Le rôle du conseil d'administration dans la gouvernance en matière de cyberrisques

Intégration de la cybersécurité à la stratégie d'entreprise

Le contexte des cybermenaces évolue constamment, tout comme les attentes et les obligations du conseil d'administration. En tant que premier responsable de la stratégie, du rendement et de la réputation de l'organisation, le conseil d'administration joue un rôle crucial dans la surveillance et l'orientation de la gestion des risques liés à la cybersécurité.

La cybersécurité doit être perçue comme faisant partie d'un cadre plus large de gouvernance des données qui tient compte de la protection des renseignements personnels et de l'intelligence artificielle (IA). Il est essentiel de comprendre quelles données sont recueillies, comment elles sont utilisées par les gens et les technologies d'IA, et comment elles sont protégées.

Le conseil d'administration devrait exiger des rapports réguliers sur les risques liés à la cybersécurité et sur l'efficacité du programme de l'entreprise à ce chapitre. Cela favoriserait le suivi de la situation de l'organisation en matière de cybersécurité et faciliterait la prise de décisions éclairées.

Les administrateurs doivent s'assurer que la direction intègre les risques liés à la cybersécurité dans sa stratégie et prend les mesures appropriées pour gérer ces risques, tout en améliorant l'agilité de l'organisation et sa capacité à se remettre rapidement d'une cyberattaque.

En outre, le conseil d'administration doit avoir la certitude que les préoccupations en matière de réglementation sont abordées et que l'organisation respecte toutes les lois pertinentes.

> **« Les administrateurs devraient voir la gestion des cyberrisques non pas comme un projet ponctuel ou un ensemble de questions, mais plutôt comme l'occasion d'assurer une surveillance globale et continue. Ainsi, ils peuvent veiller à ce que la direction ait mis en place une stratégie à l'égard des cyberrisques holistique et évolutive, adaptée aux objectifs d'exploitation et axée sur la valeur à long terme de l'organisation; un investissement pour son avenir.**
>
> ***— John Heaton Associé, Cybersécurité, KPMG au Canada***

Éléments à prendre en considération en 2024:

01

La Securities and Exchange Commission a adopté de nouvelles règles qui exigeront davantage d'information en matière de cybersécurité de la part des sociétés ouvertes cotées aux États-Unis à compter de décembre 2023. Celles-ci devront déclarer tout incident important survenu dans les quatre jours ouvrables suivants.

De plus, elles seront tenues de divulguer, dans le cadre de leur rapport annuel, des renseignements relatifs à la gestion des risques et à la gouvernance liée à la cybersécurité.

02

Le secteur de la cybersécurité continue de faire face à une pénurie de talents, ce qui a une incidence sur le recrutement et la fidélisation. Les rôles qui engendrent un niveau de stress élevé peuvent causer de la fatigue et de l'épuisement. Le conseil d'administration devrait combler cet écart en fournissant des ressources et en s'assurant que la direction se penche sur la planification de la relève.

03

L'IA générative offre de nouvelles occasions, mais aussi de nouveaux risques. Il incombe aux conseils d'administration d'assurer l'utilisation sécuritaire et éthique de cette technologie. Les organisations s'en serviront pour pallier la pénurie de talents, tandis que les cybercriminels l'utiliseront pour améliorer leurs tentatives d'hameçonnage et de fraude.

04

La résilience est une question de plus en plus importante, car même les meilleurs systèmes de sécurité ne peuvent garantir une protection absolue. Les mesures de résilience assurent la continuité des opérations même en cas d'attaque réussie. Les capacités d'intervention et de reprise sont plus importantes que jamais.

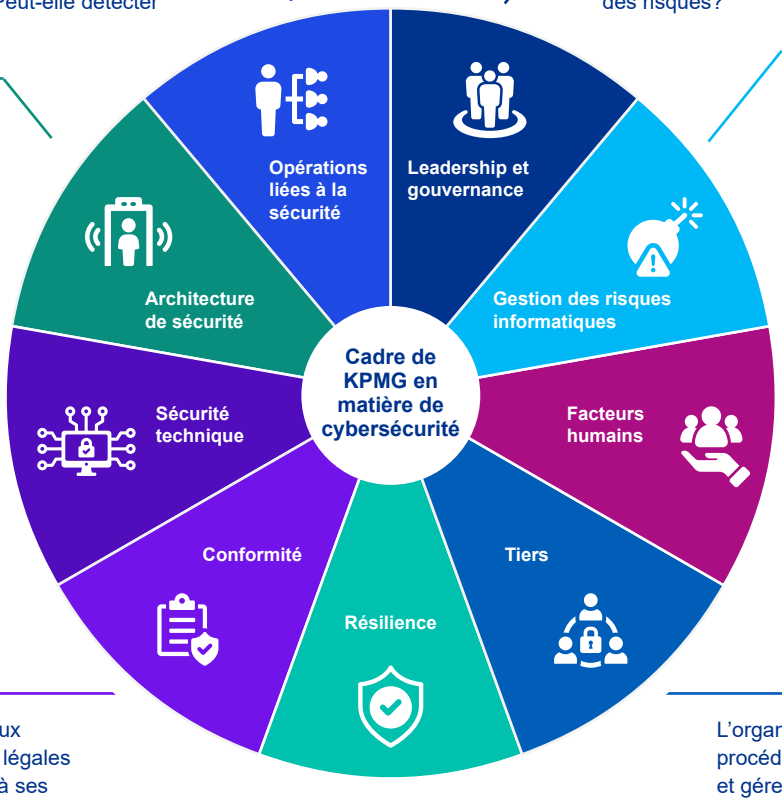
Principales questions que le conseil d'administration devrait poser au sujet des cyberrisques

L'organisation dispose-t-elle de procédures et de contrôles qui protègent les données importantes et réduisent au minimum la probabilité d'une atteinte à la cybersécurité? Peut-elle détecter une atteinte potentielle?

L'organisation a-t-elle désigné un dirigeant qualifié responsable de la cybersécurité? Y a-t-il une équipe en place pour appuyer la détection et l'atténuation des risques?

Les systèmes et processus d'information de l'organisation concordent-ils avec ses objectifs d'exploitation?

L'organisation détermine-t-elle quelles sont ses données critiques et établit-elle des priorités? Sait-elle où sont stockées ces données?



L'organisation a-t-elle élaboré des solutions de sécurité technique pertinentes pour faire face aux cyberrisques détectés?

L'organisation forme-t-elle son personnel relativement aux cyberrisques, comme l'hameçonnage? Surveille-t-elle les menaces internes?

L'organisation se conforme-t-elle aux diverses exigences contractuelles, légales et réglementaires qui s'appliquent à ses données critiques?

L'organisation a-t-elle mis en place des procédures et des contrôles pour repérer et gérer les cyberrisques dans l'ensemble du cycle de vie d'un fournisseur?

L'organisation effectue-t-elle régulièrement des tests de ses plans de gestion de crise et d'intervention afin de s'assurer qu'elle est prête à faire face à des atteintes à la cybersécurité et à minimiser leur incidence?

Compte tenu de l'importance stratégique de cet enjeu, la surveillance doit incomber au conseil d'administration.

Comme pour tout ce qui a trait à la gestion des risques au sein du conseil d'administration, il est évident que la formation des administrateurs est essentielle pour veiller à ce que tous soient au fait de la question. De plus, chaque conseil d'administration doit déterminer s'il est formé, ou veut se doter, d'administrateurs avec un savoir-faire en cybersécurité, et s'il devra faire appel à des spécialistes externes.

Nous joindre

Pour en savoir plus, communiquez avec :

John Heaton
Associé, Cybersécurité,
KPMG au Canada

(416) 476- 2758
johnheaton@kpmg.ca

Adil Palsetia
Associé, Cybersécurité,
KPMG au Canada

(416) 777 8958
apalsetia@kpmg.ca