Bulletin | Cybersecurity, Privacy and Data Protection

April 2023

Cyber risk management guidance for Canadian corporate directors – 2023 Update

Cyber risk management is a fundamental issue for organizations of all kinds and sizes. Directors of Canadian corporations have a legal responsibility to ensure their corporations effectively manage cyber risks and are prepared to respond effectively to cybersecurity incidents. Recently refreshed guidance can help corporate directors fulfil their cyber risk management duties.

Directors' duties – Cyber risk management

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 relevant to almost all organizations, regardless of size, industry, or public profile, because most organizations use or depend on information technology and data to operate their business. The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2023-2024* warns that cybercrime continues to be the cyber threat activity most likely to affect Canadians, and ransomware is a persistent threat to Canadian organizations.

Under Canadian law, corporate directors are obligated to manage or supervise the management of their corporation's business and affairs. In performing their obligations, corporate directors must: (1) act honestly and in good faith with a view to the best interests of their corporation (commonly known as the "duty of loyalty"); and (2) exercise the care, skill, and diligence that a reasonably prudent person would exercise in comparable circumstances (commonly known as the "duty of care"). The duty of care requires directors to proactively supervise corporate management, make informed, properly advised decisions, and exercise independent judgment.

In addition to the duties of loyalty and care, directors of Canadian reporting issuers (i.e., publicly traded companies) are required by securities laws to make continuous disclosure of material information about their corporation's business and operations – including information about cyber risks and cybersecurity incidents – so that investors have equal access to information that might affect their investment decisions.

For those reasons, regulators, self-regulatory organizations, industry associations, and other organizations have emphasized that corporate directors must be engaged and take an active role in their corporation's cyber risk management activities and must ensure that corporate management has properly implemented appropriate policies and practices to manage cyber risks and respond to cybersecurity incidents.

For more information, see BLG bulletin *Cyber risk management guidance for Canadian corporate directors*.

Recent guidance for directors

Government agencies, regulators, and other authoritative organizations have issued guidance to help corporate directors fulfil their cyber risk management responsibilities. Following are three examples of recently issued or updated guidance.

Australian Institute of Company Directors

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 focuses on five key principles:

(1) Set clear roles and responsibilities for cyber risk oversight, including regular robust reporting and engagement with management and advice and assurance from external experts.

(2) Develop, implement, and evolve a comprehensive cyber strategy to enhance the security of key digital assets, processes, and people over time and to help ensure legal compliance and demonstrate cyber resilience.

(3) Embed cybersecurity in existing risk management practices (including regular reporting and evaluation of cyber risk controls) that reflect the organization's board-approved cyber risk appetite.

(4) Promote a culture of cyber resilience across the organization, including through tone at the top, regular cybersecurity training/education, and incentives for strong cybersecurity practices.

(5) Plan for a significant cybersecurity incident, including by developing and evolving a director-approved incident response plan and conducting appropriate testing, training, and exercises.

The guidance provides detailed comments and recommendations for each key principle and includes recommended questions that directors can ask management.

NCSC – Cyber Security Toolkit for Boards

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. The Toolkit discusses nine aspects of cyber risk management: (1) embedding cybersecurity into the organization; (2) developing a positive cybersecurity culture; (3) growing cybersecurity expertise; (4) identifying critical assets in the organization; (5) understanding the cybersecurity threat; (6) risk management for cybersecurity; (7) implementing effective cybersecurity measures; (8) collaborating with supply chain and partners; and (9) planning responses to cyber incidents. The Toolkit includes explanatory videos, lists of essential board activities, and questions for evaluating success.

The Toolkit emphasizes that directors have a pivotal role in improving their organization's cyber resilience. The Toolkit explains that cyber risk management is "a continuous, iterative process", and consideration of cyber risks should be integrated into organization-wide risk management and decision-making processes.

NACD/ISA – Directors' Handbook on Cyber-Risk Oversight

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, including private companies and not-for-profit organizations:

(1) Directors need to understand and approach cybersecurity as a strategic, enterprise risk – not just an information technology risk.

(2) Directors should understand the legal implications of cyber risks as they relate to their organization's specific circumstances.

(3) Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on board meeting agendas.

(4) Directors should set the expectation that management will establish an enterprise-wide, cyber risk management framework with adequate staffing and budget.

(5) Board-management discussions of cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, as well as specific plans associated with each approach.

(6) Boards should encourage systemic resilience through collaboration with their industry and government peers and encourage the same from their management teams.

The Handbook provides detailed guidance and critical considerations for each principle and encourages directors to adapt the guidance "based on their organization's unique characteristics, including size, life-cycle stage, strategy, business plans, industry sector, geographic footprint, and

culture". The Handbook also includes an extensive toolkit to help directors apply the principles to their organization, including questions that directors can ask each other and senior management (including questions specific to incident response, mergers and acquisitions, and cybersecurity disclosures to investors and other stakeholders).

The Handbook emphasizes that "cybersecurity is an essential element of board-level oversight and needs to be integrated into early discussions about issues such as mergers, acquisitions, new product development, and strategic partnerships". The Handbook explains that "… boards need to employ the same principles of inquiry and constructive challenge that are standard features of board-management discussions about strategy and company performance and include cybersecurity oversight into boardroom operations planning".

Comment

Cyber risks are pervasive and increasing in frequency, intensity, and harmful consequences due to various circumstances, including increasing use of, and dependency on, information technology and data, increasing sophistication and complexity of cyber-attacks, and evolving legal requirements and liabilities. Consequently, directors of Canadian corporations should be vigilant to understand and comply with their cyber risk management duties. Following are some recommendations:

- Directors should take an active role in the foundational determinations of their corporation's cyber risk tolerance and directly oversee the management of significant cyber risks affecting their corporation.
- Directors should implement and evolve a suitable cyber risk governance structure, based on best practices and regulatory guidance, to help ensure that corporate management has properly implemented appropriate policies and practices to manage cyber risks in connection with all aspects of their corporation's business (including mergers and acquisitions) and to respond effectively to cybersecurity incidents.
- Directors' cyber risk management decisions should be fully informed – based on timely, complete, and reliable information from management and independent assessments – and made with appropriate advice from independent and qualified business, legal and technical experts.
- Directors of reporting issuers should ensure that management has implemented an appropriate program for cyber risk identification, assessment, and reporting so that directors are able to fulfil their continuous disclosure obligations under securities laws.
- Directors of reporting issuers should ensure that their corporation has appropriate insider trading policies to prevent unlawful trading and tipping using non-public information about cyber risks and cybersecurity incidents.
- Directors' cyber risk management activities and decision-making processes should be fully documented so directors are able to demonstrate compliance with their duty of care and invoke the business judgment rule if their decisions are challenged.
- Directors should ensure that their corporation has adequate insurance coverage for losses and liabilities resulting from cybersecurity incidents and for claims against directors arising from the performance of their cyber risk management duties. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.