équipé pour faire face aux nouvelles concernant les violations de données ou pour conceptualiser les conséquences d'une usurpation d'identité issue d'un vol de renseignements personnels découlant d'une atteinte à la protection des données.

Aujourd'hui, la loi, de plus en plus stricte, oblige les entreprises à assumer la responsabilité des informations dont elles ne sont pas propriétaires, et les médias ne cessent de signaler les défaillances en matière de sécurité. Les organisations faisant autorité publient des conseils facilement applicables qui s'attaquent au cœur des problèmes et catalysent l'amélioration continue. Les présentes lignes directrices mettent les pratiques de sécurité en contexte et proposent aux professionnels et aux organisations un langage commun à adopter pour résoudre les problèmes de sécurité, de protection des renseignements personnels et de conformité.

En ce moment, peu d'organisations sont en mesure de prévenir les atteintes à la sécurité et d'y répondre correctement. Les CPA peuvent maintenant guider leurs clients au moyen d'un modèle de maturité en matière de gestion des risques grâce à leur connaissance multidimensionnelle des facteurs et des objectifs financiers de la cybercriminalité. Par ailleurs, une approche structurée de la conception des contrôles et la capacité à présenter de manière concise les informations les plus importantes dépendent de grandes tendances observées à l'échelle tant nationale que mondiale. Voici quelques-unes de ces informations :

- Selon nombre d'experts, la prochaine récession pourrait être le fruit d'une cyberattaque (Business.com, 2019).
- D'ici 2020, 60 % des entreprises numériques subiront des interruptions de service majeures qui pourraient avoir des conséquences à l'échelle mondiale (CIO, 2018).

La stabilité opérationnelle d'une entreprise dépend largement de sa gestion financière. Le savoir-faire des professionnels de la comptabilité est donc essentiel à la résilience, à l'adaptabilité et à l'innovation nécessaires pour en assurer non seulement la continuité des activités, mais aussi la croissance soutenue et contrôlée.

Le statu quo en matière de gestion des risques est un exercice théorique régi par des notions abstraites et des équations complexes. Toutefois, comme nous allons le démontrer, pour améliorer l'efficacité de la prévention des risques et de la réponse à ceux-ci, il faut donner aux employés des renseignements, des exemples, des listes de contrôle et des autoévaluations qui permettent d'agir, ainsi qu'un aperçu des résultats de ces initiatives internes afin de s'assurer que chacun est en phase avec les objectifs de l'organisation et le niveau de protection contre les risques de celle-ci. Nous présenterons de nouveaux termes tels que « sécurité opérationnelle » (SECOP) pour illustrer l'importance de ces concepts dans les activités quotidiennes. La responsabilisation de chacun au sein de l'entreprise crée un « pare-feu humain » ou un « réseau de confiance » qui sert à accroître progressivement la sensibilisation et la résilience face aux risques.

Introduction au sujet : fonctionnement de la cybersécurité dans les entreprises

Dans les faits, la cybersécurité repose sur trois piliers : la sécurité informatique, la sécurité administrative et la sécurité physique. Il faut absolument connaître ces éléments fondamentaux pour comprendre comment mettre en place une entreprise résiliente et durable.

Vus sous cet angle, les atteintes à la protection des données et les incidents de cybersécurité signalés sont des situations évitables que les organisations de toutes tailles peuvent gérer. Dans les trois exemples suivants, nous examinons des situations réelles pour comprendre ce qui provoque les cyberincidents et pourquoi chaque atteinte à la protection des données est évitable.

Contrôles et mesures de protection

Les contrôles de sécurité se répartissent en trois catégories, ou piliers.

DIX EXEMPLES DE CONTRÔLES DE CYBERSÉCURITÉ POUR CHAQUE PILIER FONDAMENTAL

Sécurité informatique	Sécurité administrative	Sécurité physique
• Sauvegardes chiffrées • Pare-feu de réseau • Filtres antivirus • Systèmes de détection d'intrusion • Mots de passe de connexion • Authentification multifactorielle • Vérification de l'intégrité des données • Courriels chiffrés • Anti-rançongiciels • Analyse et tests de sécurité	• Formation du personnel • Politiques de sécurité de l'information • Politiques de protection des renseignements personnels • Politiques relatives aux données et aux mots de passe • Programme de gestion des correctifs • Réunions de l'équipe de sécurité • Classification des données • Inventaires des actifs informationnels • Planification de la continuité des activités • Processus de gestion des incidents et des violations de données	• Filtres de confidentialité pour moniteurs • Clés USB chiffrées • Câbles et serrures Kensington • Boîtiers inviolables • Surveillance par caméra en circuit fermé • Cartes d'accès • Zones de sécurité physique • Badges et registres des visiteurs • Détecteurs de mouvement • Accès biométrique

Cet ensemble diversifié de contrôles de sécurité représente les principaux facteurs de changement interne, depuis les politiques liées à la sécurité jusqu'à la couverture d'assurance, en passant par l'importance accordée au concept de GRC (gouvernance, gestion des risques et conformité).

Comprendre les trois types de contrôles de cybersécurité

Lorsqu'elle s'attaque à la cybersécurité, chaque organisation doit trouver un équilibre entre les objectifs de gestion des risques et les ressources disponibles pour protéger les actifs existants. Ces ressources doivent naturellement être affectées en priorité à la prévention des incidents de sécurité. Cependant, dans un grand nombre de cas, les statistiques montrent que les organisations prennent plus de 200 jours à détecter qu'elles ont été victimes d'une atteinte à la sécurité des données. C'est pourquoi il faut souligner que, outre la prévention, une bonne stratégie de sécurité repose également sur la surveillance et l'audit. Une fois détecté, un incident nécessite une réponse rapide et adéquate : il faut mettre en œuvre des contrôles correctifs afin que des mesures soient prises pour traiter les violations de données le plus rapidement possible. Ensemble, les mesures de prévention, de détection et de correction constituent l'essentiel de la stratégie de gestion des risques de toute organisation.

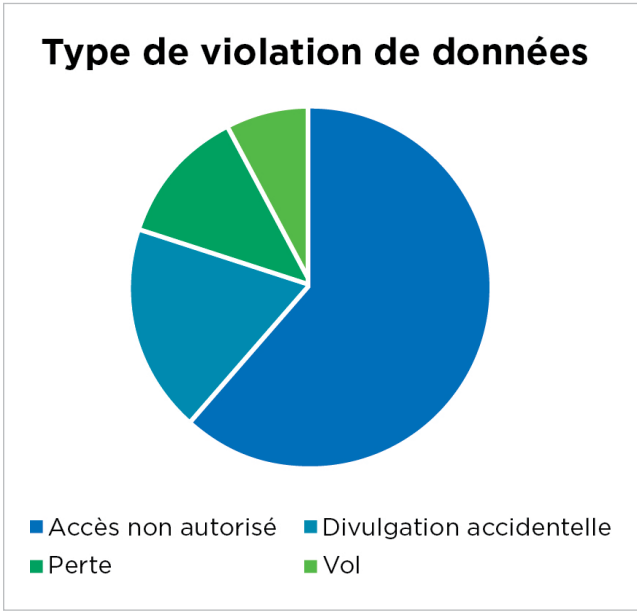
Prévention : L'accent est mis sur l'atténuation du risque qu'une vulnérabilité puisse être exploitée.

Détection : Découverte et suivi de la progression d'un incident de sécurité, et activités connexes qui s'y rattachent.

Correction : Série de mesures qui diminuent la gravité et les incidences d'un événement après qu'un incident s'est produit.

Établir la nécessité d'aller au-delà de la simple prévention

Le 1er novembre 2018, de nouvelles dispositions sont venues renforcer la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), obligeant les entreprises à surveiller et à détecter les violations des données, à les signaler si elles sont importantes et à informer les victimes s'il existe un risque de préjudice grave pour les personnes concernées.



Un an après l'entrée en vigueur de ces dispositions, le nombre d'atteintes à la protection des données signalées avait considérablement augmenté, ce qui indique qu'en l'absence de contrôles de détection, ces atteintes n'étaient tout simplement pas relevées.

- En novembre 2019, 680 rapports de violation de données avaient été déposés, soit six fois plus que l'année précédente. Le Commissariat à la protection de la vie privée a qualifié cette augmentation de révélatrice et de stupéfiante.
- En 2019, les atteintes à la protection des données ont touché 28 millions de Canadiens. Du nombre, mentionnons la violation de données à Equifax, mais aussi celles chez Desjardins et Capital One.
- Cinquante-huit pour cent des violations de données ont découlé d'un accès non autorisé, ce qui dénote une intention malveillante et indique la proportion de violations dues à des mesures de protection inadéquates et des motivations financières.

La valeur des CPA

Les professionnels en exercice ont désormais la possibilité de contribuer aux décisions stratégiques et opérationnelles dans le cadre de diverses situations, notamment comme :

- conseillers en matière de risques, assurant un leadership en résilience axé sur les contrôles internes et les processus clés;

- agents ou gestionnaires de changement, offrant un soutien en matière de formation, de réponse aux incidents et d'adaptation aux six facteurs de risque fondamentaux;
- innovateurs, en assurant une surveillance et une orientation stratégiques pour mener une transformation progressive (et rentable) de l'entreprise.

Concrètement, les CPA peuvent appliquer une vision judicieuse au défi du déploiement de solutions de cybersécurité en fonction des ressources disponibles.

Par exemple, supposons qu'une organisation a effectué une évaluation des risques ou un examen de la sécurité. Les résultats de cette activité ont été résumés simplement sous forme de recommandations concernant :

- l'élaboration d'un plan de réponse pour gérer les incidents de cybersécurité;
- la mise en œuvre d'un système de gestion des informations et des incidents de sécurité;
- la mise à jour automatique des logiciels et du matériel (le cas échéant);
- la configuration et l'activation de pare-feu, d'antivirus et d'antimaliciels à jour;
- la mise en œuvre de l'authentification à deux facteurs;
- l'élaboration de politiques concernant les mots de passe;
- la sensibilisation des employés afin de réduire au minimum les erreurs humaines;
- la sauvegarde et le chiffrement des données;
- la mise en place de défenses périmétriques appropriées, comme des pare-feu;
- la mise en œuvre du principe du « droit d'accès minimal » en ne fournissant aux utilisateurs que les fonctionnalités minimales dont ils ont besoin pour s'acquitter de leurs fonctions;
- l'utilisation d'une approche simple basée sur des listes de contrôle pour parvenir à une gestion des risques complète et évolutive qui s'applique aussi bien aux petites entreprises qu'aux organismes sans but lucratif et aux grandes organisations.

La direction se trouve alors dans une situation où elle doit décider comment allouer les maigres ressources de l'organisation à ses activités générales. Comment prioriser ces activités? Qu'est-ce qui est urgent? Qui peut être chargé de gérer ces activités?

C'est là que le CPA joue son rôle de conseiller; son point de vue sur les risques et son savoir-faire en matière de contrôles de sécurité lui permettent de bien cerner ce qui doit être fait, et le bon moment pour le faire. L'approche qu'il préconise peut être résumée dans le tableau suivant :

Priorité	Activité	Catégorie	Type
1	Activer une défense de périmètre	Physique/ Informatique	Prévenir
2	Configurer les appareils et les systèmes de manière sécuritaire	Informatique	Tous

Priorité	Activité	Catégorie	Type
3	Activer les mises à jour automatiques	Informatique	Prévenir
4	Élaborer des politiques	Administrative	Tous
5	Mettre en place des contrôles d'accès robustes	Informatique	Prévenir
6	Limiter les privilèges des utilisateurs	Informatique	Prévenir
7	Former le personnel	Administrative	Tous
8	Adopter un système d'information sur la sécurité	Informatique/ Administrative	Surveiller
9	Mettre en œuvre des procédures de réponse aux incidents	Administrative	Répondre
10	Sauvegarder les données de manière sécuritaire et tester régulièrement les sauvegardes	Physique	Répondre

L'essentiel, ici, est que les CPA montrent que la grande majorité des mesures de protection doivent porter non seulement sur les incidents de sécurité, mais aussi sur leur prévention. Si au moins trois des contrôles ci-dessus sont adoptés, il est possible de démontrer la plus-value d'une activité, chacune servant à prévenir, à détecter et à corriger les cyberincidents (ou à y répondre).

La capacité des CPA à conseiller, à transmettre des connaissances et à faire preuve d'un leadership intellectuel est renforcée par ces approches simples de planification et de mise en œuvre de la gestion des risques.

Relever le défi

L'atteinte des objectifs n'a jamais autant dépendu des capacités des professionnels de la comptabilité et des CPA. Leurs compétences et leurs valeurs se prêtent parfaitement à la tâche consistant à comprendre les incidences des risques et à déterminer les voies du succès. Les professionnels en exercice occupant des postes autres (p. ex., directeurs financiers, employés des services comptables) peuvent se voir accorder suffisamment d'autorité et de privilèges d'accès pour saisir des occasions d'affaires, établir des partenariats rentables et atténuer les risques tout en soutenant les priorités de l'organisation.

Les tendances en matière de cybersécurité varient d'une année à l'autre, mais il est important pour les conseillers de confiance de se tenir au courant de ces changements, de synthétiser les informations et de les transmettre aux parties prenantes. Par exemple, les événements actuels montrent que les criminels s'appuient essentiellement sur trois activités lorsqu'ils commettent la grande majorité des atteintes à la protection des données :

1. Infections par rançongiciels et maliciels;
2. Piratage psychologique et arnaques de type « fraude du président »;
3. Vol de données en accédant aux systèmes.

Par conséquent, les CPA doivent non seulement connaître les stratégies appropriées d'atténuation des risques, mais aussi être capables d'expliquer clairement les principales approches pour gérer chaque type de problème :

1. Infections par rançongiciels et maliciels
   a) gestion des correctifs
   b) sauvegardes de données sécurisées
   c) politiques de sécurité de l'information (y compris la gestion des violations de données)
   d) professionnels qualifiés de la sécurité informatique dans l'équipe
   e) formation de sensibilisation des employés à la sécurité
2. Piratage psychologique et arnaques de type « fraude du président »
   a) souscription d'une police de cyberassurance
   b) sécurisation des configurations et « durcissement » des systèmes
   c) formation des employés en fonction de leur rôle
   d) partage de données sécurisé
   e) pratiques sûres de gestion des mots de passe
3. Vol de données en accédant aux systèmes
   a) standardisation généralisée des contrôles
   b) audits de la sécurité physique
   c) transfert des risques
   d) chiffrement des données
   e) planification de la continuité des activités et reprise après sinistre

De nos jours, le professionnel de la comptabilité doit être un bon communicateur et un bon formateur, capable de transmettre et de bien faire comprendre les informations relatives aux risques au sein de l'organisation. Le CPA doit également être un initiateur et un catalyseur : il doit lancer des activités conçues pour « donner le coup d'envoi » et donner aux autres membres de l'équipe les moyens de poursuivre des objectifs communs. La sécurité de l'information et la gestion des risques constituent une partie fondamentale des activités des entreprises. L'efficacité de tout programme de cybersécurité repose grandement sur la réactivité, l'accessibilité et la capacité à soutenir les décisions de gestion avec des ressources alignées sur les normes actuelles. Le cycle de confiance que le professionnel en exercice doit instaurer se définit par la

capacité à répondre rapidement aux demandes de ses pairs et de la direction, ainsi qu'aux incidents et événements imprévus.

Surtout, le professionnel en exercice doit être un joueur d'équipe. Les présentes lignes directrices fournissent l'approche pratique pour transformer l'organisation de l'intérieur tout en faisant évoluer le professionnel en exercice d'un rôle d'expert à celui de membre de confiance de l'équipe-conseil. Les concepts de gouvernance des risques présentés ici concernent les chemins critiques fondamentaux des opérations liées aux données, de l'évaluation des données et des politiques connexes, en mettant l'accent sur le respect continu des obligations de protection des renseignements personnels.

Processus

On peut classer les processus internes liés aux risques en cinq catégories, que nous appellerons les « cinq domaines d'influence du CPA ». Les présentes lignes directrices proposent des activités basées sur des listes de contrôle concernant ces cinq domaines. Cliquez sur chacune des étapes ci-dessous pour en savoir plus.

Étape 1 : Gestion des risques

Étape 2 : Contrôles de cybersécurité

Étape 3 : Gouvernance

Étape 4 : Conformité

Étape 5 : Résilience et durabilité

En appliquant des mesures concrètes pour assurer la durabilité de la cybersécurité, on peut appliquer des mesures standardisées pour les cinq domaines d'influence du CPA.

Mise en œuvre au sein de votre organisation

Les listes de contrôle standardisées pour la durabilité de la cybersécurité peuvent être adaptées à un certain nombre de méthodes d'évaluation des risques, depuis le tout nouveau cadre CyberSécuritaire Canada jusqu'aux normes établies PCI DSS et NIST (National Institute of Standards and Technology), largement accessibles, qui jouissent d'une grande applicabilité à tous les secteurs d'activité. Les orientations régulièrement mises à jour de l'AICPA dans le domaine des services Trust englobent les contrôles et les politiques des organisations de services. Il est donc important de voir comment les cinq domaines d'influence s'adaptent aux besoins des organisations de différentes tailles.

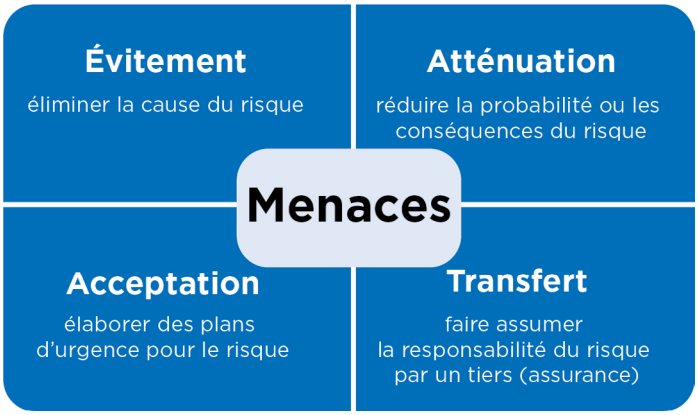


Illustration des quatre différentes options de traitement des risques selon le modèle PMBOK.

Étape 1

Gestion des risques

Étant donné que les opérations financières portent directement sur des actifs incorporels, la cybersécurité revêt une importance croissante dans la profession comptable, car elle permet de faire face aux risques liés à des situations auparavant imprévisibles et de protéger les activités des entreprises. En tirant parti de la gestion des risques, de la gouvernance et de la planification stratégique, les principales pratiques de cybersécurité présentées ci-dessous aideront les professionnels en exercice à « donner le ton » pour atteindre les objectifs des entreprises en matière de résilience, d'adaptabilité et d'innovation et ainsi assurer la durabilité de celles-ci.

Pour gérer correctement les risques auxquels font face les PME, les CPA doivent d'abord suivre ce processus de clarification des risques en trois étapes :

1. Déterminer la valeur des actifs informationnels.
2. Déterminer les incidences financières en cas de perte de ces actifs.
3. Établir la nécessité de contrôles efficaces pour atténuer le risque au minimum.

Comme c'est le cas du côté de la médecine et des sciences de la vie, les professionnels de la comptabilité doivent comprendre les quatre options suivantes de traitement des risques (résumées dans le diagramme ci-contre) et s'efforcer d'être aussi précis que possible dans leurs conseils aux clients. Une fois cernées, les menaces présentent un certain potentiel de

dommages. Pour prévenir ou atténuer ce risque, les entreprises ont la possibilité de l'accepter, de l'atténuer, de le transférer ou de l'éviter purement et simplement.

Option 1 : Éviter les risques (en cas d'exposition démesurée)

En leur qualité de conseillers, les CPA doivent recommander d'éviter les activités qui comportent un risque excessif ou important pour l'organisation, ou d'y mettre fin.

L'attribution de cotes de risque aux activités aide les organisations à déterminer où se situent ces activités sur l'éventail des risques. Le calcul de la cote de risque se fait comme suit :

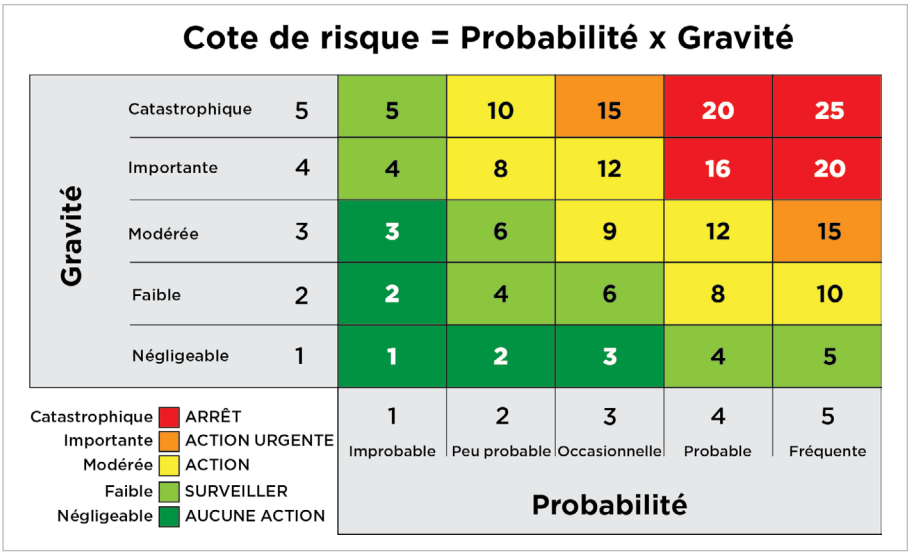
Probabilité du risque (**R**) = Probabilité (**C**) (c.-à-d. la probabilité d'un événement perturbateur)
multipliée par
Gravité (**I**) (c.-à-d. la perte résultant de l'événement).

Ainsi, le **r**isque est déterminé par l'**i**ncidence d'un événement indésirable multipliée par les **c**hances que celui-ci se produise.

Les présentes lignes directrices recommandent d'éviter les situations où un résultat préjudiciable est susceptible de se produire avec une fréquence élevée.

Option 2 : Accepter les risques (pour les résultats mineurs)

Les risques calculés peuvent être assumés ou acceptés, pour autant qu'ils soient bien compris et qu'une décision claire ait été prise d'aller de l'avant. Comme en témoignent de nombreux titres de journaux, la plupart des organisations omettent de déceler et de consigner les risques avant de les accepter. Ne pas évaluer ni gérer correctement les risques peut mettre l'organisation et les personnes concernées[1] en danger.



Rouge signifie Éviter; Vert signifie Accepter le risque. Le risque vert pâle et jaune doit être atténué autant que possible, le risque résiduel étant transféré à un souscripteur d'assurance au moyen d'une police de cyberresponsabilité adaptée à l'entreprise et approuvée par la direction.

1 Les personnes concernées désignent toutes les personnes qui peuvent être identifiées, directement ou indirectement, par un identifiant tel que leur nom, leur numéro d'identification ou des données de localisation, ou par des facteurs propres à leur identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale.

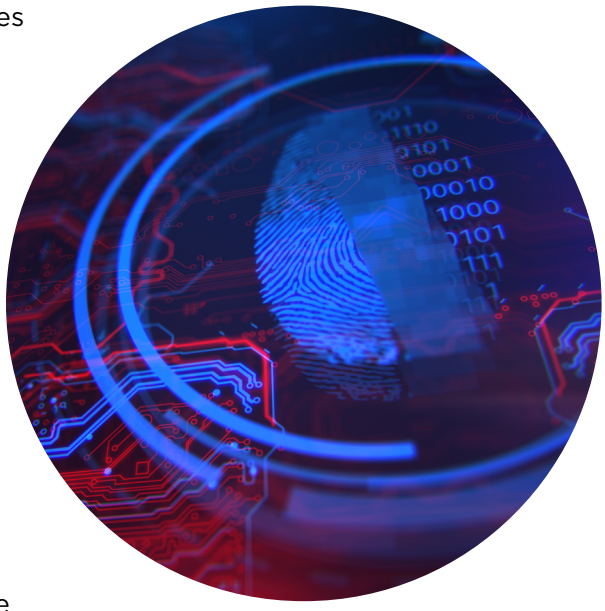
Qu'est-ce qui pourrait mal tourner? Une mauvaise évaluation des risques, un inventaire incomplet des données ou simplement des mesures de sécurité inadéquates peuvent mettre en péril la situation de l'entreprise sur le plan de la cybersécurité et de la conformité.

Un faux sentiment de sécurité peut alors venir saper les mesures de protection en place et causer des dommages durables. Malheureusement, cette situation est courante dans les organisations de toutes tailles. À titre d'exemple de violation de données évitable, les incidents impliquant des rançongiciels ont augmenté de 56 % au cours de chacun des quatre derniers trimestres (365 Technologies Inc., 2019), signe que les organisations n'ont pas mis en place de mesures de protection préventives, s'exposant ainsi à des incidents aux conséquences potentiellement désastreuses.

Option 3 : Atténuer les risques

Il s'agit de l'option la mieux comprise, comme en témoigne le passage dans l'usage des termes qui lui sont propres, comme « pare-feu », « antivirus » et « mot de passe ». Ces différentes méthodes d'application de la politique de sécurité servent à atténuer les risques spécifiques et généraux. Le fait que ces mesures soient suffisantes est souvent mis en doute lorsque les organisations ne parviennent pas à déterminer correctement les risques à l'aide d'une évaluation des menaces et des risques, ce qui entraîne une exposition inattendue ou des mesures de protection inadéquates. Les entreprises peuvent alors souffrir d'un faux sentiment de sécurité, croyant qu'elles ont pris des mesures suffisantes, voire excessives, pour protéger leurs actifs alors qu'en fait, des lacunes importantes peuvent subsister.

Pour réduire la probabilité de tels résultats, les organisations classifient des scénarios de menace distincts et élaborent des processus de traitement des risques pour la prévention, la détection et la correction des résultats indésirables. Ces approches entraînent alors des mesures de protection ou des déclencheurs d'actions à mener dans le cadre de la pratique opérationnelle.



Les contrôles sont des notions abstraites de mesures de protection appliquées par couches pour assurer la protection contre toute manipulation non autorisée. Nous savons que les contrôles tels que les antivirus, les pare-feu et surtout les serrures de porte sont les cibles préférées des attaquants malveillants. En enveloppant les objets de valeur dans ces couches de protection, les PME peuvent arrêter les attaques ou du moins, les ralentir assez longtemps pour qu'une équipe de réponse aux incidents puisse intervenir. Cette « défense en profondeur » constitue un aspect clé des cadres et des mesures de conformité, traditionnellement appelés « pratiques exemplaires ».

Option 4 : Transférer les risques

Il s'agit de la pratique consistant à identifier le risque résiduel après que toutes les autres options de traitement ont été épuisées. En présentant de façon adéquate aux décideurs le risque résiduel et la responsabilité, les CPA et les conseillers de confiance peuvent leur donner les moyens de prendre la bonne décision en transférant littéralement le risque résiduel à un tiers, généralement une compagnie d'assurance, qui assumera le risque au moyen d'une assurance cyberresponsabilité. En aidant quantitativement les organisations à effectuer des calculs de risques et à mener des évaluations de risques standardisées, les professionnels en exercice peuvent contribuer à la création d'un registre des risques, qui est une liste des risques associés à l'entreprise et des expositions à ces risques.

Par exemple, imaginons une organisation qui a appliqué plusieurs couches de contrôles pour protéger ses données de l'intérieur vers l'extérieur, c.-à-d. depuis les mécanismes de stockage interne jusqu'à la vérification des mesures de protection appliquées par ses fournisseurs de services. Une telle entreprise est bien placée pour présenter au conseil d'administration une image claire de l'assurance en matière de cybersécurité, où les risques sont atténués de manière contrôlée. Toutefois, après avoir effectué une évaluation des menaces et des risques et un exercice de test de pénétration, l'organisation a déterminé que les aspects suivants constituent une exposition continue et peuvent présenter des vulnérabilités, si un pirate motivé persistait à vouloir relever le défi :

1. Les correctifs et les mises à jour ne peuvent pas être appliqués aux systèmes et aux dispositifs dès leur sortie, car les pratiques exemplaires préconisent de les tester pour éviter qu'ils ne nuisent à la stabilité des activités de l'organisation. Cette opération prend du temps, et ce délai représente un risque pour la posture de sécurité de l'organisation. Pendant ce temps, un appareil ou une application sans correctif peut faire l'objet d'une attaque par un maliciel conçu pour rechercher les mises à jour manquantes de logiciels ou de micrologiciels et exploiter cette vulnérabilité pour accéder aux précieux actifs informationnels en question.
2. Tandis que les employés peuvent avoir été formés à la cybersécurité et continuer à recevoir des formations de remise à niveau tous les ans, certains utilisateurs peuvent avoir plus de privilèges d'accès que nécessaire. Si des pirates devaient détourner des comptes ou usurper l'identité d'utilisateurs, ils auraient les mêmes droits d'accès à l'organisation que les utilisateurs légitimes. En appliquant le principe du « besoin de savoir », l'organisation peut limiter les conséquences des violations de données au niveau d'accès accordé à chaque utilisateur. Autrement dit, indépendamment du fait que les utilisateurs soient formés et vigilants, si les contrôles d'accès se limitent à l'utilisation du secret (c.-à-d. seulement un mot de passe) par opposition à une deuxième couche d'authentification telle qu'un code ou un message texte – appelée « authentification à deux facteurs » –, le potentiel de prise de contrôle des comptes est toujours plus important.
3. Une erreur de l'utilisateur expose les organisations à des cyberattaques préméditées et opportunistes. Le risque de tels événements dépend de nombreux facteurs qui sont difficiles à limiter et à contrôler, notamment le nombre d'appareils portables ayant accès

aux données, le nombre de méthodes d'accès, les accès accordés aux utilisateurs externes ayant un accès physique aux locaux, et même le nombre de portes d'entrée et de sortie.

Non seulement de tels scénarios sont faciles à illustrer, mais ils peuvent également être présentés à la direction par des conseillers de confiance qui peuvent souligner la nécessité d'avoir des polices d'assurance cyberresponsabilité. Cette couverture est maintenant largement disponible, et de nombreuses petites et moyennes organisations souscrivent des polices chaque jour.

Selon Statistique Canada, en 2019, près du quart (24 %) des grandes entreprises ont indiqué qu'elles disposaient d'une assurance cyberresponsabilité pour se protéger contre les risques et les menaces liés à la cybersécurité, par rapport à 14 % des moyennes entreprises et à 7 % des petites entreprises. Lorsque le Bureau d'assurance du Canada a interrogé 300 propriétaires de PME, 60 % ont déclaré qu'ils n'étaient pas assurés, 21 % ont dit qu'ils étaient assurés et 19 % ne savaient pas (Canadian Underwriter, 2019).

En fait, lorsqu'on a demandé aux propriétaires s'ils avaient déjà envisagé de souscrire une cyberassurance pour leur entreprise, 62 % ont répondu que non. Sur l'ensemble des répondants, un peu plus de la moitié n'avaient pas l'intention de souscrire une police au cours de la prochaine année. À la question visant à établir pourquoi il y avait des risques non atténués et des pertes perturbatrices, les répondants ont indiqué que c'était en partie parce qu'ils ne comprenaient pas l'assurance cyberresponsabilité. Voilà qui fait ressortir l'importance des professionnels de la comptabilité dans des rôles de conseillers de confiance, capables d'expliquer les options de transfert des risques à la direction.

Étape 2

Contrôles de cybersécurité

Précédemment dans le présent document d'information, nous avons discuté de la nécessité de mettre en place des protections complémentaires pour combler les lacunes dans la couverture. Le CPA avisé recherchera des images efficaces et des métaphores utiles (p. ex., l'œuf à coquille dure avec un centre mou représentant la sécurité par couches) pour expliquer à la direction la façon uniforme dont les contrôles doivent être déployés.

De plus, les organisations répartissent instinctivement leurs mesures de protection entre mesures physiques (p. ex., serrures sur les portes), mesures technologiques (p. ex., antivirus et pare-feu) et mesures administratives (p. ex., politiques, procédures, documents de formation). En trouvant un équilibre entre ces trois piliers de la cybersécurité, les entreprises sont en mesure de compartimenter leurs efforts et de prévoir une enveloppe protectrice évolutive, durable et résistante.

La défense en profondeur est donc un moyen efficace d'intégrer la résilience dans l'enveloppe protectrice d'une entreprise. Mais comment les organisations peuvent-elles parvenir à la sécurité sans chevauchements inutiles et inefficaces? L'une des meilleures méthodes standardisées est le cadre de cybersécurité du NIST, dont les cinq principaux domaines fonctionnels sont subdivisés en 23 catégories et 108 objectifs et résultats de contrôle réels. Cette approche visuelle aide les organisations à comprendre la cybersécurité et à établir la correspondance entre leurs

politiques, procédures et priorités de conformité d'une part et, d'autre part, l'élaboration d'un programme évolutif de gestion des risques (selon la taille de l'entreprise).

Identifiant de la fonction	Fonction	Identifiant de la catégorie	Catégorie
ID	**Identifier**	ID.AM	Gestion des actifs
		ID.BE	Environnement de l'entreprise
		ID.GV	Gouvernance
		ID.RA	Évaluation des risques
		ID.RM	Stratégie de gestion des risques
		ID.SC	Gestion des risques liés à la chaîne d'approvisionnement
PR	**Protéger**	PR.AC	Gestion des identités et contrôle des accès
		PR.AT	Sensibilisation et formation
		PR.DS	Sécurité des données
		PR.IP	Processus et procédures de protection de l'information
		PR.MA	Maintenance
		PR.PT	Technologie de protection
DE	**Détecter**	DE.AE	Anomalies et événements
		DE.CM	Surveillance continue de la sécurité
		DE.DP	Processus de détection
RS	**Répondre**	RS.RP	Planification de la réponse
		RS.CO	Communications
		RS.AN	Analyse
		RS.MI	Atténuation
		RS.IM	Améliorations

Identifiant de la fonction	Fonction	Identifiant de la catégorie	Catégorie
RC	**Récupération**	RC.RP	Planification de la reprise
		RC.IM	Améliorations
		RC.CO	Communications

L'utilisation du cadre du NIST comme tableau de bord des contrôles permet aux organisations de simplifier la tâche de s'attaquer aux domaines à risque :

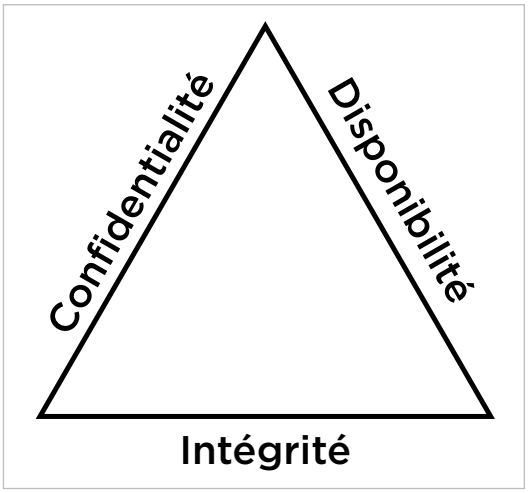
- Production d'un inventaire des actifs
- Classement des actifs par sensibilité et par valeur
- Création d'une liste de contrôle pour protéger ces actifs
- Élaboration de procédures permettant de rendre les contrôles efficaces
- Systématisation des processus de gestion et de suivi des contrôles et des procédures
- Imposition de l'utilisation de ces processus au moyen de politiques

Trouver le bon équilibre entre les contrôles de sécurité physique, les mesures de protection technologiques et la sécurité administrative est un bon moyen de combiner les couches de sécurité sans chevauchements inefficaces. Cette structure est illustrée plus en détail dans l'étude de cas qui accompagne les présentes lignes directrices, intitulée *La cybersécurité : une guerre de tranchées*.

Étape 3

Gouvernance

En fin de compte, la responsabilité de *faire ce qui convient au bon moment* repose sur les épaules de la direction. Il en découle que la surveillance constante de tous les risques est effectivement une responsabilité de gouvernance, bien qu'elle puisse être déléguée en fonction des domaines fonctionnels et opérationnels. L'équilibre entre la création de systèmes comportementaux et l'application de contraintes techniques rigides est une question d'imbrication de politiques complémentaires; là encore, un cadre de cybersécurité peut contribuer à concilier la nécessité d'équilibrer les risques avec les priorités de gouvernance que sont la conformité, la résilience, la croissance et la durabilité.



L'introduction de contrôles comportementaux et techniques par couches s'accompagne donc d'une liste de contrôle fonctionnelle qui établit une correspondance directe entre les catégories de contrôle et les politiques. Les PME devraient adopter des politiques de cybersécurité clés qui régissent :

- la sécurité des données et la protection des informations;
- la gestion des risques et des actifs;
- la gestion des incidents et les processus connexes (détection, réponse et signalement);
- la continuité des activités et la reprise après sinistre (à l'appui de la résilience).

Étape 4

Conformité

L'utilité d'un cadre de contrôle standardisé réside dans sa capacité à fournir une assurance aux parties prenantes internes et externes quant à l'adéquation des contrôles et des pratiques en matière de protection des actifs informationnels. Bon nombre de gestionnaires de risques professionnels ajustent minutieusement les contrôles très divers fournis par un tel cadre en fonction des exigences pratiques d'une organisation et des obligations de conformité aux normes et à la législation du secteur.

Il est possible que certaines législations (p. ex., les diverses lois canadiennes sur la protection des renseignements personnels) ne soient pas nécessairement normatives, mais les normes du secteur et les cadres d'audit tels que les services Trust de l'AICPA (et les exigences connexes des missions SOC 2) sont précisément conçus pour découvrir les menaces pesant sur les actifs informationnels, les opérations et la continuité des activités. En effet, les audits SOC 2 examinent les principes des services Trust en fonction des cinq critères de sécurité (c.-à-d. la sécurité, l'accessibilité, l'intégrité du traitement, la confidentialité et la protection des renseignements personnels). À cette fin, l'AICPA propose des documents de mise en correspondance, qui sont inclus dans la section « Ressources » à la fin du présent document. Les services Trust font directement « Ressources » aux trois objectifs de la sécurité de l'information : la confidentialité, l'intégrité et la disponibilité des données.

Étape 5

Résilience et durabilité

L'importance de la continuité des activités pour les PME est illustrée non seulement par le critère d'accessibilité des services Trust, mais aussi par la présence de la résilience au cœur de tout programme de gestion des risques.

Une organisation doit être imperméable aux menaces identifiées, mais doit également être résistante aux nouvelles menaces et aux risques imprévus. Pour bien aider les entreprises, les CPA doivent veiller à introduire les contrôles du cadre de cybersécurité du NIST ou leurs équivalents simplifiés dans le programme CyberSécuritaire Canada du gouvernement fédéral. Comme nous le disions plus haut, les contrôles de surveillance servent à détecter les violations de données et à anticiper les risques qu'il est possible d'atténuer ou de corriger grâce

à des mesures de protection efficaces. Par conséquent, la résilience protège les activités d'une organisation en aidant celle-ci à s'adapter aux menaces, existantes ou nouvelles, en tirant parti de la sensibilisation des employés et en mettant en œuvre des contrôles innovants.

Ce faisant, les professionnels des affaires et de la comptabilité peuvent utiliser la résilience, l'adaptabilité et les approches novatrices pour renforcer la cybersécurité à partir de l'intérieur des organisations. En adoptant des pratiques exemplaires standardisées, les organisations peuvent appliquer les éléments du RAID de CPA Canada, afin d'atteindre une croissance et des activités durables en contrôlant les risques pour les activités, les actifs informationnels et les ressources humaines.

Résumé

Comme l'a montré précédemment l'étude du Commissariat à la protection de la vie privée du Canada, les atteintes à la protection des données demeurent de toute évidence une menace constante pour toutes les organisations. Les entreprises doivent être conscientes de la multitude de risques potentiels et y faire face en combinant technologies, formations, politiques et processus.

Les tendances qui servent de moteur aux progrès économiques – innovation, fabrication, mondialisation – dépendent de plus en plus de l'utilisation des technologies pour optimiser la gestion financière. Grâce à sa compréhension des opérations et à son savoir-faire uniques, le CPA d'aujourd'hui est on ne peut mieux placé pour jouer un rôle de conseiller de confiance, d'influenceur stratégique et de visionnaire. Son rôle évolue pour répondre à la nécessité de satisfaire aux exigences de conformité à court terme, de concourir à la réalisation de la vision stratégique à moyen et à long terme, et de faire preuve de la flexibilité requise pour s'adapter aux forces du marché qui évoluent.

En tant que conseiller stratégique, le CPA doit développer et entretenir un savoir-faire en matière de gestion des risques, de gouvernance, de cybersécurité et de conformité. De plus, grâce à son rôle d'éducateur, il peut grandement contribuer à faire comprendre la protection des données et l'enjeu concret que constituent les risques pour les employés qui détiennent un rôle clé au sein de l'organisation (au moyen de ressources accessibles, d'autoévaluations et d'approches fondées sur des exemples au lieu de concepts abstraits et de modèles théoriques).

Ainsi, les professionnels en exercice avertis peuvent répondre aux besoins en constante évolution de leur entreprise et de leurs clients, en les conseillant sur la planification stratégique de la cybersécurité et en les aidant à réussir dans l'économie de la connaissance.

Les technologies ont pris une place centrale dans la relation basée sur la valeur entre le client et le conseiller, entre l'organisation et le professionnel en exercice. Les actifs incorporels sont désormais recueillis et conservés par des systèmes dont la sécurité a une incidence sur la conformité, la gouvernance et la rentabilité. La cybersécurité détermine la résilience, l'adaptabilité et la capacité de chaque organisation à rester à l'avant-plan de son secteur d'activité. Dans ce contexte, le CPA est une figure centrale de la prise de décisions stratégiques et opérationnelles opportunes qui déterminent la santé de l'organisation.

Ressources

Références

Business.com, Why Small Business Cyberattacks Could Prompt Next Recession (2019)

Canadian Underwriter, Brokers leaving a lot of SME cyber business on the table: Leger poll (2019)

CIO, By 2020, 60 percent of digital businesses will suffer major service interruptions (2018)

Cision Canada, 9 in 10 Canadian Companies suffered at least one cyber security breach last year (2018)

Cybercrime Magazine, 60 Percent Of Small Companies Close Within 6 Months Of Being Hacked (2019)

DarkReading, 55% of SMBs Would Pay Up Post-Ransomware Attack (2019)

IBM, How much would a data breach cost your business? (2020)

Infrascale, Infrascale Survey Reveals Close to Half of SMBs Have Been Ransomware Attack Targets (2020)

Commissariat à la protection de la vie privée du Canada, Un an après l'entrée en vigueur des déclarations obligatoires des atteintes à la protection des données : ce que nous avons appris et ce que les entreprises doivent savoir (2019)

Shred-it et Institut Ponemon, Sécurité des documents confidentiels en milieu de travail (2019)

Standard Chartered, The high cost of business email compromise (BEC) fraud (2020)

Statistique Canada, L'incidence du cybercrime sur les entreprises canadiennes (2017)

365 Technologies Inc., Ransomware stats and facts (2019)

Autres ressources

Aussi de Claudiu Popa :

- *Guide sur la protection des renseignements personnels et la sécurité des données au Canada* (1re et 2e éd., CPA Canada, 2015)
- *Managing Personal Information for Privacy-Savvy Organizations* (Carswell, 2012)
- *The Canadian Cyberfraud Handbook* (Thomson Reuters, 2017)
- *Tendance technologique : Cybersécurité et protection des données* (CPA Canada, 2019)

- *Tendance technologique : Protégez votre marque et votre réputation sur les médias sociaux* (CPA Canada, 2019)

Lectures complémentaires

- CPA Canada, *Lignes directrices sur la comptabilité de gestion – Pour passer des données aux décisions : Les cinq étapes du processus décisionnel fondé sur des données* (2021)
- AICPA, Controls Mapping Documents (2017)
- Industrie Canada, Le cadre de contrôle de CyberSécuritaire Canada (2021)
- NIST, Cybersecurity Framework (2020)
- Centre canadien pour la cybersécurité, En route vers la sécurité d'entreprise (2020)

À propos de l'auteur

Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC, est un professionnel agréé en sécurité de l'information et protection de la vie privée. Il traite dans les médias de questions comme la gestion des risques d'entreprise, la sécurité informatique et la protection des données. Fort de plus de 25 années d'expérience internationale dans les domaines de l'audit de sécurité, des normes internationales et des services-conseils en matière de risques auprès des conseils d'administration, M. Popa est un conseiller en gestion de confiance pour les entreprises canadiennes et leurs parties prenantes. Il soutient la mise en œuvre de stratégies liées à la sécurité, qui revêtent une importance cruciale, et la prise de décisions portant sur la conformité en matière de sécurité et de respect de la vie privée, la protection des données et la prévention de la cybercriminalité.

Il est l'auteur de quatre ouvrages, de nombreux articles et de multiples publications universitaires sur la protection de l'information, la conformité et la gouvernance des risques, fondés sur la recherche primaire en matière de cybersécurité. En tant que professionnel agréé, M. Popa demeure un ardent défenseur de la sécurité de l'information et un coach d'entreprise de confiance pour les organisations canadiennes qui sont déterminées à améliorer leur sécurité et la protection de leurs clients.