La cybersécurité peut-elle générer de la croissance?

Yogen Appalraju, leader, Cybersécurité, EY Canada

Rapport sur le sondage mondial sur la sécurité de l'information 2021 d'EY : points saillants canadiens

Meilleure la question, meilleure la réponse.
Pour un monde meilleur.

EY

Travailler ensemble
pour un monde meilleur

Bienvenue

Contenu

INTRODUCTION

Les chefs de la sécurité de l'information canadiens à la croisée des chemins

Quelque chose d'imprévu est arrivé pendant la pandémie. Alors que s'effectuait, partout dans le monde, le virage vers un accès et une connectivité à distance sécurisés, les chefs de la sécurité de l'information se sont retrouvés au-devant de la scène.

Dix-huit mois plus tard, ces leaders, et les fonctions cybersécurité, protection des renseignements personnels et gestion des risques, ont une occasion exceptionnelle de se positionner à titre de véritables leviers de croissance stratégique de l'entreprise.

Pourquoi? Les nouveaux cyberrisques se multiplient. Les cybermenaces sont de plus en plus complexes. Les exigences des consommateurs en matière de protection des renseignements personnels évoluent en conséquence. L'innovation prend une place grandissante dans les écosystèmes non traditionnels (comme l'infonuagique 2.0). Ces facteurs combinés mettent en évidence le besoin urgent que les chefs de la sécurité de l'information et la fonction cybersécurité jouent un rôle plus important dans les entreprises canadiennes.

La tâche ne sera pas de tout repos. Selon le tout dernier sondage mondial sur la sécurité de l'information d'EY réalisé en 2021, le cloisonnement des activités empêche l'avancement. Les anciens cadres de gestion des risques doivent être repensés. Les problèmes de communication interne continuent d'accentuer les lacunes en matière de sensibilisation à la valeur de la cybersécurité. Malgré cela, tout est encore possible.

En adoptant la bonne stratégie, les chefs de la sécurité de l'information peuvent transformer les progrès réalisés pendant la crise en collaboration durable, en intégration plus efficace des activités et en relations plus solides afin de générer une valeur à long terme dans un marché transformé.

Les occasions comme celle-là ne se présentent pas deux fois. La saisirez-vous ou la laisserez-vous passer?

Sommaire

Tout changement s'accompagne d'une occasion de transformation. Le sondage mondial sur la sécurité de l'information de 2021 d'EY révèle que les chefs de la sécurité de l'information ont une occasion unique de tirer parti du dynamisme créé au cours des 18 derniers mois pour renforcer leur présence et leur efficacité au sein des entreprises canadiennes.

Ce faisant, ils peuvent améliorer la cybersécurité, et l'ensemble des résultats de l'entreprise, à une époque où la sécurité, la protection des renseignements personnels et la conformité continuent d'être des priorités pour les parties prenantes internes et externes.

Pour ce faire, ils doivent s'appuyer sur les progrès réalisés pendant la pandémie et travailler de concert avec l'équipe de direction pour :

1 DÉCLOISONNER LES ACTIVITÉS DE MANIÈRE À FAVORISER LA CONNECTIVITÉ.

2 ADOPTER DE NOUVELLES APPROCHES DE GESTION DES RISQUES.

3 PROMOUVOIR UN CHANGEMENT DE CULTURE GRÂCE À UNE PLUS GRANDE SENSIBILISATION EN INTERNE.

1 Décloisonner les activités de manière à favoriser la connectivité

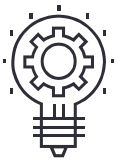
En remaniant l'organigramme et en faisant de la cybersécurité et de la protection des renseignements personnels le fil conducteur entre les capacités des fonctions, votre entreprise ne sera pas seulement plus forte, elle sera également plus efficace, gérera mieux les coûts et fera la promotion d'une collaboration qui permettra de répondre directement aux exigences des parties prenantes internes et externes en matière de sécurité des produits, des services et des solutions.

40 % des dirigeants n'ont jamais été aussi préoccupés par la gestion des cybermenaces.

POURQUOI?

Les risques ne sont plus les mêmes.

Selon les résultats du sondage mondial sur la sécurité de l'information, plus de 40 % des dirigeants n'ont jamais été aussi préoccupés par la gestion des cybermenaces auxquelles leur entreprise fait face. Ce risque disruptif ne peut être atténué que si la connexion entre les équipes fonctionnelles est améliorée.



L'innovation est omniprésente.

Le nuage est désormais le fondement de la nouvelle technologie. Les développeurs créent de nouveaux codes et définissent eux-mêmes le serveur qui les hébergera. Pourtant, dans près de 40 % des entreprises, la relation entre l'équipe de sécurité et celles de développement de produits et de R et D est considérée comme neutre, caractérisée par un faible niveau de consultation, ce qui empêche l'intégration des questions de sécurité et de protection des renseignements personnels dès la conception.

La cybersécurité et la protection des renseignements personnels entrent en jeu trop tard.

De nombreuses entreprises pensent déjà à l'après-infonuagique 2.0 et se concentrent sur la conteneurisation à titre de solution pour les technologies sans serveur et la chaîne de blocs au moyen de l'infonuagique 3.0, mais les ressources de cybersécurité continuent d'être déconnectées du processus de planification. La cybersécurité et la protection des renseignements personnels sont prises en compte dès la phase de planification que dans moins d'un quart seulement des entreprises canadiennes, ce qui peut avoir des répercussions coûteuses et forcer les concepteurs à revenir à leur planche à dessin à la dernière minute, parce qu'elles ont été conçues sans les garanties de sécurité et les paramètres de confidentialité appropriés.

Image 1 : Gérer les cybermenaces

Dans quelle mesure êtes-vous d'accord ou en désaccord avec l'énoncé suivant? : Je n'ai jamais été aussi préoccupé que je le suis maintenant par notre capacité de gérer les cybermenaces avec lesquelles l'entreprise doit composer.

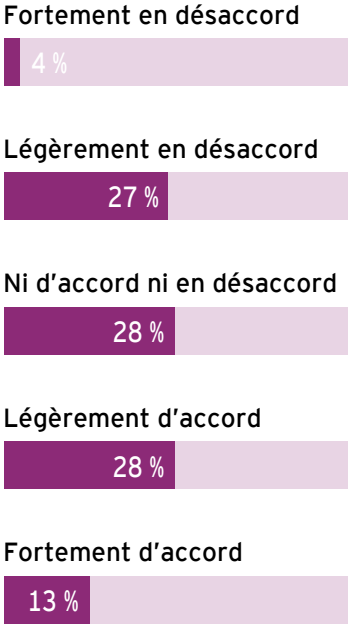
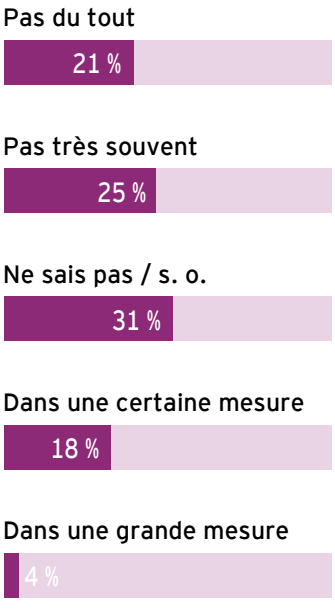


Image 2 : consulter la fonction cybersécurité

La fonction cybersécurité n'est pas consultée ou est consultée trop tard lorsqu'il faut prendre des décisions stratégiques urgentes.



COMMENT LES ENTREPRISES PEUVENT-ELLES AGIR DÈS MAINTENANT?

1 Définir le ton donné par la direction

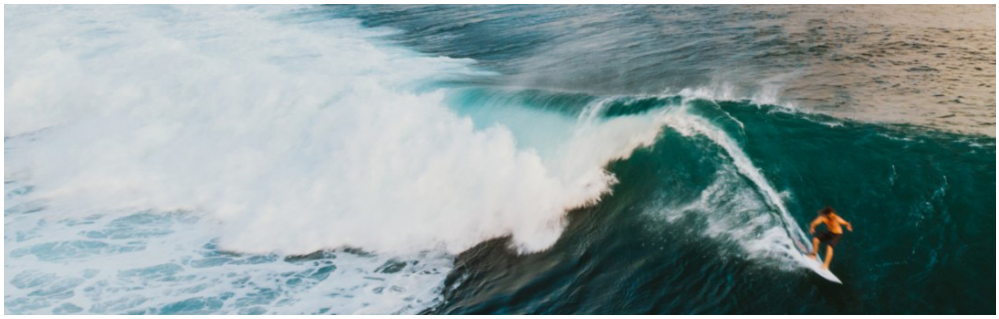
Évaluer les points de connexion entre le chef de la sécurité de l'information et l'équipe de direction élargie pour assurer que les fonctions cybersécurité et protection des renseignements personnels sont présentes aux bonnes tables de décision et que les préoccupations grandissantes et la cybervisibilité sont prises en compte au niveau du conseil d'administration.

2 Échanger les ressources de cybersécurité

Faire participer directement les membres de la fonction cybersécurité au développement des TI, des applications et des affaires et à la conception de produits et autres domaines de l'entreprise pour intégrer plus tôt la réflexion sur la sécurité et la protection des renseignements personnels à la discussion.

3 Redéfinir le cadre de R et D

Redéfinir les processus et les directives de recherche et développement pour inclure une étape de cybersécurité et de protection des renseignements personnels de façon à demander conseil dès le départ à la fonction cybersécurité plutôt que de faire appel à elle tardivement pour les questions de conformité.



“

La croyance populaire selon laquelle “ il n'y a pas de nuage, seulement l'ordinateur de quelqu'un d'autre “ est une approche dépassée et dangereuse d'exploitation des TI et de la cybersécurité modernes. De nos jours, les nouvelles technologies permettent aux entreprises de bénéficier de tout un éventail de services infonuagiques offerts au moyen d'une infrastructure-service, d'une plateforme-service ou d'un logiciel-service, ce qui nécessite un virage majeur dans la manière dont les cyberrisques doivent être gérés.

Amin Lalji
Leader en sécurité infonuagique d'EY Canada

2 Adopter de nouvelles approches de gestion des risques

Les marchés et les organisations évoluent, et les fonctions cybersécurité et protection des renseignements personnels doivent elles aussi redéfinir la manière dont elles fonctionnent. Ces fonctions critiques doivent évaluer de nouvelles méthodes de travail, adopter de nouveaux modèles et repenser les compétences requises pour effectuer un changement majeur et mieux répondre aux besoins et exigences en évolution de l'entreprise, ainsi qu'à ceux des clients et des organismes de réglementation auxquels ces groupes offrent des services.

73 % affirment que la fonction cybersécurité ne favorise pas vraiment l'innovation.

POURQUOI?

Les attentes des organismes de réglementation changent.

La moitié des dirigeants canadiens sont d'avis que la conformité aux exigences actuelles des organismes de réglementation constitue la partie la plus exigeante de leur travail. Quelque 70 % d'entre eux prévoient que la réglementation sera de plus en plus fragmentée, et qu'ils devront consacrer plus de temps et d'efforts pour s'y conformer. En interne, des réponses partielles peuvent saper les efforts et exposer l'entreprise à des risques accrus. En repensant la conformité aux exigences réglementaires du point de vue des risques, les fonctions cybersécurité et protection des renseignements personnels peuvent aller au-delà des seuls changements à la réglementation et bâtir des relations proactives qui bénéficieront à l'entreprise.

L'innovation suit un cycle de plus en plus rapide.

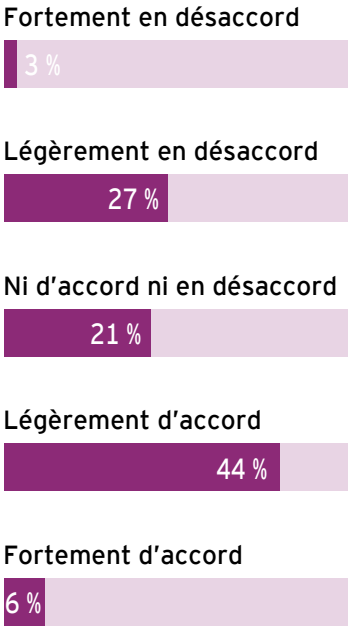
La plupart des dirigeants pensent que la fonction cybersécurité protège leur entreprise, mais 73 % d'entre eux disent que cette fonction ne stimule pas vraiment l'innovation. C'est une occasion manquée. Les cycles de l'innovation sont plus courts que jamais, de sorte que la sécurité et la protection des renseignements personnels sont de plus en plus importantes. En faisant en sorte que les priorités de ces fonctions soient recentrées sur l'innovation ainsi que sur la sécurité et la protection des renseignements personnels, les entreprises peuvent créer des solutions intrinsèquement sécurisées à l'heure où les parties prenantes sont de plus en plus préoccupées par la protection des renseignements personnels dans un milieu des affaires hybride.

Il incombe à chacun de mettre l'entreprise au cœur des priorités.

Seulement 20 % des chefs de la sécurité de l'information sont convaincus d'être sur la même longueur d'onde que les autres chefs de l'entreprise. Mais il existe une véritable logique économique qui plaide en faveur de la contribution des spécialistes en cybersécurité et en protection des renseignements personnels à toutes les unités fonctionnelles. Les entreprises progressistes veulent que la fonction cybersécurité fasse appel à sa créativité pour obtenir de nouveaux produits et de nouvelles solutions numériques et réaliser des initiatives d'amélioration des activités. Lorsque les unités fonctionnelles adoptent des méthodes de travail agiles, la sécurité et la protection des renseignements personnels dès la conception deviennent réalité. Les équipes de cybersécurité doivent également s'adapter pour gérer les risques d'un point de vue commercial pour générer plus efficacement des résultats à l'échelle de l'entreprise.

Image 3 : Assurer la conformité peut être stressant

Dans quelle mesure êtes-vous d'accord ou en désaccord avec l'énoncé suivant sur la réglementation? : Assurer la conformité en vertu de la réglementation d'aujourd'hui peut être la composante la plus stressante de mon travail.



COMMENT LES ENTREPRISES PEUVENT-ELLES AGIR DÈS MAINTENANT?

1 Évaluer les compétences

L'efficacité de la cybersécurité dépend des connaissances des professionnels de cette fonction, lesquels devront acquérir des compétences allant au-delà de l'expertise fondamentale en sécurité et en protection des renseignements personnels pour contribuer davantage.

2 Réaligner le programme de gestion des talents

Le perfectionnement des compétences actuelles pour qu'elles soient mieux adaptées au nouveau visage des fonctions et le recrutement de personnes aux talents diversifiés permettront de redéfinir le rôle de la cybersécurité et de la protection des renseignements personnels, afin de renforcer la valeur de l'entreprise et d'appuyer les alliances interfonctionnelles.

3 Modifier les relations avec les organismes de réglementation

L'élaboration d'une nouvelle approche en matière de relations avec les organismes de réglementation peut permettre à l'ensemble de l'entreprise de garder une longueur d'avance sur le changement. En nourrissant ces relations et en influant sur elles, l'entreprise peut résoudre les problèmes, plutôt que de seulement respecter les politiques.

> “Les règlements en matière de protection des renseignements personnels ne constituent pas uniquement des exigences auxquelles les entreprises doivent se conformer. Ils les rendent responsables de la manière dont les données personnelles sont collectées et traitées et protègent les droits de chacun à sa vie privée. Ils ont comme principal objectif d'aider les entreprises à élaborer des pratiques d'affaires éthiques et à gagner la confiance des consommateurs.

Roobi Alam
Leader, Protection de la vie privée et confiance en matière de données, EY Canada

3 Promouvoir un changement de culture grâce à une plus grande sensibilisation en interne

Le changement n'est percutant que dans la mesure où il peut être géré efficacement. Si vous décloisonnez les activités ou que vous changez la manière dont les fonctions cybersécurité et protection des renseignements personnels exercent leurs activités, l'entreprise doit le savoir. Grâce à l'éducation et à la sensibilisation en interne, les équipes interfonctionnelles se sentent responsables de la protection de renseignements personnels, de la protection des données et de la cybersécurité. Le succès de cette initiative bénéficiera à l'entreprise et à ses parties prenantes, tout en stimulant les résultats.

34 % des équipes de haute direction disent décrire la fonction cybersécurité comme étant flexible et collaborative.

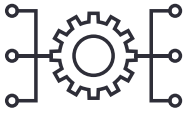
POURQUOI?

Les nouveaux investissements génèrent de nouveaux risques.

Selon notre récent sondage, 45 % des entreprises prévoient faire des investissements importants dans les données et la technologie au cours des 12 prochains mois. Mais moins de 30 % d'entre elles sont d'avis que la cybersécurité est un catalyseur d'innovation. Pour combler cette lacune, il faut sensibiliser les membres du personnel au fait que les capacités et les compétences en matière de sécurité et de protection des renseignements personnels peuvent favoriser les initiatives d'innovation, pour qu'ils envisagent de les acquérir plus tôt dans le processus.

Les entreprises ne savent pas ce qu'elles ignorent.

Seulement 34 % des équipes de direction disent percevoir la fonction cybersécurité comme flexible et collaborative. Il n'est pas utile de renouveler la composition de la fonction cybersécurité si l'entreprise continue de la percevoir et de percevoir ses valeurs de la même manière qu'elle le faisait auparavant. En donnant la possibilité d'apprendre à mieux connaître la fonction, l'entreprise favorise une collaboration fructueuse et l'amélioration de la rentabilité.



Il n'est pas toujours naturel de collaborer.

Un peu plus des deux tiers (68 %) des chefs de la sécurité de l'information disent que l'équipe de direction n'affirmerait pas que la fonction cybersécurité a une très grande sensibilité en affaires. Pour modifier cette perception, les équipes de cybersécurité et de protection des renseignements personnels devront faire la démonstration de ce qu'elles peuvent faire. Il sera possible de rallier les gens en racontant des histoires de réussite en matière d'innovation centrées sur la collaboration interfonctionnelle.

COMMENT LES ENTREPRISES PEUVENT-ELLES AGIR DÈS MAINTENANT?

1 Élaborer un plan de changement

La gestion efficace du changement passe par une planification solide. Élaborez un plan clair de la manière dont vous décloisonnerez les activités et redéfinissez votre approche globale de gestion des risques. Obtenez l'adhésion de l'ensemble des fonctions à l'égard du plan.

2 Se concentrer sur la présentation narrative sur les canaux internes

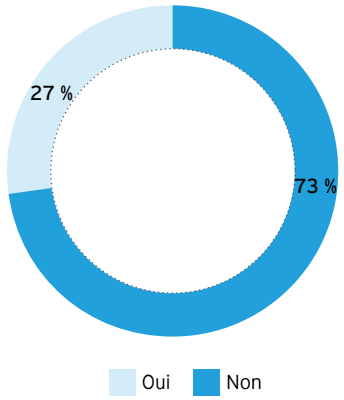
Dans le cadre de la transformation, utilisez les canaux internes pour partager délibérément et systématiquement des présentations qui illustrent le « pourquoi » du changement. Ayez recours à des exemples, à des chiffres et à des résultats pour bâtir une analyse de rentabilité interne et les arguments en faveur de l'adoption de cette nouvelle approche de cybersécurité et de protection des renseignements personnels.

3 Souligner les réussites sans modifier les objectifs

Il faut du temps pour apporter un changement durable. Une solide gouvernance de gestion du changement doit comprendre des méthodes permettant de reconnaître les progrès et les réalisations et de souligner les réussites. Dans le cadre de la transformation, pour motiver les gens, le parcours doit être aussi important que la destination.

Image 4 : Cybersécurité et innovation

À votre avis, lequel des termes suivants utiliserait la haute direction pour décrire le rôle de la fonction cybersécurité au sein de l'organisation? - Favorise l'innovation.



> “Dans une entreprise qui a réussi sa transformation numérique, les fonctions cybersécurité et protection des renseignements personnels ne peuvent se concentrer uniquement sur l'atténuation des risques. En plus de protéger la valeur, elles doivent en générer et l'optimiser. Pour ce faire, elles doivent aller au-delà des paradigmes et des modèles opérationnels traditionnels en mobilisant les unités fonctionnelles pour qu'elles intègrent la cybersécurité et la protection des renseignements personnels à leurs projets dès le départ et en leur offrant de la formation, et en faisant en sorte que ces fonctions cessent d'être seulement des garde-fous et deviennent des fonctions agiles qui exercent leurs activités à titre de véritables partenaires de l'entreprise.

Ali Varshovi
Leader de la cybersécurité du secteur des Services financiers d'EY Canada

Que faut-il en conclure?

Au Canada et dans le monde, les fonctions liées à la sécurité se retrouvent à un point d'inflexion critique. Les entreprises qui saisissent cette occasion pour regrouper la fonction cybersécurité avec les autres unités fonctionnelles démontrent au marché l'importance qu'elles accordent à leur sécurité et à la protection des renseignements personnels. Commencez par décloisonner les activités, adopter une nouvelle perception des risques et favoriser un changement de culture interne significatif. En le faisant dès maintenant, vous incorporez la sécurité et la protection des renseignements personnels dans tout ce que vous faites et vous permettez à votre entreprise de se démarquer de ses concurrentes.

MÉTHODOLOGIE DU SONDAGE

Les données présentées cette année dans le rapport sur le sondage mondial sur la sécurité de l'information sont fondées sur un sondage réalisé auprès des chefs de la sécurité de l'information et autres dirigeants de 1 010 entreprises, dont 71 répondants canadiens, de mars à mai 2021. Les chefs de la sécurité de l'information et hauts dirigeants représentaient 50 % des répondants; les autres étaient des professionnels de la cybersécurité de niveau C1. La plupart des participants ont répondu au téléphone, et une minorité, en ligne.

Communiquez avec nos leaders

MONTRÉAL

Frederic Georgel
frederic.m.georgel@ca.ey.com

Nicola Vizioli
nicola.vizioli@ca.ey.com

TORONTO

Yogen Appalraju
yogen.appalraju@ca.ey.com

Roobi Alam
roobi.alam@ca.ey.com

Omer Arshed
omer.arshed@ca.ey.com

Jason Green
jason.b.green@ca.ey.com

Amin Lalji
amin.lalji@ca.ey.com

Chandra Majumdar
chandra.majumdar@ca.ey.com

Atul Ojha
atul.ojha@ca.ey.com

Bryan Pollitt
bryan.pollitt@ca.ey.com

Esha Ponnappa
esha.ponnappa@ca.ey.com

Bryson Tan
bryson.tan@ca.ey.com

Ali Varshovi
ali.varshovi@ca.ey.com

Ryan Wilson
ryan.wilson@ca.ey.com

OTTAWA

Jamie O'Hare
jamie.ohare@ca.ey.com

CALGARY

Brian Masch
brian.masch@ca.ey.com

VANCOUVER

Simon Wong
simon.y.wong@ca.ey.com

EY | Travailler ensemble pour un monde meilleur

La raison d'être d'EY est de bâtir un monde meilleur, de créer de la valeur à long terme pour les clients, les gens et la société, et de renforcer la confiance à l'égard des marchés financiers.

S'appuyant sur les données et la technologie, les équipes diversifiées d'EY présentes dans plus de 150 pays instaurent la confiance au moyen de la certification, et aident les clients à prospérer, à se transformer et à exercer leurs activités.

Que ce soit dans les services de certification, de consultation, de stratégie, de fiscalité ou de transactions, ou encore, au sein des services juridiques, les équipes d'EY posent de meilleures questions pour trouver de nouvelles réponses aux enjeux complexes du monde d'aujourd'hui.

387692
DE 0000

ey.com/ca/fr