FEBRUARY 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Cyber Risk Management Guidance for Corporate Directors

Cyber risk management is an increasingly important challenge for organizations of all kinds and sizes. Corporate directors have a legal responsibility to ensure that their corporations have appropriate cyber risk management policies and practices and are prepared to respond effectively to cyber incidents. Corporate directors can obtain helpful guidance from regulators, industry associations and other organizations.

Cyber Risks

Cyber risks are the risks of damage, loss and liability (e.g. business disruption, financial loss, loss to stakeholder value, reputational harm, trade secret disclosure and other competitive harm, legal non-compliance liability and civil liability to customers, business partners and other persons) to an organization resulting from a failure or breach of the information technology systems used by or on behalf of the organization, including incidents resulting in unauthorized access, use or disclosure of regulated, protected or sensitive data. Cyber risks can result from internal sources (e.g. employees, contractors, service providers and suppliers) or external sources (e.g. nation-states, terrorists, hacktivists, competitors and acts of nature).

Cyber risks appear to be increasing in frequency, intensity and harmful consequences as a result of various circumstances, including increasing sophistication and complexity of cyber-attacks, increasing use of information technology (e.g. increased access points and use of third-party services and infrastructure) and data (e.g. customer personal information, payment information and Big Data), increasing regulation (e.g. regulated personal/financial information and security breach reporting obligations) and increasing legal liability (e.g. privacy breach liability). Commentators have said that 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.

Directors' Duties – General

A corporate director's responsibility for cyber risk management derives from the well-established, generally applicable director's duty of care, which requires a director to exercise the care, skill and diligence that a reasonably prudent person would exercise in comparable circumstances. The duty of care requires a director to proactively supervise management and make informed, properly advised decisions.

It is generally accepted that a director's duty of care requires the director to oversee management's activities regarding risk identification and risk management generally, and with particular attention to internal controls and management information systems. Directors are required to be an integral part of the risk management process and must play an active role in the foundational determinations (and periodic reviews) of the corporation's risk appetite and resulting risk tolerance. Directors are expected to ensure that management has taken reasonable steps to identify and manage risks through an appropriate risk management program, and directors should have direct oversight regarding significant risks affecting the corporation (which the directors should monitor and discuss regularly with senior management).

Canadian courts recognize that corporate directors and officers often have business expertise that courts do not have, that business decisions often involve some degree of risk and may be reasonable and defensible when they are made even though they are ultimately unsuccessful, and that it is inappropriate for courts to apply perfect hindsight to corporate directors' past decisions. Those considerations are the foundation of the "business judgment rule", whereby courts will defer to directors' reasonable business judgment provided that the directors acted 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.

Directors' Duties – Cyber Risk Management

Regulators, self-regulatory organizations, industry associations and other organizations have emphasized that corporate directors must be engaged and take an active role in cyber risk management activities, and must ensure that management has properly implemented

appropriate policies and procedures to manage cyber risks and to effectively respond to cybersecurity incidents. For example:

- The National Association of Corporate Directors' *Director's Handbook on Cyber-Risk Oversight* (January 2017) emphasizes that effective management of cyber risks requires conscientious and comprehensive oversight by an organization's board of directors.
- World Economic Forum's *Advancing Cyber Resilience Principles and Tools for Boards* (January 2017) emphasizes that board-level action regarding cyber resilience is "absolutely urgent", and explains that organizational leadership has a vital role to play in securing cyber resilience.
- Canadian Securities Administrators' *CSA Staff Notice 11-332 Cyber Security* (September 2016) notes that guidance documents issued by various regulatory authorities and standard-setting bodies highlight the need for an organization to manage cyber security at an organizational level with responsibility for governance and accountability at executive and board levels.
- Mutual Fund Dealers Association of Canada's *Compliance Bulletin - Cybersecurity* (May 2016) recommends that member dealers establish a cyber risk governance and risk management framework that includes the involvement of directors and senior management.
- Investment Industry Regulatory Organization of Canada's *Cybersecurity Best Practices Guide* (December 2015) 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. "Directing the implementation of a comprehensive cybersecurity program... is incumbent upon all boards – regardless of company size".
- Global Network of Director Institutes' *Perspectives Paper — Guiding Principles for Cybersecurity Oversight* (November 2015) explains that directors and boards need to treat cybersecurity as an integrated component of enterprise-wide risk management, and that cyber risk needs to be overseen by the full board, with support from appropriate committees.
- Chartered Professional Accountants Canada's *Board Bulletin — Cybersecurity Risk — Questions for Directors to Ask* (July 2015) explains that a board of directors must be satisfied that the organization has a security program that sufficiently protects internal business systems and connections to cyberspace including transactions between employees, customers, suppliers and governments, from cyber-crime and mischief.
- Institute of Internal Auditors Research Foundation's *Cybersecurity: What the Board of Directors Needs to Ask* (August 2014) emphasizes that directors must take an active role in the organization's cybersecurity or face the possibility of potential shareholder lawsuits, and even the possibility of being removed from the board.
- Conference Board's *Director Notes — The Board's Role in Cybersecurity* (March 2014) advises that corporate boards must ensure that their companies have appropriate processes in place to manage cyber risks in the context of their business.

The views expressed by regulators, organizations and associations might not have the force of law, but they may be relied on by courts in determining the standard of reasonable care, skill and diligence required of corporate directors regarding the management of a corporation's cyber risks.

Recent Guidance for Directors

Regulators, industry associations and other organizations have issued helpful cyber risk management guidance and tools for corporate directors. Following are two recent examples.

(a) NACD *Director's Handbook on Cyber-Risk Oversight*

In January 2017, the National Association of Corporate Directors (NACD) and the Internet Security Alliance published the 2017 edition of the *NACD Director's Handbook on Cyber-Risk Oversight*. The Handbook identifies and details five key steps that directors of all kinds of organizations (e.g. public companies, private companies and non-profit organizations) should consider for cyber risk management: (1) directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an information technology issue; (2) directors should understand the legal implications of cyber risks as they relate to their company'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 the board meeting agenda; (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 of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.

The Handbook includes detailed *Questions for the Board to Ask Management about Cybersecurity*, a summary of cybersecurity considerations relevant to mergers and acquisitions and suggestions for cybersecurity metrics to be included in board-level briefings.

(b) World Economic Forum *Advancing Cyber Resilience Principles and Tools for Boards*

In January 2017, the World Economic Forum published a report titled *Advancing Cyber Resilience Principles and Tools for Boards* to provide a framework and set of tools for directors to use to integrate cyber risk and resilience into business strategy.

The Report includes *Board Principles for Cyber Resilience*, which is a framework of ten principles to enable directors to encourage cyber resilience: (1) responsibility for cyber resilience; (2) command of the subject; (3) accountable officer; (4) integration of cyber resilience; (5) risk appetite; (6) risk assessment and reporting; (7) resilience plans; (8) community; (9) review; and (10) effectiveness.

The Report includes a *Cyber Principle Toolkit*, which supports the ten *Board Principles* with a set of questions to foster board-management dialogue and aid the board in fulfilling its oversight obligations. The Report also includes a *Board Cyber Risk Framework* to provide a process for use by boards to understand and evaluate their organization's cyber risks and resilience strategy.

Comment

Corporate directors should take seriously their legal responsibility to take an active role in their corporations' cyber risk management activities, and ensure that corporate management has properly implemented appropriate policies and procedures to manage cyber risks and to respond effectively to cybersecurity incidents. Directors should ensure that their cyber risk management decisions are informed (based on reasonable inquiries of management) and properly advised (based on appropriate expert advice). Directors should document their cyber risk management activities, so that they will be able to effectively respond to lawsuits and regulatory inquiries and successfully establish the due diligence and other circumstances required to invoke the business judgment rule. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

For more information about cyber risk management and BLG's related legal services, please see the BLG website.

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com