Points saillants pour le Canada

EY
Travailler ensemble
pour un monde meilleur

Cybersécurité : quelles mesures de protection devrait prendre votre entreprise pour mieux se protéger contre les cyberrisques?

21e sondage mondial d'EY sur la sécurité de l'information 2018-2019

Points saillants pour le Canada

Selon le sondage mondial d'EY sur la sécurité de l'information (GISS), 70 % des répondants canadiens ont augmenté leur budget lié à la cybersécurité au cours des 12 derniers mois, tandis que 91 % affirment qu'ils y consacreront davantage de ressources dans l'année qui vient.

Même si les organisations canadiennes considèrent que les menaces à la sécurité informatique sont une réalité, les budgets qui y sont consacrés demeurent peu élevés comparativement au budget global des TI. En fait, 63 % des répondants déclarent que les dépenses totales en sécurité de l'information représentent moins de 10 % du budget TI général.

Ceci intervient dans un contexte de modification réglementaire. En 2018, le monde a été témoin de l'entrée en vigueur du Règlement général sur la protection des données (RGPD) en Europe, un cadre réglementaire qui renforce la protection des renseignements personnels et qui impose des obligations aux contrôleurs et aux processeurs de données personnelles. Le RGPD a eu une incidence sur d'autres territoires, et le Canada a annoncé des changements à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) qui entreront en vigueur le 1er novembre 2018 et rendront obligatoire la notification des atteintes à la protection des données dans certaines circonstances.

Le Canada est en voie de devenir un des pôles d'innovation technologique de premier plan à l'échelle mondiale. Afin de protéger l'économie canadienne des menaces dans le monde cybernétique, le gouvernement fédéral a récemment lancé la Stratégie nationale de cybersécurité qui précise les mesures à prendre pour réduire les risques. Grâce à cette stratégie, le Canada a trouvé un moyen d'établir un équilibre entre l'innovation et la protection des données.

Yogen Appalraju
Associé, EY Canada
Leader, Cybersécurité – Canada

La conformité à l'égard de la protection des données et les risques liés à la réputation

Les renseignements les plus précieux pour les cybercriminels sont :

1. les renseignements personnels permettant l'identification des clients et les mots de passe;
2. l'information financière et les plans stratégiques;
3. les données personnelles des hauts dirigeants et des administrateurs.

Il en ressort deux préoccupations particulières : la conformité à l'égard de la protection des données et les risques liés à la réputation.

Les organisations canadiennes et internationales ont raison de faire de ces questions une priorité. La réglementation en matière de protection des renseignements personnels répond aux nouveaux besoins de la société numérisée et renforce des mécanismes visant à rendre les organisations responsables de leurs décisions à l'égard du traitement des renseignements personnels pouvant mener à l'identification de personnes. Les organisations qui ne protègent pas les données personnelles peuvent encourir des pénalités importantes. En outre, la déclaration d'une atteinte à la protection des données pourrait grandement nuire à leur réputation.

Les sociétés canadiennes sont de plus en plus nombreuses à reconnaître l'importance des stratégies relatives à la cybersécurité et à la protection des renseignements personnels, mais elles continuent à être plus réactives que proactives. La protection et la sécurité des renseignements personnels doivent être mises en œuvre et opérationnelles dans toutes les organisations, pas uniquement pour se conformer à la réglementation comme le RGDP, mais en raison des avantages que ces cadres présentent. Définir des contrôles aux premiers stades de la conception des systèmes d'information et des processus renforcerait non seulement la conformité, mais réduirait significativement les risques et les coûts.

Même si les entreprises canadiennes sont préoccupées par le grand intérêt des cybercriminels pour les données personnelles, 64 % des répondants disent ne pas avoir de programme de protection des données ou avoir seulement un programme informel. Les organisations canadiennes devraient commencer à s'inquiéter de la protection des données et s'attacher à définir de manière proactive des mécanismes pour permettre des contrôles efficaces de la cybersécurité et de la confidentialité des données.

58 %

des répondants canadiens affirment que la sécurité de l'information a peu ou pas d'influence sur la stratégie ou le plan d'affaires.

64 %

des répondants canadiens ont déclaré ne pas avoir de programme de protection des données ou en avoir un qui soit informel.

Le facteur humain

Les trois plus importantes vulnérabilités au cours des 12 derniers mois :

1. Des employés négligents ou ignorants (39 %)
2. Des contrôles ou une architecture de sécurité de l'information obsolètes (24 %)
3. Des accès non autorisés (11 %)

35 % des répondants considèrent l'hameçonnage comme la principale menace des 12 derniers mois.

Selon 27 % des répondants canadiens, la cause la plus probable d'une cyberattaque est un employé négligent. Au moment où les entreprises étendent leur empreinte numérique, 36 % des répondants mentionnent le comportement et la faible sensibilisation des utilisateurs comme le principal risque lié à l'utilisation croissante des appareils mobiles.

Les personnes restent le maillon faible de la cybersécurité. Pour établir une stratégie de prévention de la menace qui soit efficace, les organisations doivent offrir de la formation sur la cybersécurité qui soit efficiente afin de s'assurer que les employés sont en mesure de détecter et de prévenir les menaces à la cybersécurité.

La surveillance par le conseil d'administration

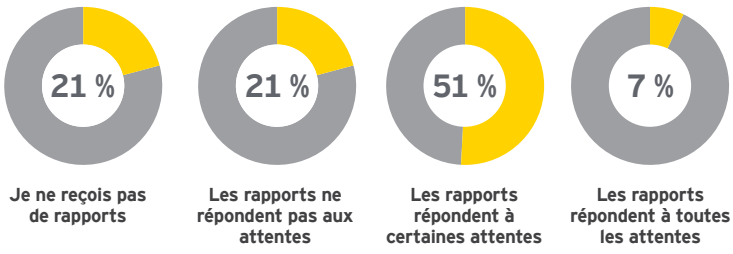
68 %

des répondants canadiens disent que la personne qui a la responsabilité directe de la sécurité de l'information n'est pas membre du conseil ou de la haute direction.

Seulement 16 %

des répondants affirment que le conseil a une compréhension exhaustive de la sécurité de l'information qui permet de bien évaluer les cyberrisques qui guettent leurs organisations et de prendre les mesures adéquates.

Rapports sur l'efficacité de la sécurité de l'information de l'organisation :



Déceler les menaces à la cybersécurité et y réagir est un enjeu commercial qui fait d'une formation en profondeur en matière de cybersécurité un impératif pour les membres du conseil d'administration. Afin de prendre les bonnes décisions et d'élaborer des contre-mesures efficaces, les membres du conseil doivent pleinement comprendre les risques et les défis liés à la cybersécurité auxquels est confrontée l'organisation et ils doivent savoir comment réagir aux menaces de manière efficiente et en mesurer les succès.

Peut-on se servir du numérique pour favoriser le progrès?

Les faits ont démontré que les organisations tendent à être plus réactives que proactives lorsqu'il s'agit de concevoir un programme de cybersécurité.

91 % des répondants canadiens disent que le budget de sécurité de l'information serait augmenté après la constatation d'une violation ayant une incidence sur l'organisation.

Depuis le début des années 2000, les organisations investissent de plus en plus dans les TI. En comparaison, les investissements ont été beaucoup moins élevés en cybersécurité. Cette lacune en matière de sécurité illustre bien que les investissements dans les TI se font sans que l'on tienne bien compte des risques de cybersécurité.

Selon le Baromètre de la croissance d'EY, 86 % des répondants ont l'intention d'adopter l'intelligence artificielle (IA) au cours des sept prochaines années. Bien que l'adoption de technologies émergentes comme l'IA puisse améliorer les processus d'affaires avec le temps, elle pourrait également exposer les entreprises à de nouveaux risques. La réussite des entreprises dépendra de la manière dont elles répondront à ces risques, de leur volonté d'accroître les budgets pour remédier aux lacunes en matière de sécurité et de l'efficacité de leurs programmes de protection des données et renseignements personnels.

La résilience

Les sociétés canadiennes reconnaissent l'importance d'avoir une équipe spécialisée dédiée à la cybersécurité. Ainsi, 72 % des répondants canadiens affirment avoir un Centre des opérations de sécurité et 27 % disent que c'est grâce à ce centre qu'ils ont constaté l'incident de cybersécurité d'importance le plus récent. Les entreprises canadiennes estiment également faire preuve d'une grande maturité dans la gestion d'incident, la mise en place de cadre de politiques et de normes, et l'adoption de stratégie en matière de cybersécurité. Cependant, lorsqu'il est question d'infrastructure de données, de gestion des risques liés à des tiers et de disponibilité de programmes spécialisés de cybersécurité, elles ont besoin de s'améliorer grandement :

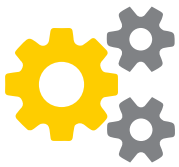
67 %
n'ont pas de programme de **renseignements sur les menaces** ou n'ont qu'un programme informel.

45 %
n'ont pas de programme de **détection des vulnérabilités** ou n'ont qu'un programme informel.

52 %
n'ont pas de programme de **détection des violations** ou n'ont qu'un programme informel.

31 %
n'ont pas de programme d'**intervention en cas d'incident** ou n'ont qu'un programme informel.

44 %
n'ont pas de programme de **gestion de l'identité et des contrôles d'accès** ou n'ont qu'un programme informel.



Seulement 13 % **des répondants déclarent faire preuve d'excellence en matière de gestion de crise.**

Bien des organisations l'ont appris, parfois à leurs dépens : la question n'est pas de savoir si une cyberattaque va se produire, mais à quel moment elle se produira. La prévention et la dissuasion ne suffisent pas. Les sociétés doivent savoir réagir aux incidents liés à la cybersécurité et y répondre, assurer la reprise des activités et maintenir la sécurité. Autrement dit, les organisations doivent faire preuve de résilience.

Pour ce faire, les sociétés doivent tenir à jour leur stratégie de reprise après sinistre et de poursuite des activités. Il est tout aussi important pour les organisations de mettre en place des plans robustes de gestion des incidents et des crises et de les mettre à l'épreuve régulièrement au moyen d'exercices de simulation auxquels participent des employés et des dirigeants afin de veiller à leur préparation dans l'éventualité d'une cyberattaque.

Les cybermenaces constituent l'un des principaux risques pour les entreprises. Bâtir la cyberrésilience pourrait avoir la plus grande incidence sur la gestion de ce risque et devrait être prioritaire.

Conclusion

83 % des répondants canadiens déclarent que la fonction de sécurité de l'information répond partiellement aux besoins organisationnels et prévoient l'améliorer.

Les organisations canadiennes comprennent qu'il est nécessaire de porter une attention particulière aux programmes de cybersécurité. Elles font le constat que les connaissances des membres du conseil sur les questions de cybersécurité sont limitées et formulent l'intention de consacrer un budget plus important à la cybersécurité. On peut y voir le reflet d'une collectivité qui s'engage pour améliorer la cyberrésilience dans un contexte où les gouvernements offrent du soutien et les organisations innovent.

Le manque de ressources compétentes fait partie des défis pour l'élaboration d'une fonction de cybersécurité aboutie au Canada et à l'échelle mondiale. Or, il faut se réjouir du fait que de nombreux collèges et universités du Canada développent des programmes et des laboratoires de cybersécurité et de protection des renseignements personnels qui contribueront à élargir le bassin de cybertalents et à fournir une main-d'œuvre capable de suivre le rythme soutenu des cyberrisques. La gestion de la cybersécurité ne cesse d'évoluer et aucune organisation ne peut anticiper toutes les menaces qui surviendront. Toutefois, en faisant de la cybersécurité une partie importante de la culture d'entreprise, en prenant les mesures nécessaires pour devenir cyberrésilient et en investissant de manière judicieuse dans un programme proactif en cybersécurité, même les risques qui sont invisibles aux organisations peuvent être minimisés.

Principaux résultats du sondage canadien

83 %
déclarent que leur fonction de sécurité de l'information répond partiellement aux besoins de l'organisation.

27 %
estiment qu'un employé négligent est la source la plus probable d'une cyberattaque.

28 %
ne disposent pas d'un Centre des opérations de sécurité, même si ces centres deviennent de plus en plus courants.

16 %
des conseils possèdent des connaissances en sécurité de l'information qui sont suffisantes pour bien évaluer les cyberrisques.

20 %
indiquent qu'il est peu probable qu'ils soient en mesure de détecter une cyberattaque complexe.

35 %
considèrent l'hameçonnage comme la principale menace des 12 derniers mois.

67 %
n'ont pas de programme de renseignements sur les menaces ou n'ont qu'un programme informel.

89 %
disent avoir besoin de financement supplémentaire pour protéger leur organisation.

63 %
disent que le budget lié à la cybersécurité est inférieur à 10 % de l'ensemble du budget des TI.

Personnes-ressources d'Ernst & Young s.r.l./s.e.n.c.r.l.

Pour discuter de votre stratégie en matière de cybersécurité, n'hésitez pas à communiquer avec nous :

Toronto

Yogen Appalraju
Associé, leader
Cybersécurité – Canada
yogen.appalraju@ca.ey.com
+1 416 932 5902

Thomas Davies
Associé délégué, Cybersécurité
thomas.davies@ca.ey.com
+1 416 943 2013

Bryson Tan
Associé délégué, Cybersécurité
bryson.tan@ca.ey.com
+1 416 943 3925

Ryan Wilson
Associé délégué, Cybersécurité
ryan.wilson@ca.ey.com
+1 416 943 7170

Carlos Perez Chalico
Chef d'équipe senior
Cybersécurité
carlos.perez.chalico@ca.ey.com
+1 416 943 5338

Calgary

Brian Masch
Associé délégué, leader
Cybersécurité – Ouest du Canada
brian.masch@ca.ey.com
+1 403 206 5096

Vitaly Sokolov
Associé délégué, Cybersécurité
vitaly.sokolov@ca.ey.com
+1 403 206 5150

Montréal

Adam Sultan
Chef d'équipe senior
Cybersécurité
adam.sultan@ca.ey.com
+1 514 879 2826

EY | Certification | Fiscalité | Services transactionnels | Services consultatifs

À propos d'EY
EY est un chef de file mondial des services de certification, services de fiscalité, services transactionnels et services consultatifs. Les points de vue et les services de qualité que nous offrons contribuent à renforcer la confiance envers les marchés financiers et les diverses économies du monde. Nous formons des leaders exceptionnels, qui unissent leurs forces pour assurer le respect de nos engagements envers toutes nos parties prenantes. Ce faisant, nous jouons un rôle crucial en travaillant ensemble à bâtir un monde meilleur pour nos gens, nos clients et nos collectivités.

EY désigne l'organisation mondiale des sociétés membres d'Ernst & Young Global Limited, lesquelles sont toutes des entités juridiques distinctes, et peut désigner une ou plusieurs de ces sociétés membres. Ernst & Young Global Limited, société à responsabilité limitée par garanties du Royaume-Uni, ne fournit aucun service aux clients. Pour en savoir davantage sur notre organisation, visitez le site ey.com/ca/fr.

À propos des Services consultatifs d'EY
À une ère de changements sans précédent, les Services consultatifs d'EY sont convaincus que travailler pour un monde meilleur signifie d'aider les clients à résoudre des enjeux sectoriels importants et complexes et à saisir les occasions en vue de favoriser la croissance, l'optimisation et la protection de leurs entreprises.

Que leurs clients soient des hauts dirigeants ou des leaders fonctionnels de multinationales figurant au palmarès Fortune 100, des entreprises novatrices qui ne font rien comme les autres ou des petites ou moyennes entreprises des marchés émergents, les Services consultatifs d'EY font équipe avec eux, de l'élaboration de la stratégie à son exécution, afin de les aider à cibler de meilleurs résultats qui s'avéreront durables.

Une perspective mondiale et une culture axée sur la diversité et la collaboration incitent les conseillers d'EY à poser de meilleures questions. Ils collaborent avec leurs clients ainsi qu'avec un réseau d'experts internes et externes pour élaborer des réponses novatrices. Ensemble, EY aide les entreprises de leurs clients à devenir meilleures.

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

2875070

DE00

ey.com/ca/cybersecurity