Borden Ladner Gervais

CYBER-RISK MANAGEMENT – GUIDANCE FOR CORPORATE DIRECTORS

Cyber-risk management is an increasingly important challenge for corporate directors. Many commentators have said that there are only two types of organizations – those that have been hacked and know it, and those that have been hacked and don't know it yet. Corporate directors have a legal responsibility to ensure that their corporations have appropriate cyber-risk management policies and practices and are prepared to effectively respond to cyber-attacks. Corporate directors can obtain helpful guidance from regulators, industry associations and other organizations.

CYBER-RISKS

Cyber-risks are risks of damage, loss or liability (e.g. financial loss, business disruption loss, loss to stakeholder value, reputational harm and legal noncompliance liability) to a corporation resulting from a failure or breach of the corporation's information technology systems. Cyber-risks can result from both internal sources (e.g. employees, contractors, service providers and suppliers) and external sources (e.g. nation states, terrorists, hacktivists and competitors).

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).

DIRECTORS' DUTY OF CARE

A corporate director's responsibility for cyber-risk management derives from the generally applicable director's duty of care, which requires a corporate director to exercise the care, skill and diligence of a reasonably prudent person in comparable circumstances. The duty of care requires a corporate director to proactively supervise corporate 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 management generally, and with particular attention to internal controls and management information systems.

DIRECTORS' RESPONSIBILITY FOR CYBER-RISK MANAGEMENT

Regulators, industry associations and other organizations (e.g. The Office of the Superintendent of Financial Institutions Canada, The Securities and Exchange Commission, The Financial Industry Regulatory Authority, Chartered Professional Accountants Canada, The Conference Board of Canada, The National Association of Corporate Directors and The Institute of Internal Auditors Research Foundation) 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 their corporations have appropriate policies and practices in place to manage cyber-risks in the context of their businesses and to effectively respond to cyber-attacks. Statements by regulators, industry associations and other groups might not have the force of law, but they will likely inform any judicial determination of the care, skill and diligence required of a corporate director regarding cyber-risk management.

GUIDANCE FOR DIRECTORS

Directors seeking to fulfil their cyber-risk management responsibilities can find helpful guidance from various sources in Canada and elsewhere. For example:

- *Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition*, published by the U.S. National Association of Corporate Directors, identifies and details the following guiding principles for cyber-risk management: (1) directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an information technology (IT) 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 risk management framework with adequate staffing and budget; and (5) board-management discussion 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.
- *Cyber Security Self-Assessment Guidance*, published by the Office of the Superintendent of Financial Institutions of Canada, includes a detailed questionnaire focussing on six key issues: (1) organization and resources; (2) cyber-risk and control assessment; (3) situational awareness; (4) threat and vulnerability risk management; (5) cybersecurity incident management; and (6) cybersecurity governance.
- *Report on Cybersecurity Practices*, published by the U.S. *Financial Industry Regulatory Authority*, includes detailed recommendations and comments on best practices regarding eight areas of concern: (1) governance and risk management; (2) risk assessment; (3) technical controls; (4) incident response planning; (5) vendor management; (6) staff training; (7) intelligence and information sharing; and (8) insurance.

Directors should document their cyber-risk management activities, so that they will be able to effectively respond to regulatory inquiries and establish a due diligence defence in litigation.

COMMENTS

Corporate directors should take seriously their legal responsibility to proactively supervise corporate management, and make informed, properly advised decisions, regarding cyber-risk management. Corporate directors can obtain helpful guidance from regulators, industry associations and other organizations.

AUTHOR

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances. Copyright © 2015 Borden Ladner Gervais LLP.

Borden Ladner Gervais

BORDEN LADNER GERVAIS
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 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
Scotia Plaza, 40 King St W, Toronto, ON, Canada M5H 3Y4
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