Deloitte.

La cybersécurité : un impératif pour tous

Guide de protection contre les cyberrisques à l'intention des hauts dirigeants et des conseils d'administration

Sécurité

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 en matière de cybersécurité.

Vigilance

Détectez les infractions et les anomalies grâce à une meilleure prise de conscience de la situation à l'échelle de l'entreprise.

Résilience

Acquérez la capacité de reprendre les activités normales et de réparer les dommages subis par l'entreprise.

Le présent document contient 10 questions sur la cybersécurité et la résilience que les conseils d'administration devraient se poser et auxquelles ils devraient être en mesure de répondre; il a été conçu dans le but de servir de guide pour déterminer si le niveau de maturité de l'organisation en matière de cybersécurité et de capacités est « élevé », « modéré » ou « faible ». Analysées sous le triple angle de la sécurité, de la vigilance et de la résilience, les questions évaluent l'importance accordée par le conseil d'administration et les hauts dirigeants à la cybersécurité, la force de la cyberculture de l'organisation ainsi que le rôle de l'organisation comme gardienne mondiale du commerce numérique, pour l'aider à cibler les lacunes importantes et les aspects pouvant être améliorés. La gestion des cybermenaces se concentrait habituellement sur le volet de la sécurité et accordait moins d'importance à la vigilance et à la résilience. Nos questions et notre évaluation de la maturité sont conçues pour remédier à ce déséquilibre et brosser un portrait global de l'entreprise cyberprotégée.

Les conseils d'administration et les hauts dirigeants ont un rôle important à jouer pour aider les organisations à déterminer comment réagir aux nouvelles cybermenaces.

Les cybermenaces et les cyberattaques sont de plus en plus nombreuses et complexes. Dans notre monde numérique axé sur l'information, la gestion des cybermenaces est devenue un impératif d'affaires stratégique. En effet, les enjeux sont plus importants que jamais. Le cybercrime est plus qu'une fraude ou un vol. Il est maintenant le terrain de jeu de vastes réseaux de criminels ainsi que de pirates informatiques étrangers financés par des gouvernements et des cyberterroristes.

Les coûts tangibles découlant du cybercrime comprennent des fonds volés, des systèmes endommagés, des amendes pour infractions à la réglementation et des compensations financières pour les parties touchées. Les coûts intangibles, quant à eux, peuvent inclure la perte d'un avantage concurrentiel en raison du vol de propriété intellectuelle, la perte de clients ou de partenaires d'affaires et des dommages globaux à la réputation et à la marque de l'organisation. Au-delà des dommages subis par les entreprises individuelles, l'étendue même des cyberattaques est telle qu'elles ont maintenant le potentiel d'entraîner des pannes massives d'infrastructure et d'avoir une incidence sur la fiabilité des systèmes financiers de tout un pays et sur la santé de l'économie.

Une cybersécurité efficace commence tout d'abord par une prise de conscience de la part des membres du conseil d'administration et des hauts dirigeants qui ont besoin de reconnaître que, à un moment donné, l'organisation fera l'objet d'une attaque. Les organisations doivent comprendre les menaces les plus importantes et savoir comment elles peuvent mettre en danger les actifs qui sont au cœur de leur mission. À mesure que les conseils d'administration et les hauts dirigeants jouent un rôle plus actif dans la protection de leurs organisations, ils sont nombreux à se demander comment accroître l'efficacité de leur rôle (quelles sont leurs responsabilités, quelles compétences ils devraient perfectionner, quelles sont les bonnes questions à poser, etc.).

Comme chaque organisation et chaque secteur sont différents, cette FAQ vise non pas à offrir des solutions passe-partout aux problèmes énoncés, mais plutôt à aider les organisations à repérer leurs enjeux les plus critiques afin de pouvoir commencer à élaborer un programme de cybersécurité personnalisé ou à améliorer celui déjà en place. Nous espérons aussi stimuler les discussions du conseil d'administration sur les cyberstratégies actuelles de la direction et sur leur efficacité à traiter des défis actuels et futurs, à atténuer les risques et à prévoir des possibilités.

Évaluez votre niveau de maturité

Les questions suivantes sur la cybersécurité ainsi que les réponses qui les accompagnent devraient permettre efficacement aux organisations d'évaluer leur état de cybersécurité; inciter dûment leur équipe responsable de la sécurité de l'information à renforcer leurs mesures de cybersécurité en posant les bonnes questions et en fournissant des informations essentielles; et les aider à surveiller en permanence la résilience de leurs systèmes et à l'améliorer dans le futur.

Cette FAQ vous aidera à repérer des forces et des faiblesses précises et des solutions d'amélioration. Déterminez où se situent les réponses de votre organisation aux questions suivantes sur l'échelle de maturité de l'entreprise en cybersécurité :

Échelle de maturité de l'entreprise en cybersécurité

Maturité élevée
L'état de la cybersécurité est excellent sur tous les plans.

Maturité modérée
Des mesures de cybersécurité sont en place, mais du travail reste à faire.

Maturité faible
L'entreprise accuse un retard en matière de cybersécurité. Peu de mesures sont en place et il reste un travail considérable à faire.

Question

1

Le conseil d'administration et les hauts dirigeants font-ils preuve de diligence raisonnable, de responsabilité et d'une gestion efficace des cyberrisques?

Maturité élevée

- ☐ Le conseil d'administration et les hauts dirigeants désignent un haut dirigeant responsable de la gestion des risques liés aux cybermenaces, supervisent l'élaboration d'un programme de cybersécurité et s'assurent de sa mise en œuvre.
- ☐ Le conseil d'administration et les hauts dirigeants se tiennent informés sur les cybermenaces et leur incidence potentielle sur leur organisation.
- ☐ Le conseil d'administration comprend au moins un membre qui connaît les TI et les cyberrisques, ou fait appel à des conseillers stratégiques au besoin.
- ☐ Un comité de la haute direction se consacre exclusivement au problème des cyberrisques ou un autre comité de la haute direction accorde le temps nécessaire pour examiner la mise en œuvre du cadre de cybersécurité.
- ☐ Les mises à jour régulières, l'analyse du budget et les questions complexes soumises à la direction mettent en évidence l'exercice d'une diligence raisonnable.

Maturité modérée

- ☐ La direction et le conseil d'administration sont préoccupés par les cyberrisques, mais les communications avec les parties intéressées et la surveillance de certaines structures demeurent très générales.
- ☐ Le conseil d'administration a des connaissances pratiques des TI et des cyberrisques.
- ☐ Il existe une lacune en ce qui a trait à la diligence raisonnable en matière de cybersécurité et à la capacité de remettre en question les idées de la direction quant aux enjeux liés à la cybersécurité.
- ☐ Le conseil évalue le cadre de la cybersécurité et les exigences en matière de stratégies de façon sporadique.

Maturité faible

- ☐ La direction n'accorde pas beaucoup d'importance à la cybersécurité et ne comprend pas bien les questions stratégiques.
- ☐ Peu d'engagement de la part de la direction à l'égard de certaines questions de sécurité informatique.
- ☐ Le conseil manque d'expérience en matière de TI et de cyberrisques, et la cybersécurité est laissée aux soins du service des TI.
- ☐ La surveillance de la cybersécurité et l'évaluation des exigences budgétaires connexes demeurent très générales.

Question

2

Avons-nous le bon leader et les bonnes compétences organisationnelles?

Maturité élevée

- ☐ Le leader de la cybersécurité possède la bonne combinaison de connaissances techniques et de sens des affaires pour comprendre le fonctionnement de l'entreprise, collaborer avec elle et savoir où concentrer les efforts.
- ☐ Des équipes d'employés passionnés et dynamiques tiennent à jour leurs connaissances sur les tendances en matière de cybersécurité, les menaces et leur incidence sur leurs activités.
- ☐ Les discussions sur le cyberrisque ont lieu au sein du conseil et de la haute direction.
- ☐ Il y a suffisamment de personnel compétent possédant une expérience sectorielle pertinente axée sur les bons domaines.
- ☐ Les programmes de rémunération et d'avantages sociaux sont conformes au secteur et au profil de risque de l'organisation.

Maturité modérée

- ☐ Un leader de la cybersécurité est en place, mais se concentre principalement sur les risques techniques associés à la cybersécurité.
- ☐ Le leader de la cybersécurité a des connaissances pratiques du secteur, mais ne comprend pas parfaitement le fonctionnement de l'organisation.
- ☐ La cybersécurité est un élément important, mais la surveillance demeure très générale.
- ☐ Les questions liées aux cyberrisques sont souvent bloquées au niveau des TI ou de la direction.
- ☐ Des employés compétents en matière de cybersécurité sont présents dans les TI et dans certains autres secteurs de l'entreprise, mais ils ne connaissent que des menaces sectorielles ponctuelles.

Maturité faible

- ☐ La direction accorde peu d'attention à la cybersécurité.
- ☐ Les connaissances en matière de cybersécurité et les talents qui les possèdent sont concentrés dans les services des TI.
- ☐ Des programmes de formation ponctuels sont élaborés pour de nouvelles technologies précises.
- ☐ Grand roulement du personnel de cybersécurité en raison d'un manque d'investissement dans la stratégie en matière de talents.

Question

3

Avons-nous établi un processus approprié d'escalade des questions relatives aux cyberrisques aux échelons supérieurs qui tient compte de notre tolérance au risque et comprend des seuils de signalement?

Maturité élevée

- ☐ La tolérance aux risques et les cyberrisques sont clairement définis et intégrés dans les processus de gouvernance et de gestion des risques.
- ☐ Le conseil d'administration a approuvé une politique de cybersécurité pour l'ensemble de l'entreprise.
- ☐ Les responsabilités et les rôles opérationnels sont clairement définis pour chacune des trois lignes de défense.
- ☐ Des indicateurs de risque et de rendement existent et des processus sont en place pour signaler les infractions aux limites et aux seuils à la haute direction pour les incidents de cybersécurité importants ou critiques.
- ☐ Le cadre de gestion des incidents inclut des critères de transmission aux échelons supérieurs conformes au programme de cybersécurité.
- ☐ La valeur de l'assurance en matière de cybersécurité est évaluée et surveillée.

Maturité modérée

- ☐ La politique établie en matière de cybersécurité n'est pas complètement mise en œuvre à l'extérieur des TI.
- ☐ Les cyberrisques sont abordés uniquement de façon générale dans les processus de gouvernance et de gestion des risques globaux.
- ☐ La tolérance au risque n'est pas intégrée dans le cadre de gestion des cyberrisques.
- ☐ La réponse aux risques tend à être plus réactive que proactive.
- ☐ Un autre comité de haute direction consacre assez de temps à l'examen de la mise en œuvre du cadre de cybersécurité.

Maturité faible

- ☐ Aucun cadre officiel de cybersécurité n'est en place.
- ☐ L'acheminement aux échelons supérieurs des questions liées aux risques est ponctuel et a lieu uniquement en réponse à des incidents.

Question

4

Nous concentrons-nous sur les bonnes choses et faisons-nous les bons investissements?

Maturité élevée

- ☐ Le cyberrisque est pris en compte dans toutes les activités (de la planification stratégique aux activités quotidiennes), dans toutes les sphères de l'organisation.
- ☐ Les investissements sont axés sur des contrôles de sécurité de base visant la majorité des menaces, et des fonds ciblés de façon stratégique sont utilisés pour gérer les risques liés aux processus et aux renseignements les plus importants de l'organisation.
- ☐ L'organisation a pris la peine de repérer les risques de type « black swan » et a élaboré un programme pour prévoir et éviter ces menaces potentiellement catastrophiques, mais improbables.
- ☐ Les investissements et les budgets de l'organisation sont conformes au risque (analyses de rentabilité claires pour les investissements liés à la cybersécurité) et sont pris en compte dans la stratégie en matière de cybersécurité.
- ☐ La haute direction fournit un financement adéquat et des ressources suffisantes pour soutenir la mise en œuvre du cadre de cybersécurité de l'organisation.
- ☐ Les gens n'hésitent pas à remettre en question les idées des autres, incluant les personnes en position d'autorité, sans crainte de représailles; les personnes qui font l'objet d'une remise en question réagissent favorablement.

Maturité modérée

- ☐ Le cadre de cybersécurité a une portée interne et ne comporte pas de processus sectoriels.
- ☐ La stratégie et les investissements en matière de cybersécurité ne sont pas harmonisés et ne se soutiennent pas mutuellement.
- ☐ Déséquilibre de l'investissement en matière de sécurité entre les contrôles de base liés à la sécurité et ceux nécessaires pour contrer les attaques plus complexes.
- ☐ La forte sensibilisation aux menaces se concentre sur la protection de l'infrastructure et des applications dans l'ensemble de l'entreprise.
- ☐ Mise en place d'une protection des renseignements fondée sur l'identité.
- ☐ Une surveillance automatisée de la vulnérabilité des actifs informatiques est en place.
- ☐ Aucun mécanisme important n'est mis en œuvre pour prévoir les risques de type « black swan ».

Maturité faible

- ☐ Absence de stratégie, d'initiatives et de plan d'investissement en matière de cybersécurité.
- ☐ Protection de base du réseau seulement ou contrôles traditionnels de la sécurité basée sur la reconnaissance de signature et faible intérêt pour les nouvelles technologies et méthodologies.
- ☐ La vulnérabilité des actifs informatiques est seulement évaluée occasionnellement.
- ☐ Les analyses de rentabilité à l'égard de l'investissement dans la cybersécurité sont rares.

Question

5

Dans quelle mesure nos capacités et notre programme de cybersécurité sont-ils conformes aux normes sectorielles et aux organisations comparables ?

Maturité élevée

- ☐ Un programme complet de cybersécurité fondé sur les normes sectorielles et les meilleures pratiques est en place pour offrir une protection contre les menaces existantes et les détecter, se tenir au courant des nouvelles menaces et permettre une réaction et une reprise rapides des activités.
- ☐ Adoption d'une approche sectorielle pour établir, exploiter, maintenir et améliorer ou adapter des cyberprogrammes.
- ☐ L'organisation a réalisé une étude comparative externe de son programme de cybersécurité.
- ☐ L'organisation vérifie périodiquement à l'interne sa conformité aux politiques, aux normes sectorielles et à la réglementation.
- ☐ L'organisation a officiellement obtenu la certification nécessaire relativement aux secteurs critiques et pertinents de ses activités (p. ex., ISO 27001:2013 certification).

Maturité modérée

- ☐ Un programme de cybersécurité met en œuvre de nombreuses pratiques exemplaires et capacités sectorielles, y compris une surveillance de base de la marque en ligne, des enquêtes informatiques sur les maliciels automatisés et des investigations informatiques manuelles, une surveillance des criminels et des pirates informatiques, un profilage du comportement de l'effectif et des consommateurs et une surveillance multiplateforme ciblée pour les utilisateurs internes.
- ☐ Une vérification de la conformité et d'autres programmes internes peut être effectuée à l'occasion, mais pas systématiquement.

Maturité faible

- ☐ Les mesures de cybersécurité sont ponctuelles et tiennent peu compte des normes et des meilleures pratiques sectorielles.
- ☐ Des examens généraux ponctuels sont parfois effectués pour se conformer aux exigences réglementaires.

Question

6

Avons-nous une mentalité et une culture axées sur la cybersécurité à l'échelle de l'entreprise?

Maturité élevée

- ☐ Grande importance accordée à la cybersécurité par les échelons supérieurs : le conseil d'administration et les hauts dirigeants encouragent la création d'une solide culture de gestion du risque et de durabilité en matière de risques et de rendement.
- ☐ Les intérêts, les valeurs et l'éthique des personnes s'harmonisent à la stratégie, à la tolérance aux risques et à l'approche en matière de cyberrisques de l'organisation.
- ☐ Les dirigeants discutent ouvertement et franchement des cyberrisques en utilisant un vocabulaire commun pour favoriser une compréhension générale.
- ☐ Campagne de sensibilisation et d'information axée sur la cybersécurité à l'échelle de l'entreprise (pour tous les employés, les tiers, les sous-traitants, etc.).
- ☐ Diffusion d'information et de formations propres à chaque description de tâche afin que les employés comprennent leurs responsabilités liées à la cybersécurité.
- ☐ Les gens assument personnellement leurs responsabilités en matière de gestion des risques et font preuve d'initiative en demandant l'aide d'autres personnes lorsqu'il le faut.

Maturité modérée

- ☐ Formation générale et sensibilisation en ce qui a trait à la sécurité de l'information.
- ☐ Sensibilisation ciblée en matière de cybersécurité fondée sur les renseignements, axée sur les risques liés aux actifs et les types de menaces.

Maturité faible

- ☐ Une politique acceptable relative à l'utilisation est mise en œuvre.
- ☐ Peu d'importance est accordée à la cybersécurité à l'extérieur du service des TI.
- ☐ Les problèmes liés à la sensibilisation et aux formations sont traités de manière réactive; les formations ne sont fournies que lorsqu'une infraction à la sécurité ou à la conformité est repérée, et visent seulement un petit groupe de personnes.

Question

7

Que fait la direction pour protéger l'organisation des cyberrisques liés aux tiers?

Maturité élevée

- ☐ Les risques de cybersécurité sont considérés comme un élément à part entière du processus de contrôle diligent pour les accords d'impartition et de sous-traitance essentiels.
- ☐ Tous les tiers participent à un processus uniforme, et des politiques et contrôles (p. ex., droit de vérifier) qui correspondent aux attentes et à la tolérance au risque de l'organisation sont mis en œuvre.
- ☐ Des formations axées sur la cybersécurité sont fournies aux tiers et sont personnalisées en fonction des besoins et des risques pertinents.
- ☐ Le programme de gestion des risques comprend le profilage et l'évaluation de toutes les relations importantes avec des tiers et de tous les flux d'information.
- ☐ Des processus ont été mis en œuvre pour signaler rapidement les incidents de cybersécurité liés aux tiers.
- ☐ Des mesures fondées sur le profilage de tiers et les évaluations des risques sont prises pour atténuer les cyberrisques potentiels liés aux accords d'impartition.

Maturité modérée

- ☐ Des mesures sont prises pour atténuer les cyberrisques potentiels liés aux accords d'impartition.
- ☐ Le contrôle diligent des accords d'impartition et de sous-traitance est encouragé, mais n'est pas appliqué de façon uniforme.
- ☐ Aucune clause contractuelle ne fait référence aux communications de tiers concernant les incidents de cybersécurité.
- ☐ Il existe une certaine corrélation entre les renseignements internes et externes sur les menaces.

Maturité faible

- ☐ Protection de base du réseau seulement.
- ☐ Aucune mesure de protection des cyberrisques ou de contrôle diligent des tiers n'a été mise en œuvre.

Question

8

Pouvons-nous contenir rapidement les dommages liés aux incidents de cybersécurité et mobiliser des ressources d'intervention diversifiées?

Maturité élevée

- ☐ Des processus de signalement et décisionnels clairs sont en place pour les mesures à prendre et les communications à diffuser en cas de failles ou d'accidents de sécurité.
- ☐ Des politiques et des procédures d'intervention en cas d'incidents de cybersécurité sont intégrées dans les plans existants de gestion de la continuité des activités et de reprise après sinistre.
- ☐ Les plans et les procédures en matière de gestion de crises et d'intervention en cas d'incidents de cybersécurité sont documentés et ont été testés dans le cadre de jeux de guerre, de simulations et d'interactions en équipes.
- ☐ Des plans de communication externes sont en place afin d'intervenir en cas d'incidents de cybersécurité touchant des parties prenantes clés.
- ☐ L'organisation participe activement à des simulations sectorielles et à des exercices de formation.

Maturité modérée

- ☐ Des politiques et des procédures d'intervention de base sont mises en œuvre en cas d'incidents de cybersécurité, mais elles ne sont pas intégrées efficacement dans les plans existants de gestion de la continuité des activités et de reprise après sinistre.
- ☐ Le service des TI effectue régulièrement des simulations de cyberattaques.
- ☐ Des exercices de cyberattaques sont organisés de façon intermittente dans l'ensemble de l'entreprise.

Maturité faible

- ☐ Certains exercices de reprise après-sinistre et de continuité des activités informatiques sont organisés.
- ☐ Les politiques, les communications et les plans d'intervention liés aux incidents de cybersécurité sont minimaux ou inexistants.

> « Bien que l'état de cybersécurité d'une organisation dépende de sa taille et de sa maturité, il est important de fixer un niveau de sécurité qui vous permettra de prévoir et de vous défendre contre les menaces les plus courantes et celles émergentes de votre secteur, et de rétablir vos activités après une attaque. »

– Adel Melek, directeur général, Service mondial des risques d'entreprise

Question

9

Comment évaluons-nous l'efficacité du programme de cybersécurité de notre organisation?

Maturité élevée

- ☐ Le conseil d'administration et les hauts dirigeants s'assurent que l'efficacité du programme de cybersécurité est évaluée et que toutes les lacunes repérées sont traitées de façon appropriée, conformément à la tolérance au risque de l'organisation.
- ☐ Le conseil d'administration ou un comité de ce conseil examine régulièrement la mise en œuvre du cadre de cybersécurité de l'organisation ainsi que le caractère adéquat des contrôles d'atténuation existants, et en discute.
- ☐ Des évaluations internes et externes (bilans de santé, tests d'intrusion, etc.) des vulnérabilités sont régulièrement effectuées pour repérer les lacunes au sein des contrôles de cybersécurité appropriés pour le secteur.
- ☐ Les activités de supervision comprennent des évaluations régulières du budget de cybersécurité, de l'impartition des services, des rapports d'incidents, des résultats d'évaluation et des processus d'examen et d'approbation des politiques.
- ☐ L'équipe de vérification interne évalue l'efficacité de la gestion des cyberrisques dans le cadre des examens trimestriels.
- ☐ L'organisation prend le temps nécessaire pour tirer parti des leçons importantes et modifier les aspects liés à la sécurité et à la vigilance de son programme afin de le renforcer.

Maturité modérée

- ☐ Des évaluations de la cybersécurité de base sont effectuées en fonction d'un calendrier fixe; ces évaluations ne se limitent pas à un seul secteur.
- ☐ L'équipe de vérification interne évalue l'efficacité de la gestion des cyberrisques une fois par année au maximum.
- ☐ Afin d'améliorer la cybersécurité, les leçons apprises sont appliquées parfois, mais de façon peu uniforme.

Maturité faible

- ☐ Les évaluations de cybersécurité et les vérifications internes sont peu courantes, voire inexistantes.
- ☐ Les mesures de cybersécurité sont relativement statiques et les améliorations ne sont pas mises à l'essai.

Question
10

Protégeons-nous notre secteur, notre pays et le reste du monde des cyberrisques en adoptant une approche holistique d'échange de connaissances et d'information?

Maturité élevée

- ☐ De solides relations sont établies avec les parties prenantes internes, les partenaires externes, les organismes de réglementation et d'application de la loi, etc.
- ☐ Les initiatives d'échange novatrices qui ne nuisent pas à la sécurité et à la confidentialité de l'information sont soutenues.
- ☐ Des connaissances et de l'information sont échangées avec le secteur, les centres d'analyse indépendants, les organismes gouvernementaux et de collecte de renseignements, les institutions d'enseignement et les cabinets de recherche.
- ☐ Élargissement des activités de mise en commun et des relations pour y inclure les partenaires, les clients et les utilisateurs finaux.
- ☐ Préférence accordée aux fournisseurs qui respectent les normes du secteur et s'adaptent aux récentes avancées en cybersécurité.
- ☐ Maintien de programmes évolués pour éviter de devenir le maillon le plus faible.

Maturité modérée

- ☐ Échange ponctuel d'information sur les menaces avec les entreprises comparables ou collaboration active avec le gouvernement et les acteurs du secteur en ce qui a trait à la collecte d'information liée aux menaces.

Maturité faible

- ☐ Peu de relations externes et aucun échange d'information ou de connaissances avec les entreprises comparables, le gouvernement ou d'autres groupes externes.

> "Lorsque les acteurs des secteurs privé et public prennent les mesures nécessaires pour améliorer leur responsabilisation et leurs compétences, il est possible d'avoir des discussions axées sur la collaboration entre les secteurs et les régions avec plus de confiance et d'expérience."

– World Economic Forum, en collaboration avec Deloitte. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience (juin 2012).

Nous devons tous améliorer notre jeu

Qu'ils soient en période de création ou de refonte, les leaders des risques organisationnels doivent définir leur cible de maturité en matière de cybersécurité. Cette cible doit être établie grâce à une compréhension du contexte d'affaires et des priorités qui y sont liées et à des discussions entre les responsables de la cybersécurité et les décideurs du reste de l'organisation. Bien que toutes les organisations n'aient pas besoin d'atteindre les plus hauts niveaux de maturité dans tous les domaines de cybersécurité, la cible établie doit permettre à l'organisation d'atteindre ses objectifs stratégiques tout en tenant compte du temps et des coûts requis pour y parvenir. Souvent, cette cible permet à l'organisation de viser des niveaux de maturité plus élevés lorsque les pratiques de cybersécurité sont jugées essentielles. Pour élaborer un programme de gestion des cyberrisques évolué et approfondi, il ne suffit pas de dépenser de l'argent différemment; il faut adopter une approche foncièrement différente en investissant dans l'élaboration de capacités en matière de sécurité, de vigilance et de résilience propres à l'organisation afin de créer un programme qui répond à ses besoins uniques.

Où vous situez-vous?

Selon les résultats de votre évaluation, votre niveau de maturité actuel soutient-il votre stratégie et votre mission ou nuit-il à celles-ci? Si votre indice de maturité ne correspond pas à votre cible, ou si vous ne vous êtes pas encore fixé d'objectifs appropriés, le temps est venu d'améliorer l'état de votre cybersécurité. À une ère où les stratégies défensives passent rapidement des solutions d'intervention en cas d'incidents à un concept de protection contre des vulnérabilités inconnues utilisé par les organisations pour prévoir les failles de sécurité et les prévenir avant qu'elles ne se produisent, les entreprises prudentes et responsables ne peuvent pas se permettre d'être à la traîne.

Bien entendu, il n'est pas possible pour une organisation d'être parfaitement sécurisée, mais il est tout à fait possible de gérer et d'atténuer de façon importante l'incidence des cybermenaces, y compris les vols, les pénalités réglementaires, les dédommagements prévus par la loi et l'atteinte à la réputation. En travaillant tous ensemble, nous pouvons minimiser la possibilité croissante des pannes d'infrastructures à grande échelle et des perturbations des activités à l'échelle nationale, voire mondiale.

Communiquez avec l'un de nos leaders pour obtenir plus de renseignements :

Nick Galletto
Leader national
Services liés aux cyberrisques
416-601-6734
ngalletto@deloitte.ca

Marc Mackinnon
Leader national
Sécurité, confidentialité et résilience
416-601-5993
mmackinnon@deloitte.ca

Adel Melek
Directeur général
Service mondial des risques d'entreprise
416-601-6524
amelek@deloitte.ca

En collaboration avec :

Paul D. Milkman
Leader du groupe de la gestion des risques technologiques et de la sécurité de l'information
Groupe Banque TD
paul.milkman@td.com

Cyber Intelligence Centre

www.deloitte.ca/cyber

Conçu et produit par le Service de conception graphique national, Canada 14-2514T