Rôle du comité d'audit dans la cybervigilance

Les comités d'audit jouent un rôle central dans la cybersécurité

Par John Heaton

La cybersécurité est un processus, et pas seulement un projet, et les comités d'audit ont un rôle à jouer dans l'ensemble du processus : s'assurer que la direction repère continuellement les données critiques et les menaces qui pèsent sur ces données, qu'elle les protège et qu'elle dispose d'une planification en cas de violations.

Identifier les données clés et comprendre les vulnérabilités

Une cybersécurité efficace commence par la compréhension du flux des données de l'organisation et l'identification claire de ses données et systèmes essentiels. La direction doit déterminer les données, les droits de propriété intellectuelle et les renseignements personnels que les clients et les fournisseurs échangent avec l'organisation, ainsi que les obligations relatives à la protection de ces données. Les comités d'audit doivent s'assurer que la direction dispose d'un processus d'identification des données essentielles en interne et dans l'ensemble de la chaîne d'approvisionnement numérique de l'organisation.

La direction doit également identifier les vulnérabilités de la chaîne d'approvisionnement numérique et comprendre toute incidence potentielle sur l'organisation. Il s'agit de repérer les personnes qui ont accès aux données les plus sensibles de l'organisation et les contrôles qui ont été mis en place par les tiers pour les protéger. Le comité d'audit devrait interroger la direction sur la certification par un tiers de la protection des données et des systèmes tant en interne qu'à l'échelle de la chaîne d'approvisionnement.

> La compréhension de votre flux de données et l'identification claire de vos données et de vos systèmes essentiels sont à la base de toute cybersécurité. Il est essentiel que la direction et les comités d'audit identifient les vulnérabilités, protègent ces données et repèrent les règlements applicables.

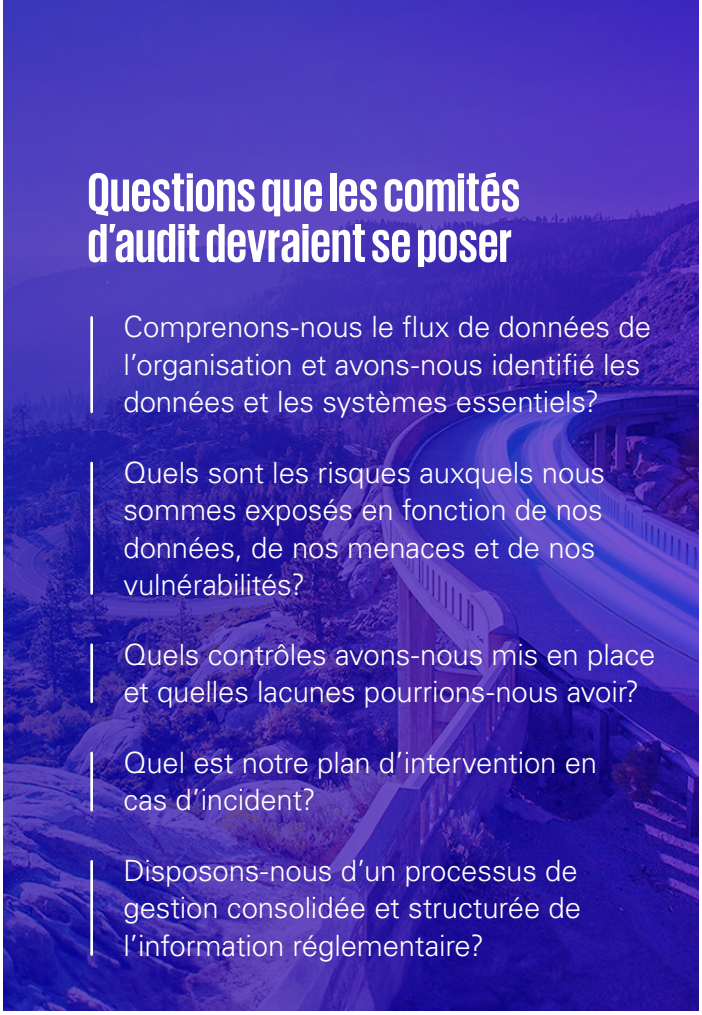
John Heaton
Associé, Services-conseils
KPMG au Canada

Idéalement, la certification viendra d'une validation officielle par un tiers, comme la certification ISO 27001 ou un rapport SOC 2. Les petites entreprises qui ne sont pas en mesure de fournir cette certification ou ce rapport pourraient devoir faire l'objet d'une évaluation par les auditeurs internes de l'organisation. De plus en plus, les entreprises adoptent une approche de certification continue en matière de surveillance de tiers et utilisent des outils pour repérer les atteintes à la sécurité par les fournisseurs.

Surveiller le contexte des menaces

Le comité d'audit devrait être informé du contexte des menaces et interroger la direction sur ses processus de surveillance et d'identification des vulnérabilités. Les auteurs de menaces qui ciblent des organisations sont principalement des cybercriminels qui se servent de rançongiciels pour extorquer de l'argent ou des États-nations ciblant des secteurs d'activité pour effectuer des missions de reconnaissance ou mettre hors service des infrastructures essentielles. Les organisations doivent surveiller les menaces qui pèsent à la fois sur la technologie opérationnelle et sur les TI, puisque cette technologie peut permettre d'accéder aux TI et qu'elle a été efficacement utilisée par les États-nations pour attaquer les infrastructures.

Les cybercriminels innovent continuellement. Par exemple, ils ont mis au point des techniques d'obtention des codes d'accès à usage unique pour l'authentification multifactorielle, et ils utilisent l'IA générative pour améliorer leurs attaques. Ils persécutent également leurs cibles. Par conséquent, les organisations doivent garder une longueur d'avance sur les cybercriminels potentiels.



Questions que les comités d'audit devraient se poser

- Comprenons-nous le flux de données de l'organisation et avons-nous identifié les données et les systèmes essentiels?
- Quels sont les risques auxquels nous sommes exposés en fonction de nos données, de nos menaces et de nos vulnérabilités?
- Quels contrôles avons-nous mis en place et quelles lacunes pourrions-nous avoir?
- Quel est notre plan d'intervention en cas d'incident?
- Disposons-nous d'un processus de gestion consolidée et structurée de l'information réglementaire?

Établir un plan

Le comité d'audit devrait s'assurer que la direction peut clairement expliquer son plan en cas de cyberincident. En plus des risques opérationnels, le cabinet pourrait faire face à d'importants risques liés à la réputation et à la réglementation. Pour atténuer ces risques, un cadre supérieur clairement désigné devrait être responsable de la communication avec les organismes de réglementation de la protection des renseignements personnels et des finances, les organismes d'application de la loi, les personnes touchées et, dans la plupart des cas, les médias avec des communications préparées.

Les organisations mettent en pratique leurs processus d'intervention en matière de cybersécurité en recourant à des exercices de simulation de cyberattaque pour améliorer leur capacité à réagir aux cyberincidents. Il s'agit essentiellement de cyberexercices où les participants appliquent les réponses prescrites à une menace, puis en font le point. Les entreprises utilisent aussi l'IA et l'apprentissage machine pour surveiller les attaques ou les activités inhabituelles et pour réagir plus rapidement. Par exemple, si un ordinateur portable est compromis, il peut être automatiquement mis en quarantaine et l'utilisateur peut être avisé.

Se remettre d'une attaque peut s'avérer plus difficile pour les entreprises que pour les TI. Il y a souvent des redondances et des sauvegardes dans le service informatique. Mais, pour assurer la reprise du secteur des affaires, il faut valider les données touchées et s'assurer qu'elles sont toujours exactes, intégrées et rapprochées. Il s'agira peut-être de s'assurer que les prix, les comptes fournisseurs et les registres de paiement sont à jour, et de déterminer le moment où la dernière transaction a été validée et l'endroit où récupérer les données nécessaires pour exécuter de nouveau les opérations manquantes. Puisque les TI n'y peuvent rien pour ces activités commerciales, le comité d'audit devra donc s'assurer que des processus opérationnels sont en place pour rétablir l'intégrité des données à la suite d'un cyberincident.

Signaler les incidents

Habituellement, les cyberincidents sont signalés au comité d'audit en priorité. Par exemple, une attaque par rançongiciel contre le système d'information financière serait signalée immédiatement, tandis qu'une infection dans l'ordinateur portable d'un employé pourrait être signalée trimestriellement. Certains incidents devront être signalés aux gouvernements et aux organismes de réglementation, et le comité d'audit voudra examiner la déclaration avant de l'envoyer.

Les comités d'audit devraient interroger la direction sur les exigences de déclaration concernant ses activités et ses bureaux, et sur le processus mis en place pour les gérer de façon structurée et consolidée. Là encore, il faut dresser un inventaire des données de l'organisation pour savoir quels sont les règlements applicables à l'organisation.

Le comité d'audit doit veiller à ce que la direction surveille également les nouveaux règlements et s'y prépare. Par exemple, à partir de décembre 2023, la Securities and Exchange Commission (SEC) des États-Unis exigera que les émetteurs inscrits et les émetteurs privés étrangers signalent les incidents de cybersécurité importants et rendent compte annuellement de leur gestion des risques de cybersécurité, de leur stratégie et de leur gouvernance [1].

Au Canada, le projet de loi C-26, *Loi sur la protection des cybersystèmes essentiels*, a été déposé le 14 juin 2022 [2]. Bien que cette loi ne soit pas encore en vigueur, elle est conçue pour s'appliquer aux secteurs « essentiels à la sécurité nationale ou à la sécurité publique », et elle imposera des exigences en matière de rapport à ces organisations [3].

1. « SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies », Washington D.C., 26 juillet 2023
2. Projet de loi C-26, *Loi concernant la cybersécurité*, modifiant la *Loi sur les télécommunications* et apportant des modifications corrélatives à d'autres lois, première session, quarante-quatrième législature, 70-71 Elizabeth II, 2021-2022
3. Projet de loi C-26.

Intégrer la cybersécurité à l'entreprise

La cyberstratégie doit être alignée sur l'entreprise et ne pas fonctionner isolément. L'équipe de cybersécurité doit participer au processus de planification des activités. Il est impératif que les clients et les autres parties prenantes aient confiance dans les nouvelles solutions et les nouveaux processus, et l'équipe de cybersécurité peut contribuer à assurer leur sécurité si elle participe au processus de conception et de mise en œuvre dès le début. Le comité d'audit doit interroger la direction sur la façon dont elle prévoit de s'assurer que la confiance est intégrée dans les nouvelles solutions et les nouveaux processus.

La cybersécurité est un risque majeur pour les organisations, qui fait partie de nombreux aspects à surveiller par les comités d'audit. C'est pourquoi l'équipe de cybersécurité et le comité d'audit doivent se concentrer sur les « actifs numériques névralgiques ». Tout comme l'approche du contrôle interne à l'égard de l'information financière (« CIIF »), il est important de se concentrer sur les systèmes et données les plus critiques, et non sur toutes les applications. Pour plus d'efficacité, les discussions avec la direction doivent porter sur les risques et l'atténuation des risques, et non sur les aspects techniques des attaques et de la protection.

La cybersécurité est un processus continu, et les comités d'audit ont un rôle à y jouer afin de s'assurer que la direction identifie et protège les données clés, qu'elle regarde vers l'avenir et qu'elle s'adapte au contexte des menaces en évolution.

Communiquez avec nous

John Heaton
Associé, Services-conseils
KPMG au Canada
416-476-2758
johnheaton@kpmg.ca

Francis Beaudoin
Associé et leader national,
Services-conseils en technologie
514-840-2247
fbeaudoin@kpmg.ca

Yassir Bellout
Associé, Services-conseils,
Cybersécurité, Montréal
514-840-2546
ybellout@kpmg.ca

Jean-Francois De Rico
Associé, Services Conseils –
Risques technologiques
418-577-3442
jderico@kpmg.ca

Guillaume Clément
Associé, Services en
cybersécurité, KPMG et Président
de KPMG Egyde Conseils
418-653-5335
guillaumeclement@kpmg.ca

Cédric Thibault
Associé, Cybersécurité et
Sécurité infonuagique
418-653-5335
cedricthibault@kpmg.ca

Guillaume Neron
Associé, Services-conseils,
Gestion des risques, Cybersécurité
514-275-1916
gneron@kpmg.ca

Samuel Bonneau
Associé, Services-conseils,
Gestion des risques, Cybersécurité
418- 577-3468
samuelbonneau@kpmg.ca