MAY 2016

CYBERSECURITY BULLETIN

Borden Ladner Gervais

CYBERSECURITY GUIDANCE FROM INVESTMENT INDUSTRY ORGANIZATION

Cyber risk management is an increasingly important challenge for organizations of all kinds. The Mutual Fund Dealers Association of Canada ("MFDA"), the national self-regulatory organization that oversees mutual fund dealers in Canada, has published a Cybersecurity bulletin to help its members manage cybersecurity risks. The Bulletin recommends using a Cybersecurity Framework to proactively manage cyber risks and to prepare for cybersecurity incidents.

CYBER RISKS

Cyber risks are risks of loss and liability (e.g. business disruption, financial loss, loss to stakeholder value, reputational harm, trade secret disclosure and other competitive harm, legal noncompliance 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 sensitive, regulated or protected data. Cyber risks can result from internal sources (e.g. employees, contractors, service providers, suppliers and operational risks) or external sources (e.g. nation states, terrorists, hacktivists, competitors and acts of nature).

Cyber risks are 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 and data, increasing regulation and increasing legal 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.

CYBERSECURITY GUIDANCE

MFDA's *Cybersecurity* bulletin recommends that member dealers establish and maintain appropriate cybersecurity procedures, controls and risk management techniques, using people, processes, tools and technologies, to adequately protect information technology devices/systems and data from attack, damage and unauthorized access. The Bulletin explains the need to focus on three fundamental goals: (1) confidentiality of information; (2) integrity of information assets; and (3) availability of information technology devices/systems and data.

The Bulletin recommends that member dealers develop a Cybersecurity Framework that has five basic functions: (1) identify important assets and related threats/risks; (2) protect assets with appropriate safeguards; (3) detect intrusions, breaches and unauthorized access; (4) respond to a cybersecurity event; and (5) recover from a cybersecurity event. The Bulletin identifies some basic issues for consideration when developing a Cybersecurity Framework, including:

- A governance and risk management framework, including involvement of directors and senior management.
- Managing insider risks from new, current and departing employees and contractors.
- Physical security for human, environmental and supply chain threats.
- Cybersecurity awareness (including mandatory on-going training for all personnel) and cybersecurity policies/procedures.
- Regular threat assessments and vulnerability testing.
- Network security measures, including multi-layered defences and restricted access.
- Technologies and practices to protect information systems, including data backup and recovery, anti-malware solutions and device controls.
- User account management and access controls.
- Information technology asset/device management.
- Cyber incident response plans.
- Information sharing and breach reporting.
- Cyber insurance.
- Vendor risk management and mitigation.

The Bulletin identifies some foundational resources, including guidance issued by Investment Industry Regulatory Organization of Canada, Financial Industry Regulatory Authority, Canadian Securities Administrators, Government of Canada and the U.S. National Institute of Standards and Technology.

COMMENT

Cybersecurity guidance issued by government agencies, industry organizations and regulators will likely be considered by courts when determining whether an organization and its directors and management used reasonable care to manage cyber risks. The MFDA's Bulletin provides a helpful summary of some basic cyber risk management practices and considerations that are useful for all organizations. For more information regarding cyber risk management guidance from investment and financial industry regulators, see the following BLG bulletins: *Cybersecurity Guidance From Investment Industry Organization* (January 2016), *U.S. Securities and Exchange Commission issues Cybersecurity Guidance Update* (May 2015), *Cyber-Risk Management – Guidance For Corporate Directors* (April 2015), *Cyber-Risk Management Guidance From Financial Institution Regulators* (March 2015) and *Regulatory Guidance for Cyber Risk Self-Assessment* (November 2013). ■

AUTHOR

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

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
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