Bulletin | Cybersecurity, Privacy and Data Protection

March 2021

Cyber risk management guidance for Canadian corporate directors

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 have appropriate cyber risk management policies and practices and are prepared to respond effectively to cybersecurity incidents. Guidance from regulators, industry associations and other organizations can help corporate directors fulfil their cyber risk management duties.

Corporate directors' duties and obligations

General

Under Canadian law, corporate directors are responsible for managing or supervising the management of their corporation's business and affairs, including activities regarding risk identification and management. In exercising their powers and performing their obligations, corporate directors are required to: (1) act honestly and in good faith with a view to the best interests of their corporation (commonly known as the "fiduciary duty" or "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").

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, including material risks that might affect their corporation's business and operations. Canadian securities laws also prohibit corporate directors from using or tipping someone else to use material non-public information about their corporation to decide whether to buy, sell or hold the corporation's shares (i.e., insider trading).

Directors who breach their duties of loyalty or care may incur personal liability to their corporation and possibly other persons as well. Directors who violate securities laws may be subject to potentially severe sanctions, including fines, imprisonment, and personal liability to investors and other persons adversely affected by the violation.

Duty of care

The duty of care requires as follows:

- Directors must proactively supervise corporate management and be satisfied that corporate management has established and implemented policies and practices to ensure their corporation carries on business in accordance with all applicable laws.
- Directors must make informed, properly advised decisions. They must use care in gathering relevant information, obtain independent advice (where required), act carefully, deliberately and responsibly after due deliberation and not act with undue haste.
- Directors must exercise independent judgment. They must not subordinate their power and authority to the will of other persons.

The standard of the duty of care is objective, meaning that a director's conduct is measured against the standard of what a reasonably prudent person would do in comparable circumstances. The directors' duty of care does not require perfection – directors are required to make reasonable decisions, not perfect decisions.

Independent advisors

Under Canadian law, corporate directors are not required to be experts in all fields. Directors may reasonably and in good faith rely on the advice of external expert advisors (e.g., lawyers, accountants and technical experts) provided that: (1) the advisors are independent (i.e., no conflict of interest) and qualified to give the advice; and (2) the directors ultimately exercise their own reasonable judgment.

While there is no specific corporate law requirement for corporate directors to obtain independent expert advice, in some circumstances failing to do so might increase the risk that the directors will not fulfil their duty to make fully informed and reasonable business decisions. Consequently, directors often obtain independent expert advice for decisions involving matters that are beyond the directors' core competence or present higher risks of shareholder scrutiny or complaint.

Business judgment rule

Canadian courts have adopted a rule of deference to directors' business decisions, known as the "business judgment rule", which prevents courts from second-guessing directors' legitimate decisions provided that the directors acted honestly and in good faith, independently and without conflict of interest, and used an appropriate degree of prudence and diligence in reaching a business decision that falls within a range of reasonable alternatives at the time it was made.

The business judgment rule will shield directors' business decisions from judicial scrutiny only if the decisions are made prudently and in good faith, and where the directors' actions demonstrate the exercise of their business judgment. The rule will not prevent a court from finding directors negligent if they fail to use reasonable care to obtain necessary information and advice, fail to consider facts that they knew or should have known, or ignore important information in their possession.

Directors' duties – Cyber risk management

General

Cyber risks – risks of loss/harm and costs/liabilities resulting from a failure or breach of the information technology systems used by or on behalf of an organization or its business partners – 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. While large, high profile companies that handle valuable data are obvious targets for cyber attack, cyber criminals are increasingly targeting small and medium size organizations as direct targets, to obtain information about their customers and business partners, and as a means of accessing the systems and data of their business partners. Commentators have said there are only two kinds of organizations – those that have been hacked and know it, and those that have been hacked and don't know it yet.

Canadian corporate directors' responsibility for cyber risk management derives from the directors' general duty to manage or supervise the management of their corporation's business and affairs. Directors are required to: (1) play an active role in the foundational determinations of their corporation's risk appetite and resulting risk tolerance; (2) ensure that management has taken reasonable steps to identify and manage risks through an appropriate risk management program; and (3) have direct oversight regarding significant risks affecting their corporation, which the directors should monitor and discuss regularly with senior management.

Canadian 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 example:

- Investment Industry Regulatory Organization of Canada *Cybersecurity Best Practices Guide* emphasizes that cybersecurity is a multi-faceted challenge that requires a sound governance framework — strong leadership, board and senior management engagement and clear accountability — for a successful cybersecurity program.
- Canadian Securities Administrators (CSA) *Staff Notice 11-332 Cyber Security* notes that guidance documents issued by various regulatory authorities and standard-setting bodies highlight the need for an organization to manage cybersecurity at an organizational level with responsibility for governance and accountability at the executive and board levels.
- Mutual Fund Dealers Association of Canada *Compliance Bulletin — Cybersecurity* recommends that member dealers establish a cyber risk governance and risk management framework that includes the involvement of directors and senior management.

- Chartered Professional Accountants Canada *Cybersecurity Bulletin for Directors* explains that directors should adopt a cybersecurity governance framework for assessing cyber risk within their organization.
- CSA *Multilateral Staff Notice 51-347, Disclosure of cyber security risks and incidents* explains CSA's expectations for continuous disclosure regarding cybersecurity risks and incidents by reporting issuers.

Recent guidance for directors

Following are three recent examples of helpful cyber risk management guidance and tools for corporate directors.

NCSC – *Cyber Security Toolkit for Boards*

In 2019, the United Kingdom's National Cyber Security Centre published guidance titled *Cyber Security Toolkit for Boards* to help boards develop a suitable cybersecurity strategy. The guidance explains important aspects of cybersecurity, recommends actions by individual directors and by their organization, and provides questions and answers for discussions to determine what constitutes "good" cybersecurity for the organization. The guidance discusses nine aspects of cyber risk management: (1) embedding cybersecurity into organizational structure and objectives; (2) growing cybersecurity expertise; (3) developing a positive cybersecurity culture; (4) establishing a baseline and identifying priorities; (5) understanding cybersecurity threats; (6) risk management; (7) implementing effective cybersecurity measures; (8) collaborating with suppliers and partners; and (9) planning cyber incident response.

The guidance emphasizes that directors are pivotal in improving the cybersecurity of their organizations. The guidance explains that cyber risk management is "a continuous, iterative process", and the management of cyber risks should be integrated into general organizational risk management processes.

CPA Canada – *20 questions directors should ask about cybersecurity*

In 2019, Chartered Professional Accountants Canada published guidance titled *20 questions directors should ask about cybersecurity* to help directors understand and fulfil their duty to oversee their organization's cyber risk management activities. The guidance uses the National Institute of Standards and Technology *Cybersecurity Framework* to organize and explain twenty broad questions (many with detailed sub-questions) about the following issues: (1) cyber risk management governance; (2) cybersecurity risk identification; (3) asset identification/prioritization; (4) cybersecurity controls; (5) cybersecurity incident detection; (6) cybersecurity incident response/recovery; and (7) reporting to the board. The guidance includes detailed recommendations to help directors fulfil their cybersecurity responsibilities, and advice regarding specific cybersecurity controls.

The guidance explains that "cybersecurity is not a technology issue; all executives and their departments play a role in reducing cybersecurity risk", and "cybersecurity is an ongoing process that requires constant review and improvement". The guidance encourages directors to ask management "How close are we to reducing our cybersecurity risk to targeted levels?", and recommends that directors who are not comfortable assessing management's answers to their questions should engage external cybersecurity professionals to provide another perspective.

NACD – *Directors' Handbook on Cyber-Risk Oversight*

In 2020, the National Association of Corporate Directors (NACD) and the Internet Security Alliance published an updated edition of the *NACD Director's Handbook on Cyber-Risk Oversight*. The Handbook focuses on five key principles to enhance cyber-risk oversight for organizations of all kinds and in all industry sectors: (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) directors 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; and (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.

The Handbook provides detailed guidance for each of the key principles and includes an extensive toolkit to help directors apply the principles to their organization. The toolkit includes questions that directors can ask each other and senior management (including questions specific to mergers and acquisitions and cybersecurity disclosures to investors and other stakeholders) and sample dashboards.

The Handbook emphasizes that cyber risks "must be treated with the same vigilance as more traditional vectors of business disruption and loss of profit", and that effective cybersecurity requires both technical capabilities and robust risk-management practices. The Handbook also explains that the board's role is "to bring its judgment to bear and provide effective guidance to management, in order to ensure the cybersecurity program is appropriately designed and sufficiently resilient given their corporation's strategic imperatives and the realities of the business ecosystem in which it operates".

Comment

Cyber risks are pervasive and increasing in frequency, intensity and harmful consequences because of 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 comply with their cyber risk management duties. Following are some recommendations:

- Directors should take an active role in their corporations' cyber risk management activities.
- Directors should implement, and periodically review and revise, an appropriate 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 made with the benefit of appropriate advice from independent and properly 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 the directors are able to successfully invoke the business judgment rule if their decisions are challenged.
- Directors should ensure that their corporation has procured adequate insurance coverage for losses and liabilities resulting from cybersecurity incidents and for claims against directors and officers arising from the performance of their cyber risk management duties. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national Cybersecurity, Privacy and Data Protection Group offers comprehensive advice on compliance with privacy laws at the federal and provincial levels as well as with European data protection legislation. We provide both proactive compliance advice and legal advice to help respond to a contravention of privacy laws.