Les comités d'audit doivent miser sur les occasions en interne pour lutter contre les cybermenaces

La protection contre les cyberattaques passe tout d'abord par l'analyse des processus, des contrôles et des partenaires d'une organisation

Par Hartaj Nijjar

Les actes de piratage et les brèches de sécurité peuvent coûter cher, compromettre la réputation d'une société et ouvrir la voie à des litiges, ce qui fait de la cybersécurité l'un des enjeux les plus pressants auxquels les organisations sont actuellement confrontées. Les sociétés doivent mettre en place une cyberstratégie pour protéger à la fois leurs activités et les données de leurs clients. Les comités d'audit, qui surveillent la performance de la société et bon nombre de ses activités, doivent être certains que la direction se tient au courant de l'évolution de l'ensemble des menaces et qu'elle a mis en place de solides stratégies pour identifier et atténuer les risques.

Les cybermenaces évoluent constamment

Dans le dernier sondage *Perspectives des chefs de la direction* mené par KPMG, 85 % des chefs de la direction canadiens déclaraient qu'il est essentiel d'instaurer une solide stratégie de cybersécurité pour bâtir la confiance de leurs principales parties prenantes. Il est toutefois difficile d'instaurer une telle stratégie, étant donné que les menaces évoluent en permanence. On observe une hausse des actes de piratage touchant les appareils mobiles, mais aussi l'implication d'États-nations dans de tels actes et dans l'utilisation d'hypertrucages à des fins politiques. Par ailleurs, les cybercriminels vendent des solutions clés en main à certains acteurs à l'origine de menaces moins à l'aise avec la technologie pour qu'ils aient accès à des organisations et causent des dégâts.

Au vu des turbulences actuelles sur la scène géopolitique, les organisations accordent une plus grande attention aux menaces potentielles qui pèsent sur leur technologie opérationnelle et aux retombées que des attaques dirigées contre des infrastructures essentielles pourraient avoir sur leurs propres activités et au-delà.

> Les comités d'audit doivent s'assurer que la direction se tient au courant de l'évolution de l'ensemble des menaces et qu'elle a mis en place de solides stratégies pour identifier et atténuer les risques.

Hartaj Nijjar
Associé, Cybersécurité
KPMG au Canada

Les autorités de réglementation régissent l'utilisation des renseignements personnels

Une évolution majeure ayant cours actuellement à l'échelle mondiale ne représente pas nécessairement une nouvelle menace, mais bien un nouvel environnement réglementaire. Dans le sillage de ce mouvement mondial, et sous l'impulsion de textes réglementaires comme le *Règlement général sur la protection des données* (« RGPD ») en Europe, Québec a présenté son projet de loi no 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. La première série d'exigences a été mise en œuvre le 22 septembre 2022, et les exigences suivantes le seront en 2023 et 2024.

Le projet de loi no 64 s'applique aux sociétés établies au Québec ainsi qu'aux sociétés d'autres juridictions qui exercent des activités au Québec et qui recueillent, traitent ou détiennent des renseignements personnels concernant des résidents du Québec. Il oblige les sociétés à être plus rigoureuses et plus transparentes dans le cadre de leurs pratiques en matière de données à caractère personnel en fixant de nouvelles règles concernant notamment la déclaration des atteintes à la protection des renseignements personnels, les responsables de la protection des renseignements personnels, le consentement et l'anonymisation des données. Les comités d'audit voudront interroger la direction au sujet des répercussions de ce projet de loi sur leur organisation et s'assurer qu'il existe un plan pour s'y conformer.

Les organisations devraient également considérer cette loi québécoise comme un baromètre. Des lois similaires seront probablement adoptées à l'échelle pancanadienne et, à en croire les premières informations données par d'autres juridictions, les amendes pour non-respect de la législation pourraient être élevées. En plus de satisfaire aux obligations réglementaires, les organisations devraient se servir de ce nouveau projet de loi comme d'un catalyseur pour revoir leurs pratiques en matière de données et de protection de la vie privée.

Questions que les comités d'audit devraient poser :

- Dans quelle mesure notre stratégie en matière de protection des données est-elle rigoureuse et suffisante, compte tenu de la multiplication de la réglementation?
- De quelle façon recherchons-nous les angles morts?
- Comment effectuons-nous des vérifications auprès des tiers et des autres parties, et comment nous assurons nous qu'ils se conforment à nos exigences de façon continue?
- De quelle manière protégeons-nous nos processus automatisés, et comment vérifions-nous que les robots que nous utilisons dans l'ensemble de la société n'ont pas été manipulés?

L'une des premières étapes consiste à déterminer quelles données doivent être recueillies. Elles devront également examiner la façon dont elles recueillent les renseignements et l'endroit où est stocké, au sein de l'organisation, l'ensemble des données permettant d'identifier une personne, y compris le stockage structuré et non structuré. Elles doivent également veiller à disposer de contrôles d'accès adéquats et à mettre en œuvre des procédures et des processus afin suivre et de tracer les données.

Pour ce faire, il convient d'examiner le cycle de vie des données, de leur intégration à leur destruction, et de s'assurer que les contrôles encadrent les données à chaque fois qu'elles entrent en contact

avec l'organisation. Si les données sont stockées ailleurs, il peut être nécessaire d'effectuer un audit des contrôles des tiers et d'autres parties. Les grandes organisations disposent probablement de nombreux systèmes de contrôle distribués. Dans ce cas, l'objectif devrait être de centraliser autant que possible les contrôles à l'échelle de l'entreprise, ce qui faciliterait l'application d'un ensemble standard de contrôles.

Cette initiative nécessitera beaucoup de ressources et de temps. Cependant, les plus grands obstacles auxquels la plupart des entreprises seront confrontées sont l'orientation des investissements nécessaires et le recrutement des talents adéquats. Les comités d'audit devraient interroger la direction au sujet de leurs contrôles en matière de données et de protection de la vie privée, et s'assurer que la société affecte des ressources suffisantes à la mise en œuvre de ces mesures et à l'embauche des talents nécessaires.

Les organisations sont à la recherche des angles morts

Les sociétés doivent aussi consacrer des ressources à la recherche des angles morts. Il s'agit d'événements connus sous le nom de « cygnes noirs » auxquels ils n'ont pas encore pensé. À titre d'exemple, les interruptions des services infonuagiques et de télécommunications qui ont récemment fait les manchettes ont perturbé les activités d'un grand nombre de clients. Ces interruptions ont incité les organisations à s'interroger sur les éventuels angles morts qui pourraient affecter leurs activités, et à renforcer leur résilience pour veiller à être capables de résister au prochain événement.

Il ne s'agit pas d'une science exacte. L'exercice consiste à réfléchir aux catastrophes potentielles et à imaginer de quelle façon elles pourraient perturber l'organisation, et à quel niveau. Il convient de commencer par les processus les plus critiques, en les retraçant du début à la fin, et en examinant les interconnexions avec les personnes, les processus, les infrastructures et les applications. L'objectif est d'identifier les points où un problème pourrait survenir (en interne ou à l'externe), de mettre en place des contrôles à ces points, puis de créer des plans de sécurité en cas de défaillance de ces contrôles. Les comités d'audit voudront interroger la direction sur ce que fait la société pour identifier les événements perturbateurs potentiels et sur les plans de résilience mis en place pour atténuer les risques.

Les risques liés aux tiers sont à l'ordre du jour

La recherche d'angles morts est rendue indispensable par le fait que toutes les organisations dépendent de tiers relativement à leurs services ou à leurs données. Cette dépendance les expose au risque d'interruptions de service des tiers, qui pourrait affecter des services essentiels. Elle les expose en outre au risque qu'une cyberviolation au sein de leur chaîne de valeur s'étende à l'organisation. L'identification et la gestion des risques liés aux tiers et à d'autres parties figurent à l'ordre du jour de la plupart des conseils d'administration et des comités d'audit.

Habituellement, il est demandé aux fournisseurs de remplir des questionnaires au sujet de leurs contrôles et de leurs pratiques en matière de protection des données et de signer des contrats en vertu desquels ils s'engagent à maintenir un certain nombre de mesures de protection et de contrôles. Il est toutefois difficile, dispendieux et chronophage de vérifier les pratiques des tiers, et rien ne garantit que les

fournisseurs vérifient à leur tour les pratiques de leurs propres tiers, ce qui les expose à des risques, tout comme votre organisation.

L'audit s'automatise

Il existe un fort désir d'automatisation pour les organisations qui cherchent à accroître leur efficience ou à réaffecter leurs employés à des fonctions de plus grande valeur. De plus en plus, l'automatisation sert à surveiller les opérations et l'exécution des contrôles, ce qui signifie que les comités d'audit doivent comprendre les raisons qui poussent la direction à avoir confiance en l'efficacité de ces contrôles automatisés; ceux-ci doivent donc avoir été mis en place adéquatement et être exploités efficacement.

La fonction d'audit a aussi recours à l'automatisation. Les audits nécessitent beaucoup de temps et de main-d'œuvre. Par conséquent, les équipes d'audit se tournent vers l'automatisation pour évaluer continuellement les sous-ensembles de contrôles (plutôt que de sélectionner des échantillons de certaines périodes au cours de l'exercice). Cela permet aux équipes d'audit d'améliorer la qualité et de se concentrer sur les évaluations des contrôles plus complexes.

Bien que l'automatisation dans ces domaines aide à réaliser des gains d'efficience, elle ajoute également de nouvelles cibles pour les cyberattaques potentielles. Les comités d'audit doivent s'assurer que la direction comprenne bien la façon dont les robots sont utilisés au sein de la société et qu'elle est capable de percevoir les signes de manipulations potentielles.

L'élaboration d'une solide cyberstratégie commence souvent par l'analyse des processus, des contrôles et des partenaires de l'organisation. Les comités d'audit qui cherchent à être rassurés à l'égard de la cybersécurité et de la protection de la vie privée voudront être certains que la direction a examiné ses processus de bout en bout, qu'elle a identifié les secteurs de vulnérabilité potentielle et qu'elle a mis en place des plans de contrôle.

Découvrez la série Accélération

Communiquez avec nous

Hartaj Nijjar
Associé, Cybersécurité
KPMG au Canada
416-228-7007
hnijjar@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

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

Cédric Thibault
Associé
418 653-5335
cedricthibault@kpmg.ca

Pascal Fortin
Associé, Services-conseils, Gestion
des risques, Cybersécurité Conseils
514-840-2102
pfortin@kpmg.ca