Cybersecurity Bulletin

March 2019

Investment Funds Institute of Canada Issues Cybersecurity Guide

In February 2019, the Investment Funds Institute of Canada issued a *Cybersecurity Guide* to help its members develop a robust cybersecurity program. The guide is consistent with guidance issued by other financial industry regulators, and is a useful reminder of cybersecurity best practices for organizations in all business sectors.

Cyber Risks

Cyber risks are risks of harm (e.g. business disruption loss, financial loss, reputational harm, trade secret disclosure and other competitive harm) and costs/liabilities (e.g. incident response and remediation costs, litigation/regulatory proceeding costs, and liabilities to stakeholders, business partners, customers and regulators) suffered or incurred by an organization as a result of a failure or breach of the information technology systems used by or on behalf of the organization or its business partners (e.g. suppliers and service providers), including incidents involving loss or theft of, or unauthorized access, use, disclosure, modification or deletion of, data in the organization's possession or control. Cyber risks can result from internal sources (e.g. employees, contract workers and system failures) or external sources (e.g. nation-states, terrorists, competitors, hackers, fraudsters and acts of nature).

Cyber risks are relevant to almost any organization, regardless of size or industry, because almost all organizations use or depend on information technology and data to operate their business. Cyber risks appear to be increasing in frequency, intensity and harmful consequences as a result 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. 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.

IFIC Cybersecurity Guide

The Investment Funds Institute of Canada (IFIC) is the industry association for the investment fund industry in Canada. IFIC members represent all facets of the investment fund industry – fund managers, distributors and professional and back office firms that support the sector.

The *IFIC Cybersecurity Guide*, issued February 21, 2019, explains that cybersecurity is an area of focus for investment industry firms and regulators globally due to the potential harm to clients, firms and the investment industry in general. The Guide cautions that cybersecurity threats are numerous, wide-ranging and rapidly evolving.

The Guide reminds that all registered securities firms are required to establish and maintain policies and procedures to create a system of controls and supervision to manage business risks, including cybersecurity risks, in accordance with prudent business practices. The Guide explains that cybersecurity controls should ensure that networks, computers, programs and data are adequately protected from attack, damage or unauthorized access.

The Guide emphasizes the importance of a cybersecurity framework to help firms: (1) identify valuable assets and related threats and risks; (2) protect those assets with appropriate safeguards; (3) detect intrusions, breaches and unauthorized access; (4) respond to potential and actual cybersecurity events; and (5) recover from cybersecurity events.

The Guide identifies six essential components of a cybersecurity framework: (1) policies and procedures; (2) training; (3) risk assessment; (4) incident response plan; (5) vendor/service provider risk management; and (6) insurance. Following is a summary:

- **Policies and Procedures:** Implement and maintain policies/procedures that address cybersecurity incident prevention, detection, training and business continuity, including: using electronic communications; using devices; losing or disposing of electronic devices; using public/personal electronic devices or public/personal internet connections; detecting unauthorized activity; protecting data; updating software; due diligence of vendors and service providers with system access; and escalating and reporting cybersecurity incidents. The policies/procedures should be reviewed at least annually to ensure they remain current and relevant.
- **Training:** Conduct frequent (no less than annual) cybersecurity training for employees, including: recognizing risks; identifying and responding to cyber threats; handling confidential information; using passwords; securing devices; and identifying and escalating cybersecurity incidents.
- **Risk Assessments:** Conduct periodic cybersecurity risk assessments, including: identifying valuable assets and data; identifying vulnerable areas of operations; determining potential consequences of cyber threats; and evaluating and improving preventative controls and the incident response plan.
- **Incident Response Plan:** Establish and periodically test a documented incident response plan, including: identifying individuals responsible for communications about an incident, and the information that should be communicated to each relevant person or group; procedures for containing various types of incidents; recovering or restoring data; investigating incidents; and reviewing and modifying systems, policies and procedures to prevent similar incidents from occurring.
- **Vendors/Service Provider Risk Management:** Implement and maintain robust policies/procedures for due diligence and oversight of third party vendors and service providers. Written agreements with third party vendors and service providers should include provisions regarding cybersecurity and reporting cybersecurity incidents.
- **Insurance:** Periodically review and assess the adequacy of cybersecurity insurance coverage.

The Guide references additional Canadian and international cybersecurity resources, including guidance issued by Canadian Securities Administrators, the Investment Industry Regulatory Organization of Canada, the Mutual Fund Dealers Association of Canada and the Office of the Superintendent of Financial Institutions.

Comment

The *IFIC Cybersecurity Guide* provides a helpful summary of some basic cyber risk management best practices that are useful for organizations of all sizes and in all industries. The Guide is consistent with cyber risk management guidance issued by Canadian and American financial industry regulators and self-regulatory organizations. For more information, see BLG bulletins: *Cybersecurity Guidance from Investment Industry Organization (May 2016)*; *Cybersecurity Guidance from Investment Industry Organization (January 2016)*; *Cybersecurity Guidance from Canadian Securities Administrators*; *New York State Cybersecurity Regulation for Financial Services Companies*; *U.S. Securities and Exchange Commission Issues Cybersecurity Guidance Update*; *Cyber-Risk Management Guidance from Financial Institution Regulators*; *Regulatory Guidance for Cyber Risk Self-Assessment*.

Organizations engaged in cyber risk management activities should be mindful of their legal obligations to report, notify and disclose cybersecurity incidents imposed by statute, contract and common/civil law. For more information, see BLG bulletins *OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting*; *Canadian Investment Industry Regulator Proposes Mandatory Cybersecurity Incident Reporting*; *Data Incident Notification Obligations*; *Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*; *Preparing for Compliance with Canadian Personal Information Security Breach Obligations*.

Organizations engaged in cyber risk management activities should have an appropriate legal privilege strategy to help avoid inadvertent and unnecessary disclosures of privileged legal advice, or inadvertent waivers of legal privilege. For more information, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*; *Cyber Risk Management – Legal Privilege Strategy (Part 2)*; *Legal Privilege for Data Security Incident Investigation Reports*; *Loss of Legal Privilege over Cyberattack Investigation Report*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at **blg.com/cybersecurity**.

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