September 13, 2023

Cyber risk management is a fundamental issue for universities, public bodies, and other organizations. The Auditor General of British Columbia recently issued an audit report finding a university's board of governors had not provided adequate oversight of the university's cybersecurity risk management practices. The report provides helpful guidance for university boards and other public boards of directors in British Columbia and across Canada.

Background

Cyber risks – risks of losses and costs/liabilities suffered or incurred by an organization as a result of an incident that adversely affects the organization's information technology systems or the confidentiality, integrity, or availability of the organization's data – are a critical organizational risk. The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2023-2024* warns that ransomware is a persistent threat to Canadian organizations.

Cybersecurity should be a priority for all Canadian universities. Numerous Canadian universities have been subject to high-profile ransomware attacks resulting in service disruptions, loss of sensitive data (including personal information), and damage to reputation. Their role in conducting research also makes universities targets for espionage and intellectual property theft, including by state-sponsored actors. This threat is paired with a unique challenge: university information technology networks are highly distributed, which makes them difficult to secure, and collegial governance and cultural norms at universities can impede the adoption of strong cybersecurity practices.

A university's board of governors usually has overall responsibility for the management, administration, and control of the university's property, revenue, business, and affairs, which requires the board to effectively supervise the decisions and activities of the university's management. Consequently, a university's board of governors must be engaged and take an active role in the university's cyber risk management activities and ensure that the university's management has effectively implemented appropriate policies and practices to manage cyber risks and respond to cybersecurity incidents.

The Auditor General's report

The Auditor General of British Columbia is an independent officer of the British Columbia Legislature, responsible for conducting audits of government entities to inform the people of British Columbia and their elected representatives on how government is managing its responsibilities and resources. In August 2023, the Auditor General released a report of an audit of the cybersecurity oversight practices of the board of governors of Vancouver Island University (VIU), a public university under the British Columbia *University Act* with a main campus in Nanaimo, an enrollment of 12,200, and a 15-member board of governors. The report explains that VIU was selected for the audit "because it is a similar size to many other universities in British Columbia".

In a YouTube video announcing the report, the Auditor General explains that cybersecurity attacks are increasing and each university's board of governors has "a critical role in overseeing cybersecurity risk management. They review strategies to protect IT systems and personal data, and they hold university management accountable for those strategies". The Auditor General's report further explains the roles of VIU's management and board of governors. Management is responsible for conducting risk assessments, implementing and operating risk mitigation processes, and reporting the status of risk management programs to the board. The board is expected to oversee cybersecurity risk management by evaluating whether management: (1) has current cybersecurity policies and procedures; (2) regularly assesses and monitors cybersecurity risks; and (3) receives regular reports on the institution's cybersecurity posture.

The Auditor General found that VIU's board of governors had defined roles and responsibilities for overseeing risk management and set expectations for management to improve enterprise risk management, including cybersecurity. However, the Auditor General concluded that the board had not provided adequate oversight of VIU's cybersecurity risk management practices. The report explains the following findings:

1. The board established oversight roles and responsibilities, but policies were out of date and feedback was not documented.

The Auditor General looked for VIU to have documented roles and responsibilities for board oversight of cybersecurity risk management through governance and risk management policies, including board evaluation of whether the president met expectations for managing cybersecurity risk.

The Auditor General found that the risk management policy was out of date. The board last reviewed and approved the policy in 2012, despite a scheduled review in 2017. The board had reviewed but not formally approved an updated policy in 2023.

The Auditor General also found that the board had established presidential goals relating to cybersecurity and addressed presidential performance against objectives through quarterly updates, but the board had not documented its feedback to the president.

2. The board did not have adequate orientation/training to oversee cybersecurity risk management.

The Auditor General looked for VIU to have a board orientation program that specifically addressed the board's oversight responsibility for cybersecurity risk management, and an annual development (training) program for board members to help increase their subject matter knowledge in areas of risk, including cybersecurity risk, to assist them with their oversight responsibilities or to address changes to the board's oversight role.

The Auditor General found that VIU was deficient in respect of both requirements. The board's orientation program, though addressing risk management and mentioning cybersecurity, did not include information about the board's oversight responsibilities for cybersecurity risk management. In addition, the board did not have an annual development program to update areas of significant risk, such as cybersecurity risk management, even though VIU's governance policy required a program.

3. VIU had a documented risk management framework, but the board did not timely review management's risk mitigation strategies.

The Auditor General looked for the board to regularly review management's cybersecurity risk assessments, including how management evaluated and mitigated cybersecurity risks, prioritized risk areas, and documented mitigation actions and outcomes. The Auditor General also looked for the board to confirm that management had assessed compliance with legal and regulatory requirements.

The Auditor General found that the board reviewed VIU's cybersecurity risk management framework and confirmed that the framework and policies were communicated to staff, students, and other key groups. However, the Auditor General also found that the board was too slow in performing its oversight responsibilities because of a delay between management's June 2022 identification of cybersecurity as a priority risk and the board's March 2023 review of management's documented risk assessment and mitigation plan. The report explains: "The board has a responsibility to request management to provide [cybersecurity risk mitigation strategies] throughout the year to help ensure an ongoing evaluation of management's response to cybersecurity risk".

The report summarizes the Auditor General's four recommendations:

- Ensure that governance and policy documents defining roles and responsibilities for cybersecurity risk management are reviewed and approved as scheduled.
- Create an annual development program and ensure board members receive annual training on cybersecurity risk management to support them in their oversight role.
- Update the board orientation program to include information on the roles and responsibilities for oversight of cybersecurity risk management.
- Review cybersecurity risk mitigation strategies annually.

The report confirms that VIU accepted all recommendations.

Other helpful guidance

The Auditor General's report is part of a growing body of guidance issued by government agencies, regulators, and authoritative organizations to help boards fulfil their cyber risk management responsibilities. Following are examples of recently published or updated guidance.

- In October 2022, the Australian Institute of Company Directors and the Australian Cyber Security Cooperative Research Centre published guidance titled *Cyber Security Governance Principles* to help directors, governance professionals, and their organizations proactively oversee and manage cyber risk. The guidance is designed for organizations of all kinds and sizes, including small and medium enterprises and not-for-profits. The guidance explains that cybersecurity should be embedded in existing risk management practices (including regular reporting and evaluation of cyber risk controls) that reflect the organizations' board-approved cyber appetite.

- In March 2023, the United Kingdom's National Cyber Security Centre announced a refreshed version of its *Cyber Security Toolkit for Boards* to help boards ensure that cyber resilience and risk management are embedded throughout their organizations. The Toolkit explains important aspects of cybersecurity, recommends actions by individual directors and their organizations, and provides questions and answers to help directors make informed cyber risk management decisions. Like the Auditor General's report regarding VIU, the Toolkit explains that cybersecurity risk management ought to be "a continuous, iterative process" and consideration of cyber risks should be integrated into organization-wide risk management and decision-making processes.

- In March 2023, the National Association of Corporate Directors and the Internet Security Alliance published the fourth edition of the *Director's Handbook on Cyber-Risk Oversight* to provide corporate directors with updated guidance that reflects changes in the cyber threat landscape. The Handbook focuses on six key principles to enhance cyber risk oversight for organizations of all kinds and sizes. The principles are consistent with the practices recommended in the Auditor General's report regarding VIU. For example, boards should require management to identify and quantify cyber risks, stipulate which risks should be accepted, mitigated, or transferred, and document risk management plans.

Comments

Cybersecurity risk management requires an organization's board and senior management to make risk-based business decisions consistent with the organization's risk tolerance. For those decisions to be reasonable and defensible, they should be informed (i.e., based on timely, complete, and reliable information) and made honestly and in good faith with the benefit of appropriate advice from independent and qualified business, legal, and technical experts. See BLG bulletin *Cyber risk management guidance for Canadian corporate directors*.

Managing cybersecurity risks implicates compliance with privacy/personal information protection laws, labour/employment laws, and human rights laws, and often requires special consideration when negotiating and administering contracts with service providers/suppliers and customers. Timely legal advice can help an organization manage cybersecurity risks in accordance with regulatory guidance and best practices while complying with legal requirements. In addition, legal counsel who regularly act as a cybersecurity incident coach can provide unique insight about the current threat environment and prevailing incident response practices. For those reasons, the NACD/ISA *Director's Handbook on Cyber-Risk Oversight* explains that boards "should understand the legal implications of cyber risks as they relate to their [organization's] specific circumstances", and recommends that boards should have "regular sessions on legal, regulatory, or contractual trends" and engage outside counsel to provide "a multi-client and industry-wide perspective on cyber-risk trends".

By: Daniel J. Michaluk

Services: Cybersecurity, Privacy & Data Protection, Compliance with Privacy & Data Protection, Universities and Colleges

---

Key Contacts

Daniel J. Michaluk
NATIONAL CO-LEADER, PRIVACY & CYBERSECURITY

Toronto
DMichaluk@blg.com
416.367.6097

Eric S. Charleston
PARTNER AND NATIONAL CO-LEADER, PRIVACY & CYBERSECURITY

Toronto
ECharleston@blg.com
416.367.6566