13 septembre 2023

La gestion des cyberrisques est un enjeu fondamental pour les universités, les organismes publics et d'autres organisations. Le vérificateur général de la Colombie-Britannique a récemment publié un rapport de vérification dans lequel il a conclu que le conseil des gouverneurs d'une université n'avait pas adéquatement contrôlé les pratiques de gestion des risques de cybersécurité. Ce rapport est source d'indications utiles pour les conseils universitaires et autres conseils d'administration publics, en Colombie-Britannique comme ailleurs au Canada.

Contexte

Les cyberrisques, soit les risques de pertes, notamment financières, et de responsabilités auxquels une organisation est exposée à la suite d'un incident et qui sont susceptibles de nuire à ses systèmes informatiques ou à la confidentialité, l'intégrité ou la disponibilité de ses données – constituent un risque critique pour les organisations. Selon *l'Évaluation des cybermenaces nationales 2023-2024 du Centre canadien pour la cybersécurité*, les attaques par rançongiciel sont une menace constante pour les organisations canadiennes.

Chaque université canadienne doit faire de la cybersécurité une priorité. Nombre d'entre elles ont été victimes d'attaques au rançongiciel médiatisées ayant causé perturbations de services, pertes de données sensibles (dont des renseignements personnels) et atteinte à la réputation. Qui plus est, le rôle des universités dans la recherche fait d'elles des cibles de choix pour l'espionnage et le vol de propriété intellectuelle, notamment aux mains d'acteurs parrainés par des États. À cette menace se conjugue un défi inédit : les réseaux de technologies de l'information des universités sont fortement étalés, ce qui en complexifie la protection, et les normes culturelles et de gouvernance collégiale universitaires peuvent entraver l'adoption de pratiques de cybersécurité robustes.

En général, le conseil des gouverneurs d'une université est globalement responsable de la gestion, de l'administration et du contrôle des biens, des revenus, des entreprises et des affaires de celle-ci, ce qui, dans les faits, lui impose de superviser les décisions et activités de la direction universitaire. Cela l'oblige donc à participer activement aux activités de gestion des risques de cybersécurité de l'université, de même qu'à s'assurer que la direction a mis en œuvre des politiques et des pratiques appropriées pour gérer les cyberrisques et réagir aux incidents de cybersécurité.

Le rapport du vérificateur général

Le vérificateur général de la Colombie-Britannique, un agent indépendant de l'Assemblée législative provinciale, a pour mandat de soumettre des entités publiques à des vérifications pour informer la population et les élus de la façon dont leur gouvernement s'acquitte de ses responsabilités et administre ses ressources. En août 2023, le vérificateur général a publié le rapport d'une vérification des pratiques de contrôle de la cybersécurité du conseil des gouverneurs de l'Université Vancouver Island (UVI), une université publique régie par l'*University Act* de la Colombie-Britannique, dont le campus principal se trouve à Nanaimo, et qui compte 12 200 étudiants et un conseil des gouverneurs de 15 membres. Le rapport justifie la sélection de la UVI du fait que celle-ci [traduction] « est de taille similaire à plusieurs autres universités de Colombie-Britannique ».

Dans la vidéo YouTube annonçant le rapport, le vérificateur général explique que dans un contexte de hausse des attaques de cybersécurité, le conseil des gouverneurs de chaque université [traduction] « joue un rôle critique dans le contrôle de la gestion des risques de cybersécurité. Il évalue les stratégies de protection des systèmes de TI et des données personnelles, pour lesquelles il demande des comptes à la direction universitaire ». Le rapport du vérificateur général détaille les rôles de la direction et du conseil des gouverneurs de l'UVI. La direction est chargée d'évaluer les risques, d'appliquer les mesures d'atténuation et de rendre compte au conseil de l'état des programmes de gestion des risques. Quant au conseil, il doit contrôler la gestion des risques de cybersécurité en évaluant si la direction : (1) dispose de politiques et de procédures de sécurité à jour; (2) évalue et contrôle régulièrement les risques de cybersécurité; et (3) reçoit des rapports réguliers sur la situation de l'établissement en matière de cybersécurité.

Le vérificateur général a constaté que le conseil des gouverneurs de l'UVI avait défini des rôles et des responsabilités pour la supervision de la gestion des risques et qu'il avait fixé des attentes à l'égard de la direction quant à l'amélioration de la gestion des risques de l'organisation, y compris en matière de cybersécurité. Cependant, il a également constaté que le conseil n'avait pas adéquatement supervisé les pratiques de gestion des risques de cybersécurité de l'UVI. Le rapport présente les conclusions suivantes :

1. Le conseil a défini des rôles et des responsabilités pour la supervision, mais les politiques étaient désuètes et la rétroaction, non documentée.

Le vérificateur général a cherché à voir si l'UVI avait établi et documenté des rôles et responsabilités pour le contrôle de la gestion des risques de cybersécurité par le conseil au moyen de politiques de gestion des risques et de gouvernance, qui prévoyaient notamment d'évaluer si la présidence répond aux attentes de gestion des risques de cybersécurité.

Or, il a constaté que la politique de gestion des risques était désuète. En dépit d'une révision prévue pour 2017, le conseil l'avait révisée et approuvée pour la dernière fois en 2012. Il avait révisé une version de la politique mise à jour en 2023, sans toutefois l'approuver officiellement.

Le vérificateur général a également constaté que le conseil avait fixé des cibles de cybersécurité pour la présidence, et qu'il avait évalué son rendement en regard des objectifs chaque trimestre – sans toutefois documenter la rétroaction qui en ressortait.

2. Le conseil n'était pas adéquatement encadré ou formé pour superviser la gestion des risques de cybersécurité.

Le vérificateur général a cherché à savoir si l'UVI disposait d'un programme d'orientation pour le conseil qui traitait explicitement de ses responsabilités de gestion des risques de cybersécurité, de même qu'un programme de formation annuel pour ses membres visant à accroître leurs connaissances sur des secteurs de risque – dont la cybersécurité – pour leur permettre de mieux s'acquitter de leurs responsabilités de supervision ou de naviguer des changements au rôle de supervision du conseil.

Le vérificateur a constaté des lacunes à ces deux égards à l'UVI. Même s'il traitait de gestion des risques et faisait mention de la cybersécurité, le programme d'orientation du conseil était muet sur ses responsabilités en matière de surveillance de la gestion des risques de cybersécurité. De plus, le conseil n'était pas doté d'un programme de formation annuel permettant de se tenir à jour sur les secteurs de risque importants, comme la gestion des risques de cybersécurité, contrairement aux exigences de la politique de gouvernance de l'UVI.

3. Même si l'UVI disposait d'un cadre de gestion des risques documenté, le conseil n'évaluait pas en temps opportun les stratégies d'atténuation des risques de la direction.

Le vérificateur général a cherché à savoir si le conseil se penchait régulièrement sur les évaluations de risques de cybersécurité de la direction – et notamment sur la façon dont cette dernière jauge et atténue ces risques –, de même que s'il priorisait les secteurs de risque et documentait les mesures d'atténuation et leurs résultats. Il a également demandé au conseil de confirmer que la direction avait évalué la conformité aux exigences légales et réglementaires.

Le vérificateur général a constaté que le conseil avait évalué le cadre de gestion des risques de cybersécurité de l'UVI, de même que confirmé que le cadre et les politiques avaient été communiqués au personnel, aux étudiants et à d'autres groupes clés. Toutefois, il a également constaté que le conseil avait été trop lent à s'acquitter de ses responsabilités de supervision : même si la direction avait défini la cybersécurité comme un secteur de risque prioritaire en juin 2022, le conseil ne s'est penché sur son plan d'évaluation et d'atténuation des risques qu'en mars 2023. Comme en fait état le rapport : [traduction] « Le conseil doit exiger de la direction qu'elle prévoie des stratégies d'atténuation des risques de cybersécurité tout au long de l'année pour aider à assurer l'évaluation continue des mesures qu'elle prend en réponse à ces risques. »

Le rapport résume les quatre recommandations du vérificateur général :

- Veiller à l'évaluation et l'approbation, dans les délais impartis, des documents de gouvernance et de politique définissant des rôles et responsabilités en matière de gestion des risques de cybersécurité.
- Créer un programme de formation annuel et veiller à ce que les membres du conseil reçoivent chaque année une formation sur la gestion des risques de cybersécurité leur permettant de mieux remplir leur rôle de supervision.
- Mettre à jour le programme d'orientation du conseil en y ajoutant de l'information sur les rôles et responsabilités relatifs à la supervision de la gestion des risques de cybersécurité.
- Réviser chaque année les stratégies d'atténuation des risques de cybersécurité.

Le rapport indique que l'UVI a accepté toutes ces recommandations.

Autres indications utiles

Le rapport du vérificateur général s'inscrit dans un corpus croissant d'orientations émises par des entités publiques, des organismes de réglementation et des instances officielles pour aider les conseils à remplir leurs obligations en matière de gestion des risques liés à la cybersécurité. Voici quelques exemples d'orientations récemment publiées ou mises à jour.

- En octobre 2022, l'Australian Institute of Company Directors (l'institut australien des administrateurs de sociétés) et l'Australian Cyber Security Cooperative Research Centre (le centre australien de recherche coopérative sur la cybersécurité) ont publié des directives intitulées *Cyber Security Governance Principles* (principes de gouvernance en matière de cybersécurité) pour aider les administrateurs, les professionnels chargés de la gouvernance et leurs organisations à surveiller et à gérer les cyberrisques de façon proactive. Ce guide s'adresse aux entreprises de toutes tailles, y compris les petites et moyennes entreprises et les organismes sans but lucratif. Il préconise l'intégration de la cybersécurité aux pratiques de gestion des risques existantes – y compris la production périodique de rapports et l'évaluation des mesures de contrôle des cyberrisques – qui tiennent compte de la stratégie de tolérance aux cyberrisques de l'organisation approuvée par le conseil.

- En mars 2023, le National Cyber Security Centre (centre national de cybersécurité) du Royaume-Uni a annoncé la publication d'une nouvelle mouture de sa *trousse de cybersécurité* afin d'aider les conseils d'administration à faciliter l'intégration de la cyberrésilience et de la gestion des risques à l'échelle de leur entreprise. La trousse explique certains aspects importants de la cybersécurité, recommande les mesures à prendre par les administrateurs et leur entreprise et présente une foire aux questions pour aider les administrateurs à prendre des décisions éclairées en matière de gestion des risques liés à la cybersécurité. Elle explique que la gestion des risques liés à la cybersécurité est un processus continu et itératif, et qu'il convient de tenir compte des cyberrisques en les intégrant aux processus de gestion des risques et de prise de décisions à l'échelle de l'entreprise.

- En mars 2023, la National Association of Corporate Directors (l'association nationale des administrateurs de sociétés) des États-Unis et l'Internet Security Alliance (l'alliance pour la sécurité sur Internet) ont publié la quatrième édition de leur *Director's Handbook on Cyber-Risk Oversight* (le guide sur la surveillance des cyberrisques à l'intention des administrateurs) pour fournir aux administrateurs de sociétés des consignes à jour qui tienne compte des changements survenus en matière de cybermenaces. Le guide met l'accent sur six principes clés pour améliorer la surveillance des cyberrisques par les entreprises de toutes tailles. Ces principes cadrent avec les pratiques recommandées dans le rapport du vérificateur général sur l'UVI. Par exemple, les conseils devraient obliger leurs directions à identifier et quantifier les cyberrisques, à indiquer lesquels accepter, atténuer ou transférer, et à documenter leurs plans de gestion des risques.

Commentaires

La gestion des risques de cybersécurité nécessite la prise, par le conseil et la haute direction d'une organisation, de décisions opérationnelles cadrant avec le degré de tolérance au risque de cette dernière. Pour être raisonnables et justifiables, ces décisions devraient être éclairées (c.-à-d. fondées sur des renseignements actuels, complets et fiables) et prises honnêtement et de bonne foi sur la base des conseils appropriés d'experts opérationnels, juridiques et techniques indépendants et qualifiés. À ce sujet, consultez le bulletin de BLG intitulé *Cyber risk management guidance for Canadian corporate directors* (en anglais).

La gestion des risques de cybersécurité suppose le respect des lois sur la protection de la vie privée et des renseignements personnels, des lois sur l'emploi et le travail et des lois sur les droits de la personne, et elle mérite souvent une attention particulière dans la négociation et la gestion de contrats avec des fournisseurs de services et de produits comme avec la clientèle. Grâce à des conseils juridiques opportuns, il est possible de faire face aux risques de cybersécurité dans l'observation des règlements et pratiques exemplaires et le respect des exigences légales. De plus, l'avocat-conseil qui agit fréquemment comme accompagnateur en matière d'incidents de cybersécurité peut offrir un regard unique sur l'évolution des menaces et les pratiques de gestion des incidents les plus répandues. C'est dans cette optique que le *Director's Handbook on Cyber-Risk Oversight* (le guide de l'administrateur sur la surveillance des cyberrisques) de la NACD et de l'ISA explique que les conseils [traduction] « doivent comprendre les répercussions juridiques des cyberrisques en fonction de la situation particulière de leur organisation », et recommande que les conseils « se réunissent régulièrement pour discuter des tendances légales, réglementaires et contractuelles » et retiennent les services d'avocats-conseils externes afin d'obtenir « une perspective multiclient et à l'échelle du secteur sur les tendances en matière de cyberrisques ».

Par : Daniel J. Michaluk

Services : Cybersécurité, respect de la vie privée et protection des renseignements personnels, Conformité à la législation sur le respect de la vie privée et la protection des renseignements personnels, Universités et collèges

Principaux contacts

Daniel J. Michaluk
CORESPONSABLE NATIONAL, RESPECT DE LA VIE PRIVÉE ET CYBERSÉCURITÉ

Toronto
DMichaluk@blg.com
416.367.6097

Eric S. Charleston
CORESPONSABLE NATIONAL, CYBERSÉCURITÉ

Toronto
ECharleston@blg.com
416.367.6566