Borden Ladner Gervais

CYBER-RISK MANAGEMENT GUIDANCE FROM FINANCIAL INSTITUTION REGULATORS

Cyber-risk management is an increasingly important challenge for organizations of all kinds. 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. Financial industry regulators in Canada and the United States have issued helpful guidance for cyber-risk management. The guidance emphasizes the need for organizations to proactively manage cyber-risks and to prepare for cybersecurity incidents.

FINRA

In February 2015, the Financial Industry Regulatory Authority ("FINRA"), an independent regulator for securities firms doing business in the United States, issued its *Report on Cybersecurity Practices* to provide guidance regarding cyber-risk management. The Report discusses key risk management issues (e.g. governance and risk management, risk assessment, technical controls, incident response planning, vendor management, staff training, intelligence and information sharing and insurance) and provides a helpful summary of principles and effective practices. The Report confirms FINRA's expectation that securities firms will make cybersecurity a priority and will devote sufficient resources to understanding and preparing for current and evolving cybersecurity threats.

U.S. SECURITIES AND EXCHANGE COMMISSION

In February 2015, the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") issued a *Risk Alert* to provide summary observations of its initial examination of the cybersecurity preparedness of over 100 registered broker-dealers and investment advisers conducted as part of a Cybersecurity Examination Initiative. An earlier *Risk Alert*, issued in April 2014, explained the Initiative and attached a sample request for information and documents covering a wide range of cyber-risk management issues, including identification of risks/governance, protection of networks and information, risks associated with remote access, risks associated with vendors and other third parties, and detection of unauthorized activity.

In June 2014, Commissioner Aguilar of the U.S. Securities and Exchange Commission gave a speech in which he emphasized the critical role that corporate directors play in their corporation's prevention and response to cyber attacks. The Commissioner explained that a corporation's directors must take seriously their responsibility to ensure that the corporation appropriately addresses cyber-risks, including ensuring the adequacy of the corporation's cybersecurity preparedness and response plans. The Commissioner warned that boards that choose to ignore, or minimize, the importance of their cybersecurity oversight responsibility do so at their own peril. The Commissioner encouraged corporate boards and management to use the February 2014 *Framework for Improving Critical Infrastructure Cybersecurity* issued by the National Institute of Standards and Technology. The Commissioner concluded that there is no substitution for proper preparation, deliberation and engagement on cybersecurity issues.

IIROC

In January 2015, the Investment Industry Regulatory Organization of Canada ("IIROC"), the national self-regulatory organization for investment dealers in Canada, published its *Annual Consolidated Compliance Report* outlining key examination and surveillance priorities for 2015. The Report notes that proactive cyber-risk management is critical, and emphasizes that enterprise-wide cybersecurity planning is an important part of an organization's overall risk-management program. The Report explains that cyber-risk management is an important strategic issue to be addressed by corporate directors and senior management.

CSA AND OSFI

In late 2013, the Canadian Securities Administrators ("CSA") and the Office of the Superintendent of Financial Institutions of Canada ("OSFI") each issued cyber-risk management guidance. CSA's *Staff Notice 11-326 - Cyber Security* reminds issuers, registrants and regulated entities of the importance of cyber-risk management (including the need to regularly review cybersecurity control measures and consider relevant prudent business practices) and the need for cyber-risk disclosures in prospectuses and continuous disclosure filings. OSFI's *Cyber Security Self-Assessment Guidance* explains that senior management of federally regulated financial institutions should regularly review their institution's cyber-risk management policies and practices to ensure that they remain appropriate and effective, and that an institution's board of directors (or board committee) should regularly review and discuss the institution's cyber-risk management practices.

COMMENT

Cyber-risk management guidance issued by financial industry regulators, while directed to financial institutions and securities industry participants, can be helpful for all organizations. The regulatory guidance might also establish best practices against which the actions of an organization and its management might be measured by regulators and courts in the event the organization is the victim of a cyber attack or other kind of cybersecurity incident.

AUTHOR

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

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