Deloitte.

Devenir un leader de la gestion des cyberrisques

Passer à une sécurité de niveau supérieur

Table des matières

Introduction

Tandis que le Canada prend le virage vers une économie basée sur les connaissances, la transformation numérique et l'utilisation des technologies exponentielles créent des occasions sans précédent pour les entreprises canadiennes. Mais chaque nouvelle occasion s'accompagne aussi de nouvelles menaces. Et dans un monde de bouleversements numériques, les cyberrisques constituent l'une des plus grandes menaces.

Les cyberrisques, qui représentent déjà un grand défi, augmentent de manière exponentielle. Selon un récent rapport, d'ici 2020, le monde devra se porter à la cyberdéfense de 50 fois plus de données qu'aujourd'hui[1]. Compte tenu des nouveaux risques qui se profilent chaque jour, les organisations doivent constamment mettre au point de nouvelles cyberstratégies et cyberdéfenses, alors que les pirates trouvent des façons de contourner les mesures de cybersécurité déjà en place.

1. Cybersecurity Ventures, 2016 Cybersecurity Market Report, http://cybersecurityventures.com/cybersecurity-market-report/ Consulté le 9 mai 2017.

Pour toutes les organisations, quelle que soit leur forme ou leur taille, la question n'est plus de savoir si elles seront la cible d'une attaque, mais plutôt *quand* elles le seront (et *comment*).

La révolution numérique bat son plein et il n'y a rien que vous puissiez – ou devriez – faire pour l'arrêter. Au cours des prochains mois et des prochaines années, les innovations numériques et les technologies exponentielles seront des moteurs clés de croissance et de réussite au Canada, et offriront à votre organisation des occasions sans précédent de créer de la valeur et d'acquérir un avantage concurrentiel.

Mais pour réussir dans ce nouveau monde numérique, il vous faut une stratégie de cybersécurité solide, qui augmentera la sécurité, la vigilance et la résilience de votre organisation. L'espoir n'est pas une stratégie.

Les cybercapacités ne doivent pas se borner à la gestion des menaces qui existent *aujourd'hui*. Les technologies exponentielles alimentent les perturbations numériques et ouvrent la voie à des cybermenaces d'un tout nouveau genre, en plus d'amplifier celles qui existent déjà. Aussi, les entreprises doivent commencer dès maintenant à élaborer des méthodes de *niveau supérieur*. Comme l'affirmait le père de Wayne Gretzky, il faut aller où la rondelle se trouvera, plutôt que là où elle se trouvait.

Les cyberrisques ne sont pas une question informatique. Il s'agit plutôt d'un enjeu d'affaires et d'un impératif stratégique. Les leaders de la gestion des risques et de la sécurité, ainsi que les chefs d'entreprise, doivent chercher constamment à comprendre les occasions et les risques associés à l'innovation numérique, puis parvenir à un équilibre entre le besoin de protéger leur organisation contre les cybermenaces et le besoin d'adopter de nouveaux modèles d'affaires et de nouvelles stratégies qui tirent parti des technologies numériques et préparent le terrain pour réussir.

Cela dit, si les perturbations numériques et la cybersécurité présentent des obstacles de taille, ces obstacles ne sont pas insurmontables. En sachant quelles mesures il faut prendre, et en ayant la prévoyance et le courage requis pour relever les défis, vous pouvez devenir maître de votre cyberavenir et devenir un agent perturbateur, plutôt que de laisser la concurrence vous perturber.

Le milieu changeant des cyberrisques

Dans le rapport de 2017 sur les risques mondiaux du Forum économique mondial[2], les cyberrisques sont reconnus comme l'un des risques commerciaux les plus importants avec les risques économiques, environnementaux et géopolitiques. Les technologies numériques et l'innovation connaissent une croissance exponentielle, ce qui accélère les cyberrisques, crée de nouveaux vecteurs d'attaque et élargit énormément la surface d'attaque que les organisations doivent surveiller et protéger.

Internet et la connectivité mobile jouent un rôle de plus en plus indispensable dans chaque aspect de notre vie, de notre travail et de nos activités, ouvrant ainsi la voie à d'innombrables possibilités de multiplier les cyberattaques. Du même coup, les cybermenaces sont de plus en plus complexes, malveillantes et bien financées, ce qui place la barre toujours plus haut sur le plan de la cybersécurité.

2. Forum économique mondial, *The Global Risks Report 2017, 12th Edition,* http://cybersecurityventures.com/cybersecurity-market-report/ Consulté le 9 mai 2017.

Les facteurs clés qui redéfinissent le contexte des cybermenaces sont les suivants :

La dissolution du périmètre : les innovations telles que les technologies hybrides, l'infonuagique et les écosystèmes numériques brouillent les frontières entre les organisations et estompent le périmètre de son réseau qu'une organisation doit protéger.

Les technologies exponentielles : l'utilisation accrue de technologies exponentielles, telles que la robotique, l'automatisation, les micropuces 3D, la capacité cognitive et le développement agile, modifie le rythme des innovations commerciales et technologiques. Cela accélère les cyberrisques et peut compliquer les cyberprogrammes, qui sont souvent axés sur des approches de TI et des échéanciers traditionnels.

Les réseaux mobiles : la technologie mobile est plus qu'une simple fonctionnalité que les organisations doivent offrir à leurs clients. Pour un nombre croissant de consommateurs, particulièrement ceux de la génération Y, la technologie mobile est un mode de vie. Pour eux, c'est plus qu'un autre canal; c'est le seul canal qui compte. Par conséquent, la technologie mobile suscite de tout nouveaux comportements d'achat. Elle augmente aussi grandement la surface d'attache des cybermenaces, car les réseaux mobiles sont géographiquement vastes et fluides.

L'Internet des objets (IdO) : qu'il s'agisse de capteurs intelligents dans une « usine intelligente » (Industrie 4.0) ou d'une connexion à distance à une pompe à insuline, l'IdO a un potentiel transformateur et devrait avoir une incidence positive sur notre vie. Toutefois, il donne aussi accès à tout un monde d'appareils à exploiter, ce qui peut tempérer la croissance ou l'acceptation de ces technologies.

La nature changeante des activités : les organisations novatrices créent de nouveaux modèles de revenus et d'exécution qui s'accompagnent de cyberdéfis à tous les niveaux, à commencer par les échelons supérieurs en ce qui a trait à la stratégie d'affaires.

L'intelligence artificielle (IA) : l'intelligence artificielle commence à compléter ou à remplacer les experts humains. Ce phénomène peut entraîner une grande amélioration des capacités et une réduction des coûts; mais il apporte aussi de nouveaux risques, comme des agents conversationnels qui deviennent incontrôlables et se comportent de manière inappropriée.

Les plates-formes de collaboration : les logiciels qui intègrent les réseaux sociaux aux processus d'affaires peuvent contribuer à favoriser l'innovation au sein de l'organisation, mais ils entraînent aussi une plus grande exposition aux risques provenant de sources externes.

Ces facteurs transformeront notre monde en créant des débouchés inimaginables sur le marché. Mais ils donneront également lieu à de nouveaux genres de cybermenaces qu'il est impossible de prévoir totalement.

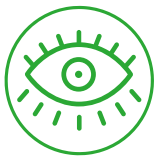
Passer à une cybersécurité de niveau supérieur

Même les menaces qu'une organisation croit bien maîtriser pourraient refaire surface si elles évoluent et gagnent en complexité. Par exemple, si les attaques par déni de service distribué (DDoS) existent depuis des années, elles sont aujourd'hui plus présentes, trompeuses et complexes que jamais, et visent souvent à détourner l'attention des attaques secondaires comme l'exfiltration de données, les attaques physiques ou l'implantation de logiciels de rançon.

Pour faire face aux cybermenaces en évolution et émergentes, une organisation doit s'assurer d'avoir mis en place des cybercapacités de base qui lui permettent de se protéger contre les menaces actuelles dès maintenant, tout en investissant dans des capacités de niveau supérieur en vue de se protéger contre les menaces qui pourraient se manifester à l'avenir. Ces capacités actuelles et de niveau supérieur se classent dans trois grandes catégories :

Sécurité

Vos moyens de défense concrets contre les attaques, allant des stratégies de cybersécurité aux systèmes et contrôles, en passant par les politiques et procédures.



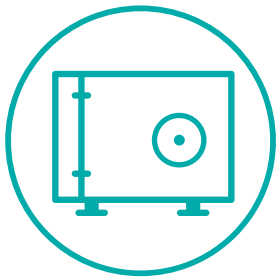
Vigilance

Vos systèmes d'alerte rapide, qui vous permettent de cerner les menaces potentielles avant qu'elles ne se manifestent, et de déceler rapidement les attaques et les failles à mesure qu'elles se produisent.

Résilience

Votre capacité de répondre promptement aux attaques et de reprendre rapidement vos activités de façon à ce que l'incidence sur votre organisation, votre réputation et votre marque soit minime.

Dans les pages qui suivent, nous examinons chacune de ces catégories et abordons les capacités actuelles et de niveau supérieur dont votre organisation a besoin pour assurer sa sécurité, aujourd'hui et à l'avenir.



Securité

Améliorez les contrôles axés sur les risques pour vous protéger contre les menaces connues et émergentes, et conformez-vous aux règles et aux normes sectorielles de cybersécurité

On entend par « sécurité » les moyens de défense d'une organisation ainsi que tous les éléments et les capacités connexes. À l'instar des clôtures et des portes verrouillées dans le monde physique, ce sont les mécanismes qui tiennent les intrus à l'écart. Sur le plan de la cybersécurité, cela comprend des capacités telles que la protection de l'infrastructure, la gestion des vulnérabilités, la protection des applications, la gestion des identités et des accès, et la confidentialité et la protection des renseignements.

Où vous devriez vous situer maintenant

Intégrez la cyberstratégie à la stratégie d'affaires

Dans un monde numérique, la cyberstratégie et la stratégie d'affaires vont de pair. Même si les objectifs d'affaires sont primordiaux, il n'est plus possible d'élaborer des stratégies d'affaires et des modèles d'affaires efficaces sans tenir compte de la façon dont ils seront touchés – et, dans bien des cas, dont ils seront soutenus – par les technologies numériques et par les moyens que l'organisation met en place pour se protéger contre les cybermenaces. Même la stratégie d'affaires la plus créative et la plus géniale au monde est inutile si l'organisation ne sait pas vraiment comment défendre les opérations essentielles contre les cyberattaques.

Une organisation doit envisager les conséquences et l'atténuation des cybermenaces dès le départ, au moment où elle élabore sa stratégie, pas des mois ou des années plus tard, alors que l'organisation a déjà commencé à mettre en œuvre les systèmes et les processus nécessaires et consacré d'innombrables ressources à la mise en œuvre d'un plan d'action particulier.

Définissez et protégez vos actifs essentiels

Même si, en théorie, une cyberstratégie qui assure la protection complète de tous les éléments au sein de l'organisation semble être la solution idéale, dans la pratique, ce n'est tout simplement pas réaliste. Si les cybermenaces sont infinies, les budgets et ressources de cybersécurité ne le sont pas. Cela signifie que vous devez établir des priorités, en plaçant vos « actifs attrayants » en tête de liste. C'est le cas dans les situations suivantes :

- **Les gens.** Les personnes clés qui pourraient être visées.
- **Les actifs.** Les systèmes et les autres actifs qui sont primordiaux pour votre entreprise et vos activités.
- **Les processus.** Les processus importants qui pourraient être perturbés ou exploités.
- **L'information.** Les données, l'information ou les renseignements qui pourraient être utilisés à des fins frauduleuses, illégales ou concurrentielles.

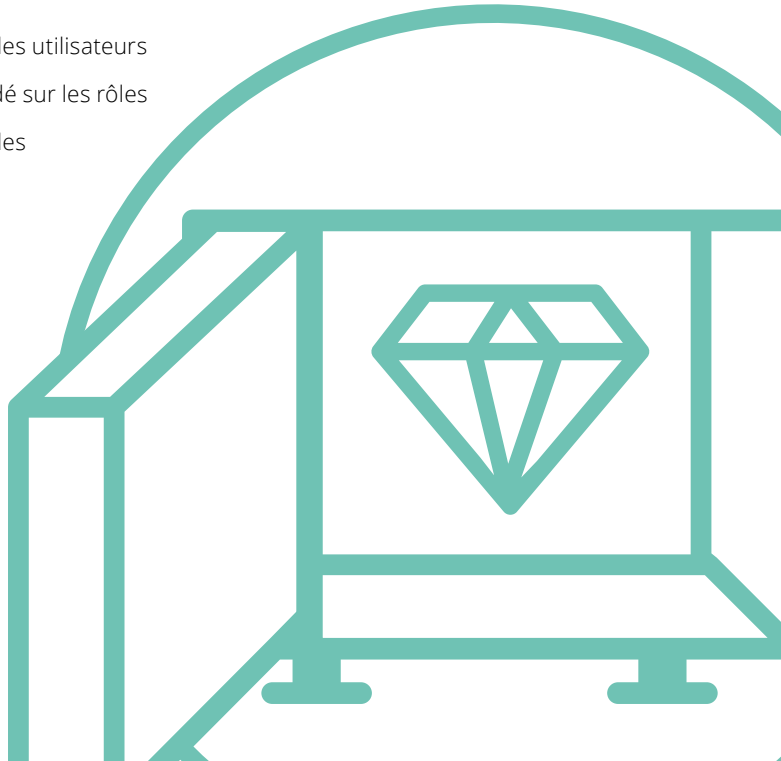
Les organisations qui n'établissent pas explicitement leurs stratégies en fonction de ces actifs attrayants risquent souvent d'affecter leurs ressources au hasard, et de trop investir dans des domaines peu importants et moins dans les domaines où ça compte vraiment, laissant ces derniers dangereusement vulnérables.

Une fois que vous avez déterminé quels sont vos actifs attrayants, la prochaine étape consiste à évaluer les menaces auxquelles ils sont particulièrement vulnérables, puis à dégager et à combler les lacunes en matière de sécurité et de contrôle qui pourraient les exposer à certains dangers.

Élaborez un cadre de cybersécurité solide

Une fois que vous avez créé une stratégie globale pour protéger vos actifs attrayants, la prochaine étape consiste à élaborer un cadre qui permettra d'intégrer la stratégie de cybersécurité à la stratégie d'affaires, et qui aidera votre organisation à la concrétiser. Comme c'est le cas de toutes les stratégies de cybersécurité, les détails précis du cadre sont uniques à chaque organisation. Cependant, le cadre comporte normalement quelques éléments de base :

- Stratégie et modèle opérationnel
- Politiques, normes et architecture
- Culture et comportements liés aux cyberrisques
- Gestion, paramètres et signalement des cyberrisques
- Gestion du cycle de vie
- Contrôle de l'accès par les utilisateurs
- Contrôle de l'accès fondé sur les rôles
- Contrôle de l'accès par les utilisateurs privilégiés



Cybersécurité : passer au niveau supérieur

Intégrez la cybersécurité partout, dès le départ

La cybersécurité a traditionnellement été traitée comme une question informatique qui s'ajoute ni plus ni moins après coup aux applications et aux systèmes de TI. Mais dans un monde numérique, cette approche complémentaire ne suffit plus. Les organisations doivent plutôt intégrer la cybersécurité à leur ADN et à l'ensemble de leurs activités, et ce, dès le départ. Comme il est indiqué ci-dessus, il est essentiel d'intégrer la stratégie de cybersécurité à la stratégie d'affaires. Par ailleurs, comme la plupart des organisations exécutent maintenant leur stratégie d'affaires sous forme d'entreprise étendue, elles doivent absolument tenir compte de la cybersécurité lorsqu'elles créent leur écosystème de fournisseurs, de distributeurs et de partenaires, et qu'elles collaborent avec ces derniers.

La cybersécurité doit aussi faire partie intégrante du développement d'applications. De nos jours, les développeurs se fient énormément à des méthodes telles que DevOps et Agile, qui sont axées sur la vitesse et la collaboration, et qui leur permettent de produire des applications beaucoup plus rapidement, ce qui est devenu un impératif numérique. Par contre, cette rapidité de mise en marché se fait parfois au détriment de la sécurité, puisque les contrôles et les fonctions de sécurité appropriées ne sont pas nécessairement intégrés à chacune des phases. En fait, de nombreux développeurs perçoivent encore la cybersécurité comme une entrave ou un obstacle à la rapidité et à l'efficacité d'exécution. C'est un conflit qu'il faudra résoudre alors que les organisations font passer leurs capacités de cybersécurité au niveau supérieur.

Heureusement, on a de plus en plus tendance à intégrer la sécurité à la méthode DevOps – qui réunit le développement et les opérations – et à la transformer essentiellement en méthode SecDevOps. Et si cette terminologie est un peu boiteuse, le fait d'intégrer la sécurité au développement et aux opérations est un grand pas dans la bonne direction.

Mettez au point de meilleurs moyens de gérer les données

Les données sont une précieuse ressource qui augmente de manière exponentielle à mesure que les gens et les organisations partout dans le monde adoptent tous les aspects de l'univers numérique. Aussi, il faut gérer cette précieuse ressource minutieusement pour en assurer la sécurité tout en exploitant sa pleine valeur.

La gestion du cycle de vie de l'information est l'une des clés du succès. Il s'agit d'une approche exhaustive pour gérer et sécuriser tous les aspects des données et de l'information, depuis l'acquisition jusqu'à la cession, en passant par toutes les étapes intermédiaires.

Ici, « plus » n'est pas nécessairement synonyme de « mieux », car plus vous avez de données, et plus vous les conservez longtemps, plus vous augmentez votre surface d'attaque, votre exposition aux risques et votre responsabilité juridique. Sans compter qu'il devient de plus en plus difficile et laborieux de gérer les données au jour le jour. Les quantités de données augmentent plus rapidement que jamais, en raison de l'utilisation croissante des technologies mobiles et l'essor de l'IdO. Et les données sont de plus en plus complexes, alors que les formats (structurés et non structurés) et les sources (y compris les tiers) se multiplient.

Comme pour la stratégie de cybersécurité globale, il convient d'accorder la priorité à la protection des données et de l'information les plus importantes. Les organisations qui tentent de sécuriser l'ensemble de leurs actifs d'information sont vouées à l'échec. Et il en va de même pour les organisations qui se concentrent sur leurs actifs attrayants, mais qui commettent l'erreur de tenter de protéger ces actifs essentiels contre toutes les menaces possibles.

En fin de compte, dans ce domaine, la réussite repose sur l'établissement des bonnes priorités : déterminer quels sont vos actifs les plus importants, puis protéger ces actifs contre les plus grandes menaces.

Vigilance

Détection et prévision des infractions et des anomalies grâce à une meilleure connaissance de la situation

La vigilance, c'est le système d'alerte rapide d'une organisation. Tout comme les caméras de sécurité et le gardien à l'accueil, les capacités de vigilance permettent de détecter et de prévoir les menaces avant qu'elles ne deviennent des attaques, les attaques avant qu'elles ne deviennent des atteintes à la sécurité, et les atteintes avant qu'elles ne se transforment en crises.

Où vous devriez vous situer maintenant

Prenez connaissance de la situation

La vigilance passe par la compréhension de vos adversaires, c'est-à-dire qui pourrait vous attaquer et pourquoi, puis par une connaissance de la situation afin de vous permettre de conserver une longueur d'avance. De nombreuses organisations croient qu'elles peuvent prendre suffisamment connaissance de la situation au moyen de rapports automatisés sur les cybermenaces, qui sont essentiellement des fils de nouvelles sur les menaces et les problèmes émergents. Malheureusement, une véritable vigilance nécessite beaucoup plus que cela. Plutôt que de vous contenter d'une connaissance générale des cybermenaces actuelles, vous devez comprendre votre propre contexte à l'égard de la cybersécurité, notamment les éléments qu'il faut absolument protéger et en quoi ils sont particulièrement vulnérables.

Plus précisément, les organisations devraient s'efforcer d'avoir une connaissance continue de la situation afin d'être en mesure de repérer les changements qui sont susceptibles de modifier leur exposition aux risques. Parmi ces changements, citons les fusions, les acquisitions, la diversification des modes d'exécution (p. ex., la délocalisation), les nouveaux fournisseurs, et même l'impartition de fonctions stratégiques (p. ex., le conseiller juridique).

Lorsque vous innovez, c'est une bonne idée de faire appel à des équipes de sécurité tôt dans la démarche afin qu'elles puissent effectuer des examens des systèmes qui permettront de dégager et de gérer les incidences imprévues liées aux menaces. De plus, grâce à des processus de surveillance robustes, il est possible de demeurer constamment à l'affût de ce qui se passe dans l'ensemble de l'environnement de cybersécurité. Est-il toujours sécurisé? Est-il victime d'une attaque? Y a-t-il eu violation? Un nombre étonnamment élevé d'organisations sont victimes d'une attaque ou d'une violation sans même s'en rendre compte.

Prêtez attention à l'ensemble de votre écosystème

Les fournisseurs, distributeurs et partenaires, voire les clients, peuvent tous être un point d'entrée pour les attaques. Cela signifie que, même si une organisation est très sécurisée, elle pourrait néanmoins être vulnérable. Car après tout, une chaîne est aussi solide que son maillon le plus faible.

Pour rester à l'affût, effectuez constamment des évaluations de la cybersécurité de votre écosystème afin de vous assurer que les éléments externes ne créent pas une exposition inacceptable aux risques. Par ailleurs, vous pouvez faire partie de la solution en transmettant de l'information aux partenaires dans l'écosystème et en favorisant la collaboration pour repousser les adversaires communs.

Il est également essentiel d'exercer une surveillance continue afin de déceler les activités suspectes ou atypiques, peu importe où elles pourraient se produire. Même si ce sont les attaques extérieures qui font les manchettes, bon nombre des plus grandes cybermenaces proviennent de l'intérieur et prennent naissance au sein de l'organisation ou de son entreprise étendue. Ces incidents internes peuvent être encore plus dommageables que les attaques provenant de l'extérieur, mais on a tendance à les taire. Qui plus est, dans certains cas, les dommages sont dénués d'intentions malveillantes et sont simplement le fruit de la négligence ou de la faiblesse des contrôles et des procédures.

Cybersécurité : passer au niveau supérieur

Utilisez des technologies de pointe pour repérer et désamorcer les attaques de manière proactive

Les organisations de premier plan exploitent la puissance de l'intelligence artificielle, de l'apprentissage cognitif, de l'analytique approfondie, des technologies de corrélation et des renseignements sur les cybermenaces pour accéder à un niveau supérieur de connaissance de la situation, ce qui leur permet de prévoir et de dégager les nouvelles menaces potentielles avant qu'elles ne se manifestent.

L'analytique approfondie et les technologies de corrélation peuvent aider une organisation à mieux comprendre comment une attaque a été lancée, quels types de pirates l'utilisent et quels points d'entrée ont été ciblés. Ces technologies permettent aussi la détection prédictive des menaces, qui contribue à anticiper et à atténuer les futures menaces susceptibles de découler des menaces actuelles, à mesure que les pirates trouvent des façons de contourner les mécanismes de sécurité existants.

Les renseignements sur les cybermenaces relèvent des professionnels formés dans ce domaine, qui surveillent un large éventail de sources d'information, notamment le web invisible, les rapports sur les logiciels malveillants et les activités en ligne afin de déceler les risques propres à votre organisation. Ces professionnels tirent des leçons des attaques dont sont victimes d'autres organisations, puis appliquent les renseignements recueillis afin de protéger les aspects les plus à risque au sein de votre organisation.

En plus d'assurer une surveillance, les équipes de renseignements chevronnées repèrent activement les nouvelles menaces. Si, par exemple, une équipe met au jour une nouvelle source de logiciels malveillants, elle peut créer un modèle analytique pour détecter les nouvelles occurrences et instances d'un logiciel malveillant. De là, elle peut créer des algorithmes et des processus automatisés pour repérer les menaces émergentes et empêcher les dommages.

Pour réussir dans ce domaine, il faut avoir une excellente compréhension des activités, qui découle d'une intégration et d'un engagement directs. En intégrant ces capacités de détection précoce des menaces aux processus d'affaires fondamentaux, vous pourrez mettre les renseignements sur les cybermenaces à profit dans l'ensemble de l'organisation, en rapprochant de la source la responsabilité de détection et de gestion des cyberrisques. Cette approche répartie et axée sur l'action gagnera en importance à mesure que votre surface d'attaque s'accroît et que les cybermenaces deviennent plus répandues et plus difficiles à repérer.

Comprenez et gérez les menaces exponentielles

Les technologies exponentielles et perturbations numériques amènent les organisations en terrain inconnu. Ce changement crée de nouveaux débouchés intéressants sur le marché; mais il augmente aussi considérablement la surface d'attaque, et présente des risques peu familiers et difficiles à prédire. Une hypothèse que nous pouvons formuler sans trop nous tromper, c'est que bon nombre de ces nouveaux risques seront très différents de ceux auxquels les organisations ont fait face par le passé et, par conséquent, ils nécessiteront de nouvelles approches.

Aujourd'hui, la plupart des organisations ont au moins fait l'essai de technologies exponentielles, en cherchant à faire croître leur entreprise, à améliorer considérablement leur productivité et leur efficacité, et à créer un avantage concurrentiel durable. Mais dès qu'une technologie exponentielle atteint une masse critique, le rythme de changement explose; il peut alors devenir difficile de faire face à l'émergence rapide des menaces.

Il est temps de commencer à réfléchir sérieusement aux conséquences des technologies exponentielles et des perturbations numériques sur la cybersécurité, et à créer les capacités nécessaires pour demeurer à l'abri. Cela nécessitera une vigilance encore plus prospective que d'habitude, car il s'agit de prévoir les menaces émergentes issues d'innovations et de technologies qui sont elles-mêmes encore en émergence. Aussi, ce point de vue futuriste vous amènera à prendre des décisions plus avisées et plus éclairées à court terme, et à jeter les bases nécessaires pour mettre en place, à long terme, des capacités suffisamment souples pour composer avec les menaces de demain.

Vous ne pouvez pas toujours faire cavalier seul

De nombreuses organisations peinent à mettre en œuvre leurs propres solutions d'analytique avancée et de renseignements sur les cybermenaces, surtout si leurs ressources internes et leur expertise sont limitées.

L'impartition d'une partie ou de l'ensemble de vos activités de cybersécurité à un fournisseur de services de sécurité gérés (FSSG) peut être un moyen pratique d'étendre les capacités des ressources et des talents à l'interne. Les FSSG offrent une vaste gamme de services utiles, dont la surveillance des menaces, la détection proactive des événements à risque, les renseignements, le suivi et l'analytique avancée.

Il pourrait également être utile de vous joindre à une communauté de partage de renseignements sur les cybermenaces ou d'en mettre une en place. Ces communautés ont pour but d'aider les organisations à améliorer leur position en matière de vigilance de différentes façons : en permettant un partage intersectoriel avec des organisations semblables, en mobilisant une expertise en cybersécurité, en tenant des discussions de groupe ouvertes, en améliorant la conformité aux exigences réglementaires, en élaborant un cadre de financement et en établissant des relations avec les gouvernements. C'est comme combattre le feu par le feu car, après tout, les cyberpirates tirent parti des communautés en ligne pour consolider leurs attaques. Ne devriez-vous pas faire de même pour consolider vos moyens de défense?

Résilience

La capacité de rétablir rapidement les activités et de réparer les dommages à votre entreprise

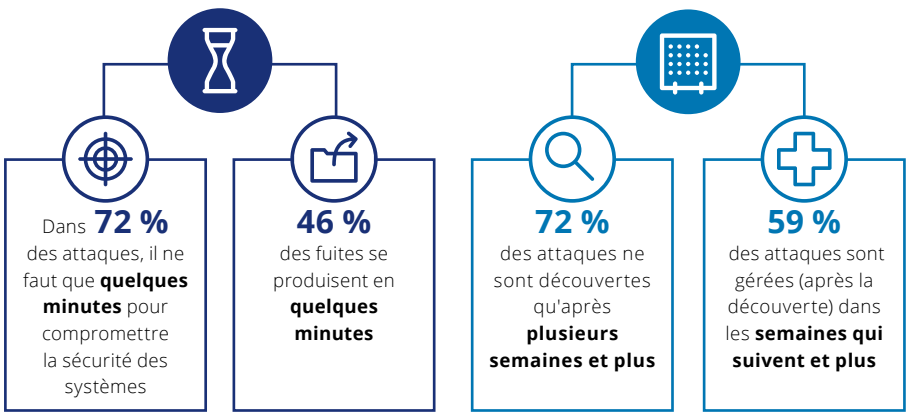
La résilience, c'est la capacité d'une organisation à gérer les cyberincidents efficacement, à réagir rapidement pour réduire les dommages au minimum en cas d'incident, et permettre le retour à la normale de l'entreprise et des activités dans les plus brefs délais.

Peu importe les fonds et les efforts que vous consacrez à la consolidation de vos cyberdéfenses, à un moment donné, vous serez victime d'une attaque. Quand cela se produira, que ferez-vous?

Au beau milieu d'une attaque, il n'y a pas de temps à perdre; avec chaque minute qui s'écoule, les dommages s'amplifient (voir le diagramme ci-dessous). Pourtant, de nombreuses entreprises demeurent essentiellement en mode réactif lorsqu'il s'agit de gérer les cyberincidents et les conséquences qui en découlent. En fait, selon un récent sondage réalisé par Nasdaq et Tanium, plus de 90 % des dirigeants d'entreprise affirment que leur organisation n'est pas prête à faire face à une importante cyberattaque[3].

Pour être résilient, vous devez établir un plan. Vous devez également assurer une gouvernance et une surveillance efficaces afin de coordonner les plans et les activités

Anatomie d'une cyberattaque



Le temps est précieux

3. Tom DiChristopher, « Execs: We're Not Responsible for Cybersecurity » (Avril 2016), CNBC, http://www.cnbc.com/2016/04/01/many-executives-say-theyre-not-responsible-for-cybersecurity-survey.html. Consulté le 9 mai 2017.

de réponse pour l'ensemble des parties prenantes, y compris les membres du conseil d'administration et les dirigeants autres que des TI. Pour la plupart des organisations, cette approche globale nécessite un changement de mentalité; en effet, il faut cesser de considérer les cyberfailles comme un risque de TI et comprendre que la cybersécurité est un enjeu d'affaires stratégique qui devrait être pris en considération en tant que partie intégrante de la planification de la reprise après sinistre d'une organisation.

Le processus de préparation est constant et continu – développer, tester, évoluer et répéter – et l'objectif est de se doter d'un plan d'intervention qui gagne constamment en maturité et qui évolue de façon à s'adapter aux menaces émergentes et aux changements touchant les cybermenaces au sein de l'organisation.

Où vous devriez vous situer maintenant

Établissez d'abord un plan de résilience

Lorsque vous êtes au beau milieu d'une crise, ce n'est pas le moment de tenter de comprendre tout ce qui se passe. Il faut élaborer longtemps à l'avance un plan de résilience efficace, suffisamment clair et concis pour que les gens puissent le comprendre facilement dans le feu de l'action, mais aussi suffisamment détaillé pour être réalisable sur-le-champ. Voici des éléments types qui peuvent y figurer :

1. **Gouvernance.** Établissez la coordination interfonctionnelle, la documentation et la communication avec les parties prenantes.
2. **Stratégie.** Créez une stratégie organisationnelle solide et harmonisée pour gérer les cyberincidents, notamment la communication avec la haute direction, le conseil d'administration et les clients.
3. **Technologie.** Comprenez les éléments techniques de l'intervention en cas d'incident et la documentation des atteintes à la sécurité. (Quelles enquêtes numériques seront réalisées? L'équipe dispose-t-elle de processus pour consigner les incidents et effectuer une analyse des incidents avec l'aide du groupe d'opérations des TI?)
4. **Gestion des opérations.** Créez des processus intégrés de reprise des activités après une catastrophe et de continuité des opérations, y compris des communications proactives. (Un plan de résilience opérationnelle a-t-il été mis en place en cas de cyberincident?)
5. **Risque et conformité.** Assurez-vous que le plan de résilience prévoit la participation des gestionnaires du risque de cybersécurité et de la conformité, notamment des échanges avec les organismes de réglementation, les conseillers juridiques et les autorités policières.

Mettez votre organisation à l'épreuve

Une fois qu'une organisation a mis en place un plan solide, elle doit régulièrement effectuer des exercices et des simulations dans un environnement contrôlé de façon à convaincre tout le monde que le plan fonctionne. Ces essais et séances pratiques comprennent des jeux de guerre, des simulations d'attaque (équipe rouge) et l'évaluation des compromissions.

Les jeux de guerre consistent à simuler les actions et réactions qui se produiraient au cours d'un cyberincident. Cela permet à l'organisation de voir son plan d'action à l'œuvre et de dégager les écarts qui doivent être comblés. Des dirigeants sont affectés à la gestion des divers éléments de l'atteinte simulée, ce qui permet de vérifier la mesure dans laquelle ils réagiraient efficacement dans une réelle situation d'attaque. Souvent, les participants ne savent pas qu'il ne s'agit que d'une simulation, ce qui donne aux organisations la possibilité de déterminer avec honnêteté et exactitude à quel point les équipes réagissent rapidement, si le conseil d'administration est engagé, et comment les décisions sont prises. Cela comprend la décision d'informer ou non le Commissariat à la protection de la vie privée, un poste réglementaire établi récemment en vertu des nouvelles lois exigeant que les organisations signalent toute atteinte à la protection des données qui présente un « préjudice grave » pour les personnes.

L'équipe rouge effectuera un piratage dissimulé et sanctionné, normalement à la demande et avec l'approbation des dirigeants ou du conseil d'administration de l'organisation, pour mettre les moyens de défense à l'épreuve et dégager les points faibles. Bon nombre d'organisations ne savent pas à quel point leur cyberenvironnement est mis en danger et ne seront portées à le croire que si on leur présente des preuves. Une solide attaque par l'équipe rouge peut apporter ces preuves, en dérobant des données des clients sans même atteindre le réseau central. Une fois que l'équipe rouge a porté atteinte à la sécurité, elle peut évaluer la rapidité et l'efficacité avec laquelle l'équipe défensive de l'organisation (l'équipe bleue) cerne l'attaque et intervient. Traditionnellement, les équipes rouge et bleue fonctionnent en vase clos. Toutefois, de plus en plus d'organisations mettent sur pied des équipes hybrides, au sein desquelles les équipes rouge et bleue collaborent afin d'échanger des renseignements et des leçons apprises.

L'évaluation des compromissions est un autre outil utile qui permet à une organisation de déterminer, dans le doute, si l'on a porté atteinte à sa sécurité et s'il y a une présence criminelle au sein de son système.

Individuellement et collectivement, tous ces tests révèlent des renseignements essentiels sur les forces et les lacunes d'une organisation à l'égard de sa résilience, ce qui peut se traduire par des améliorations à la gouvernance, à la transmission des cyberincidents aux

échelons supérieurs, à la stratégie de communication, à la sensibilisation de la direction, aux capacités de réaction aux cyberattaques et à l'analyse prospective. Les résultats des tests peuvent contribuer à faire passer le message en démontrant concrètement la vulnérabilité : quelle a été la « perte » d'argent, quelles données ont été « corrompues », etc.

Ces tests feront presque assurément en sorte que l'organisation sera plus forte et résiliente. Par contre, ils ne devraient pas être menés au hasard ou une seule fois. Les jeux de guerre et les simulations devraient être réalisés chaque année, tandis que l'équipe rouge devrait intervenir de façon ponctuelle, mais soutenue. Les organisations devraient également mettre à jour leur plan global de cyberrésilience au moins une fois par année, puis le mettre à l'épreuve, l'évaluer et le modifier au besoin en fonction de l'évolution des menaces.

Cybersécurité : passer au niveau supérieur

Élaborez des guides adaptés aux menaces et aux situations

Dans les cas des menaces extrêmes, surtout celles qui touchent les actifs attrayants de l'organisation, il convient d'élaborer à l'avance des guides qui sont adaptés à des situations ou à des menaces précises. Ces guides décrivent les événements successifs qui sont susceptibles de se produire lorsqu'un type d'attaque particulier se déroule, de même que les mesures à appliquer pour réduire les dommages au minimum et prendre le dessus.

Dans une situation de crise, chaque moment compte, et chaque faux pas peut se révéler désastreux. Les guides adaptés aux menaces et aux situations vous permettent d'effectuer une planification réfléchie et rigoureuse, en dehors du contexte d'une crise, de façon à pouvoir réagir plus rapidement et efficacement lorsqu'une attaque survient. Ils donnent aussi une vue d'ensemble des menaces potentielles, ce qui vous permet d'établir des priorités claires et de vous concentrer sur ce qui compte le plus pour votre organisation, plutôt que de commettre l'erreur fréquente de consacrer la majeure partie de votre temps et de vos ressources à vous défendre contre les attaques qui ont fait les manchettes récemment.

Élaborez une approche fondée sur une intervention unique

Le but ultime d'un plan de cyberrésilience devrait être l'élaboration d'une approche de gestion des atteintes à la sécurité fondée sur une intervention unique. Un trop grand nombre d'organisations, même parmi celles qui considèrent qu'elles maîtrisent la résilience, ont mis en place une stratégie d'intervention multidimensionnelle qui comporte trop de disparités entre ses nombreuses variables.

Une approche fondée sur une intervention unique signifie qu'il est possible d'entreprendre une démarche cohésive et coordonnée sur les plans juridique, de l'assurance, de la cybersécurité et de la juricomptabilité. En plus d'accroître la résilience, cela favorise la conformité aux exigences des nouveaux règlements sur la déclaration obligatoire des atteintes à la protection des données (qui entreront en vigueur à l'automne 2017).

En vertu de cette nouvelle loi, les organisations seront tenues d'aviser toute personne concernée, de même que le Commissariat à la protection de la vie privée du Canada, de toute atteinte à la protection des données qui présente un « un risque réel de préjudice grave à l'endroit de l'intéressé ». Les organisations doivent le faire « le plus rapidement possible », sous peine d'amendes pouvant atteindre 100 000 $.

La dimension humaine

Malgré la priorité accordée à la technologie et à l'innovation, l'efficacité de la sécurité repose sur les gens, qui mettent à profit leur expertise approfondie et leurs points de vue stratégiques pour lutter contre la cybercriminalité. Les outils sont importants, mais les pirates sont passés maîtres dans l'art de les contourner. Pour être efficace, la cybersécurité doit pouvoir compter sur une combinaison de gens, de processus et de technologies.

L'art et la science de la cybersécurité

La cybersécurité est à la fois un art et une science. Pour freiner les attaques, il vaut mieux faire appel à des spécialistes qui maîtrisent l'art de la cybersécurité et qui, en plus de pouvoir utiliser les outils préventifs appropriés, sont en mesure de comprendre les motivations des attaquants, et possèdent l'acuité tactique et le sens des affaires nécessaires pour aligner la stratégie de cybersécurité sur la stratégie d'affaires. Malheureusement, ces compétences sont une denrée rare de nos jours. Aussi, bon nombre d'organisations ont du mal à réunir un bassin de professionnels compétents pour assurer leur cybersécurité.

Les outils et les logiciels destinés à la cybersécurité sont de plus en plus évolués, ce qui peut aider une organisation à en faire plus avec moins. Par contre, ils ne sauraient remplacer des experts humains, qui peuvent souvent déceler les anomalies et les menaces qui échapperaient à un logiciel.

Le rôle du chef de la sécurité de l'information

Le chef de la sécurité de l'information joue un rôle de premier plan dans la démarche de cybersécurité. Il doit être habilité par l'organisation à contribuer à la stratégie, ce qui signifie qu'il doit participer à la prise des décisions stratégiques et bien comprendre les priorités de l'organisation du point de vue technique et des affaires.

La cyberstratégie a une incidence sur tous les secteurs de votre entreprise; aussi, elle doit être perçue comme un risque d'affaires, pas seulement comme une question informatique. C'est au chef de la sécurité de l'information qu'il incombe de mener cette transformation. Évidemment, cela est souvent plus facile à dire qu'à faire.

L'amélioration de la cybersécurité représente un important défi qui soulève un paradoxe difficile pour les chefs de la sécurité de l'information. Selon un récent sondage réalisé auprès des chefs de la sécurité de l'information, 61 % d'entre eux croient que la cybersécurité est l'une des principales attentes envers eux et le service des TI. Parallèlement, 33 % d'entre eux sont d'avis que l'entreprise considère la gestion de la sécurité et des risques comme une corvée de conformité, un coût pour l'entreprise ou une dépense opérationnelle[4].

Dans les organisations qui ont atteint la cybermaturité, les chefs de la sécurité de l'information ont beaucoup d'autorité et sont considérés comme des conseillers stratégiques par le conseil d'administration, la direction et les employés. Parce que leur organisation reconnaît que la cybersécurité constitue un risque d'affaires qui doit être géré de façon collective, les chefs de la sécurité de l'information peuvent jouer un rôle moins tactique et plus transformateur et stratégique, en mettant l'accent sur des risques plus généraux comme ceux qui sont associés au lancement de nouveaux produits et de nouvelles applications, ou à la transmission de renseignements au sein de l'entreprise étendue.

4. Presses de l'Université Deloitte, *Navigating Legacy: Charting the Course to Business Value—2016–2017 Global CIO Survey (2016)*, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-cio-survey-2016-2017-full-report.pdf. Consulté le 9 mai 2017.

Devenir un leader de la gestion des cyberrisques

Alors que l'économie canadienne est de plus en plus basée sur les connaissances, les perturbations numériques et les technologies exponentielles deviendront les principaux moteurs de croissance et de rendement, offrant aux organisations des occasions sans précédent de créer de la valeur et d'acquérir un avantage concurrentiel. Mais pour en profiter, elles devront adhérer sans réserve à l'innovation numérique et, forcément, aux cyberrisques qui l'accompagnent.

Pour réussir, vous devez vous attaquer aux cyberrisques avec brio, en élaborant et en mettant en œuvre une robuste stratégie de cybersécurité qui assurera la sécurité, la vigilance et la résilience de votre organisation. Cette stratégie doit porter non seulement sur les menaces qui existent aujourd'hui, mais aussi sur les menaces de niveau supérieur qui ne se sont pas encore manifestées.

Heureusement, si les cyberrisques constituent un défi important et croissant, ils ne sont pas insurmontables. Et même si l'espoir n'est pas une stratégie, la situation est loin d'être désespérée. En fait, nous constatons déjà des changements positifs dans la façon dont les organisations canadiennes de premier plan réagissent à l'impératif de cybersécurité.

En plus d'améliorer leurs compétences générales de gestion des cyberrisques, notamment en étendant les rôles et la portée du chef de la sécurité de l'information et de la fonction de gestion des risques, les organisations ayant atteint la cybermaturité s'efforcent d'intégrer la cybersensibilisation au cœur même de leur organisation. De plus, elles commencent à tirer parti des technologies intelligentes pour détecter, prévoir et atténuer les risques, tout en reconnaissant que la cybersécurité est à la fois un art et une science, et que même les outils les plus évolués ne peuvent remplacer la créativité, la perspective et le jugement des experts humains.

Les cyberrisques ne sont pas une question informatique. Il s'agit d'un enjeu d'affaires. Aussi, les leaders de la gestion des risques et de la sécurité, ainsi que les chefs d'entreprise, doivent chercher constamment à parvenir à un équilibre entre le besoin de mettre en place un solide système de cybersécurité et les besoins stratégiques de l'entreprise.

En sachant quelles mesures il faut prendre, et en ayant la prévoyance et le courage requis pour relever les défis, votre organisation peut devenir maître de son propre cyberavenir et devenir un agent perturbateur, plutôt que de se laisser perturber.

Annexe A
Principaux points à retenir pour passer de l'état actuel à la sécurité de niveau supérieur

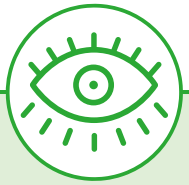
Sécurité

Maintenant

- Intégrez la cyberstratégie à la stratégie d'affaires
- Identifiez et protégez vos actifs attrayants
- Élaborez un cadre de cybersécurité solide

Niveau supérieur

- Intégrez la cybersécurité partout, dès le départ
- Mettez au point de meilleurs moyens de gérer les données



Vigilance

Maintenant

- Prenez connaissance de la situation
- Prêtez attention à l'ensemble de votre écosystème

Niveau supérieur

- Utilisez des technologies de pointe pour repérer et désamorcer les attaques de manière proactive
- Comprenez et gérez les menaces exponentielles

Résilience

Maintenant

- Commencez par un plan de résilience
- Mettez votre organisation à l'épreuve (jeux de guerre, équipe rouge, simulations d'attaque, évaluation des compromissions)

Niveau supérieur

- Élaborez des guides propres aux menaces et aux situations
- Élaborez une approche fondée sur une intervention unique

Annexe B Éléments clés d'une cyberstratégie

Les défis de demain seront différents de ceux d'aujourd'hui. Comment pouvez-vous conserver une longueur d'avance?

Pour qu'une organisation soit en mesure de faire face à une cyberattaque, elle doit mettre en place un excellent cyberprogramme reposant sur des bases solides. Voici les principaux éléments d'une solide cyberstratégie :

1. Stratégie, gestion et risques

Des incidents comme la récente attaque du logiciel de rançon WannaCry nous rappellent que les cybermenaces évoluent constamment. La cybersécurité nécessite une mentalité d'amélioration continue et un effort conscient visant à assurer que des contrôles de cybersécurité adéquats sont en place pour gérer les principales menaces qui planent sur l'organisation. Une solide cyberstratégie signifie que l'organisation peut efficacement évaluer et comprendre les risques auxquels elle fait face, et qu'elle a mis en place un plan d'action concret en vue de mettre en œuvre les contrôles nécessaires pour assurer sa protection.

2. Politiques et procédures

Les politiques et procédures de l'organisation transforment sa cyberstratégie en interventions et en comportements significatifs. Souvent, elles définissent les rôles et les responsabilités des différents intervenants en cas d'incidents de cybersécurité importants ainsi que les étapes requises pour gérer la situation et limiter les dommages. Les organisations les mieux sécurisées répéteront périodiquement leurs procédures de réponse et mettront en place des plans d'intervention en cas d'incident afin d'assurer une réaction concertée à différents types d'incident.

3. Moyens de défense techniques

Les moyens de défense techniques et autres mesures de protection constituent souvent la première ligne de défense d'une organisation contre les cybermenaces. De nombreuses solutions techniques peuvent être mises à profit pour protéger l'organisation contre les menaces, qu'il s'agisse de pare-feu ou d'une protection de base contre les logiciels malveillants, ou de solutions pointues permettant de repérer et de contrer les attaques provenant de l'intérieur. Quelles que soient les solutions retenues, l'organisation doit bien comprendre les cybermenaces auxquelles elle fait face afin de déterminer les investissements les plus efficaces. Par ailleurs, l'organisation doit constamment revoir ses défenses techniques afin de veiller à ce qu'elles demeurent pertinentes au fil de l'évolution des menaces.

4. Surveillance et connaissance de la situation

Toutes les organisations doivent atteindre un équilibre entre leurs contrôles de sécurité destinés à la protection et à la détection. En général, les contrôles de protection font partie de la première ligne de défense de l'organisation. Dans l'éventualité où une attaque parvient à pénétrer le réseau, les capacités de détection de l'organisation entrent en jeu afin d'établir comment le pirate est parvenu à ses fins et quels actifs ont été touchés. Ce n'est qu'au moyen d'une surveillance efficace et d'une bonne connaissance de la situation que l'organisation pourra entreprendre des procédures de réponse en vue de limiter les dégâts. Cependant, les organisations très vigilantes se sont déjà dotées d'une surveillance et d'une connaissance de la situation qui leur permet de reconnaître les menaces et les attaques potentielles avant même qu'elles ne réussissent à pénétrer leur réseau.

5. Sécurité des fournisseurs

La plupart des organisations font appel à des fournisseurs externes pour obtenir des services ou obtenir des avis. Elles doivent souvent établir un partenariat étroit avec ces fournisseurs, ce qui les expose à des cybermenaces supplémentaires. Par exemple, une organisation qui fait l'acquisition de logiciels auprès d'un fournisseur externe compte sur l'efficacité des contrôles de sécurité du fournisseur pour détecter les codes malveillants. Le fait de comprendre le rôle des fournisseurs externes au sein de l'écosystème de cybersécurité de l'organisation permet à cette dernière d'appliquer les contrôles techniques et contractuels appropriés afin de limiter son exposition.

6. Sensibilisation des employés

Aussi efficaces soient-ils, les contrôles techniques ne suffisent pas, et les employés continueront de jouer un rôle important pour assurer votre cybersécurité. Lorsqu'un employé reçoit un courriel d'un expéditeur inconnu comportant une pièce jointe suspecte, sa décision d'ouvrir la pièce jointe ou de la supprimer, puis de signaler le courriel, pourrait faire la différence entre le cours normal des activités et un important incident de cybersécurité. La formation et la sensibilisation sont des éléments importants à la mise en place d'une culture de cyberrisques appropriée qui favorise l'adoption des bons comportements.

Personnes-ressources

Auteurs

Marc MacKinnon

Associé, Services liés aux cyberrisques
mmackinnon@deloitte.ca

Mark Fernandes

Associé, Services liés aux cyberrisques
markfernandes@deloitte.ca

Personnes-ressources

Nick Galletto

Leader global, Amériques et Canada
Services liés aux cyberrisques
ngalletto@deloitte.ca

Amir Belkhelladi

Associé, leader national
Cybersécurité
abelkhelladi@deloitte.ca

Robert Masse

Associé, leader national
Cyberrésilience
rmasse@deloitte.ca

Rocco Galletto

Associé, leader national
Cybervigilance
rgalletto@deloitte.ca

Deloitte.