Le rôle du comité d'audit face aux cyberrisques en évolution

Le comité d'audit joue un rôle central pour guider la direction dans un contexte où les cybercriminels misent sur de nouveaux outils.

L'intensification des attaques basées sur l'intelligence artificielle (IA) a amené la cybersécurité au-delà du domaine des technologies de l'information, devenant un enjeu central de confiance, de réputation et de gouvernance. Selon notre plus récent sondage annuel *Perspective des chefs de la direction* [1], la cybersécurité demeure une préoccupation majeure pour les chefs de la direction canadiens. Bien que la plupart des organisations reconnaissent l'importance de la cybersécurité, les comités d'audit ont un rôle central à jouer dans la surveillance et l'orientation des pratiques en matière de cybersécurité.

> « La plupart des organisations investissent dans la cybersécurité, mais beaucoup n'ont pas de programme à cet effet. Les comités d'audit peuvent aider la direction à élaborer et à mettre en œuvre un plan adaptable et évolutif en matière de cybersécurité et de reprise des activités.

Alexander Rau
Associé, Services-conseils, Cybersécurité, KPMG au Canada

Le contexte des menaces évolue

Les auteurs de cybermenaces sont tellement occupés qu'ils ne prennent plus de pause comme avant et utilisent des agents conversationnels alimentés par l'IA pour gérer les négociations entourant leurs attaques de routine par rançongiciel. Ils deviennent également plus agressifs et demandent des rançons plus élevées, des tactiques qui portent leurs fruits et encouragent encore plus la criminalité.

Dans notre sondage *Perspective des chefs de la direction en 2025*, 97 % des chefs de la direction canadiens ont exprimé des préoccupations au sujet de la fraude, du vol d'identité et des cyberattaques[2]. Au cours de la prochaine année, les attaques par rançongiciel devraient demeurer élevées, en partie en raison d'une augmentation du pourcentage des organisations ciblées qui paient la rançon. En effet, les auteurs des menaces ciblent les petites et moyennes entreprises (PME) qui décident qu'elles ne peuvent pas se permettre les temps d'arrêt qui accompagnent le long processus de négociation et de récupération des données.

[1] KPMG au Canada, « La productivité sous la loupe », consulté le 15 octobre 2025.
[2] KPMG au Canada, « Le leadership face à l'adversité », consulté le 15 octobre 2025.

Les organisations n'ont pas toutes mis en place les contrôles de sécurité adéquats, et c'est pourquoi il est impératif qu'elles disposent d'un plan d'intervention en cas d'attaque par rançongiciel ou d'autres intrusions. Le comité d'audit peut apporter des perspectives utiles en demandant à la direction dans quels cas elle paierait une rançon, quel montant elle serait prête à payer, qui serait chargé de prendre les décisions pendant un incident, et de quelle façon l'organisation prévoit de reprendre ses activités à la suite d'une attaque. Le comité d'audit devrait également s'assurer que la direction a une stratégie claire pour communiquer de façon transparente avec les clients touchés, les organismes de réglementation et les autres parties prenantes, de façon à maintenir la confiance et à montrer qu'elle assume ses responsabilités.

Les fraudes du président devraient également demeurer une grave menace. Cette escroquerie se produit lorsqu'un cybercriminel s'infiltre dans le système de courriel d'une organisation, se fait passer pour un membre de la direction, et demande à un autre membre du personnel de lui fournir des renseignements sensibles ou de lui faire un virement direct à son insu. Ces stratagèmes sont devenus beaucoup plus efficaces avec l'IA, qui est utilisée pour rendre les courriels d'hameçonnage plus difficiles à détecter. Les cybercriminels peuvent même ajouter une touche personnelle en faisant suivre leurs courriels d'un appel téléphonique, de plus en plus souvent au moyen d'une voix générée par l'IA qui imite la personne qu'ils prétendent être.

Malgré les outils technologiques avancés dont se servent les cybercriminels, l'approche traditionnelle consistant à former les employés à des pratiques de cybersécurité appropriées demeure un outil important pour prévenir ces attaques. Les comités d'audit devraient s'assurer que la direction offre une formation continue sur la cybersécurité à l'échelle de l'organisation qui traite des menaces actuelles ainsi que des procédures d'atténuation et de signalement.

Questions que les comités d'audit devraient poser

- Quel est notre plan en cas d'attaque par rançongiciel?
- Quelle formation offrons-nous à notre personnel?
- Comment atténuons-nous le risque lié aux tiers?
- Qui est responsable de la cybersécurité?
- Comment évaluons-nous l'efficacité de nos mesures de cybersécurité?

Les assureurs scrutent le sujet

À mesure que les niveaux de menace et le montant des paiements augmentent, les sociétés de cyberassurance se montrent plus rigoureuses dans l'évaluation des demandes de règlement. En 2025, un assureur a refusé la réclamation d'une organisation canadienne qui avait subi une cyberattaque majeure. L'assureur a fait valoir que l'organisation ciblée n'avait pas mis en œuvre l'authentification multifacteur exigée dans sa police d'assurance et que cette défaillance avait joué un rôle déterminant dans la perpétration de l'attaque. À la suite de ce refus, l'organisation a été tenue de dépenser plusieurs millions de dollars.

Il est essentiel que les organisations soient en mesure de se décharger du risque lié aux cyberincidents, car les coûts peuvent être suffisamment élevés pour menacer leur survie. Les comités d'audit devraient s'assurer que la direction connaît bien les clauses de la police d'assurance, notamment ce qui est couvert et à quelle hauteur. La direction doit également bien comprendre les limites, les exclusions et les conditions de la couverture, et s'assurer que la société se conforme aux exigences énoncées dans la police. Il peut être utile de simuler divers scénarios d'attaque, et d'évaluer ce qui serait couvert par la police et si la couverture serait valide au regard des pratiques actuelles de l'organisation en matière de cyberdéfense.

Les comités d'audit doivent surveiller les exigences réglementaires

Les organisations devraient se conformer à tous les règlements applicables, au minimum. Au cours de la dernière année, la réglementation a évolué au Canada et dans l'Union européenne (UE). Ces nouveautés entraîneront de nouvelles obligations de déclaration et influeront sur la façon dont les organisations élaborent leurs programmes de cybersécurité. Par exemple, la directive de l'UE sur les réseaux et la sécurité de l'information (SRI 2) impose la gouvernance des cyberrisques, la gestion des risques et des obligations de déclaration à certaines organisations européennes. Elle devait entrer entièrement en vigueur en 2025, mais son déploiement a été inégal parmi les pays membres.

Au Canada, le projet de loi C-8 a été déposé en juin 2025. S'il est adopté, il s'appliquera aux organisations qui exercent leurs activités dans des secteurs essentiels comme les services financiers, les télécommunications, les services publics et les transports, ce qui obligera ces organisations à élaborer et à mettre en œuvre un programme de cybersécurité devant être soumis à un examen annuel. Il exigera également que les organisations visées signalent les incidents de cybersécurité au Centre canadien pour la cybersécurité (CCSC) dans les 72 heures. Il permettra en outre au gouvernement d'émettre des ordonnances juridiquement contraignantes pour que les organisations prennent des mesures spécifiques liées à la cybersécurité, et imposera des pénalités importantes en cas de non-conformité.

Les comités d'audit doivent se tenir au courant des nouveautés réglementaires à l'échelle mondiale et s'assurer que la direction prend les mesures appropriées pour surveiller les nouvelles réglementations, déterminer si elles visent l'organisation et s'y conformer, le cas échéant. Les comités d'audit de la plupart des organisations bien établies comptent parmi leurs membres des personnes ayant de l'expérience en cybersécurité, mais bon nombre d'organisations pourraient tout de même bénéficier d'un processus officiel et continu permettant au comité d'audit de faire le suivi des nouveautés et des changements réglementaires.

À cet égard, la communication entre les organisations, principalement par l'intermédiaire des organismes sectoriels, est une nouvelle source d'échange d'informations. Grâce à cette coopération, les organisations peuvent échanger des renseignements sur les nouvelles menaces, les mesures d'atténuation et la réglementation. Les comités d'audit pourraient déterminer avec la direction s'il s'agit d'une avenue utile à explorer, si l'organisation n'y participe pas déjà.

Les comités d'audit peuvent orienter les organisations vers un programme de cybersécurité évolutif

Il ne suffit pas de respecter les normes et les règlements. Un programme de cybersécurité doit être axé sur les risques et tenir compte de tous les cyberrisques potentiels, en les abordant par ordre de priorité pour l'organisation. Les comités d'audit, qui exercent une surveillance étendue de ces risques et de leur importance pour l'organisation, peuvent fournir des conseils éclairés en interrogeant la direction sur son plan de cybersécurité. Le comité d'audit peut aussi contribuer à façonner les pratiques de cybersécurité et exercer son influence au sein de l'organisation au moyen de l'audit interne, qui peut tenir la direction responsable du programme de cybersécurité.

La plupart des organisations ont beaucoup investi dans la cybersécurité, mais un grand nombre ne parvient pas à mettre en œuvre un véritable programme de cybersécurité. Le comité d'audit devrait s'assurer que la direction a élaboré un programme qui évolue et s'adapte continuellement pour répondre à l'évolution de la réglementation, des menaces, des cybercriminels et des technologies. Ce plan devrait comprendre une structure de gouvernance bien définie indiquant clairement quels services et quelles personnes sont responsables de la cybersécurité, et décrivant les mesures à prendre pour tester et évaluer l'efficacité du programme. Le comité devrait également s'assurer que la direction ne se contente pas de suivre les règlements ou les menaces les plus récents ou les plus médiatisés au détriment de la gestion continue d'autres risques. Les organisations doivent continuer à couvrir les éléments fondamentaux, comme la mise en place de correctifs de routine, tout en s'attaquant aux nouveaux risques.

Ironiquement, le succès passé d'un programme de cybersécurité peut entraver son succès futur. Comme des programmes de cybersécurité efficaces préviendront les attaques et atténueront les dommages causés par celles qui passent entre les mailles de leur filet, les organisations risquent de commencer à croire que les cybermenaces ne sont pas si graves et ne pas consacrer suffisamment de ressources au maintien d'un programme de cybersécurité robuste.

À une époque où les cybermenaces évoluent rapidement et où les exigences réglementaires s'intensifient, les comités d'audit doivent dépasser la simple conformité et remettre activement en question le degré de préparation de la direction en matière de cybersécurité, s'assurer de la mise en place de plans d'intervention rigoureux en cas d'incident, et plaider en faveur d'un investissement continu dans la cybersécurité. En jouant un rôle proactif, les comités d'audit peuvent aider leur organisation à demeurer résiliente et prête à faire face aux menaces de demain.

Contactez-nous

Alexander Rau

Associé, Services-conseils, Cybersécurité,
KPMG au Canada
alexanderrau@kpmg.ca

kpmg.com/ca/audit-fr