Cyber Risk Management — Regulatory Guidance From The Canadian Securities Administrators

September 29, 2016

On September 27, 2016, the Canadian Securities Administrators published an updated cyber security notice for financial market participants. The notice emphasizes the need for financial market participants to follow guidance issued by regulatory authorities and standard-setting bodies to proactively manage cyber risks and prepare for cybersecurity incidents. The notice provides important guidance that is useful for all organizations.

Cyber Risks

Cyber risks are the 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 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 are increasing in frequency, intensity and harmful consequences as a result of various circumstances, including increased sophistication and complexity of cyber-attacks, increased use of information technology and data and increased regulation.

The CSA's 2013 Notice

In September 2013, the Canadian Securities Administrators ("CSA") published Staff Notice 11-326 *Cyber Security* to remind financial market participants (i.e. issuers, registrants and regulated entities) of the importance of "strong and tailored cyber security measures" to protect themselves and their clients and stakeholders. The 2013 Notice recommended various cyber security measures (e.g. educating staff, following guidance and best practices from industry associations and information security organizations, conducting regular vulnerability and security tests and assessments, and regularly reviewing cybersecurity control measures) and emphasized the need for financial market participants to have a risk management system that addresses cyber risks in accordance with prudent business practices. The 2013 Notice also encouraged issuers to consider the need for cyber risk disclosures in prospectuses and continuous disclosure filings.

The CSA's 2016 Notice

In September 2016, the CSA published Staff Notice 11-332 Cyber Security as a replacement for the 2013 Notice. The 2016 Notice highlights the importance of cyber risks for financial market participants, outlines the CSA's cyber security initiatives to assess and promote market participant readiness and resilience, references relevant standards and guidance documents, and sets out general expectations for market participants' cyber risk management activities.

The 2016 Notice lists some cyber security guidance documents issued by regulatory authorities and standard-setting bodies, and summarizes some of the key recommendations, including:

- manage cyber security at an organizational level, with executive and board level responsibility and accountability;
- organize cyber security activities to "Identify, Protect, Detect, Respond, and Recover";
- establish and maintain a robust cyber security awareness program for staff;
- understand business drivers and security considerations specific to the use of technology, systems and networks;
- understand the likelihood that a cyber incident will occur and the resulting impact to determine an acceptable level of risk according to risk tolerance, budget and legal requirements;
- manage cyber security risks arising from the use of services provided by independent vendors;
- consider a methodology to protect individual privacy and cyber security breach reporting obligations;
- consider sharing information about cyber incidents with other organizations;
- communicate, collaborate and coordinate with other organizations;
- stablish plans to promptly restore capabilities or services impaired by a cyber incident;
- and update and improve cyber security programs on an ongoing basis.

The 2016 Notice sets out the CSA's expectations for financial market participants' cyber risk management activities, as follows:

- **Issuers:** Provide detailed and specific disclosures of material cyber risks in prospectuses and continuous disclosure filings. Have a cyber-attack remediation plan that includes how the materiality of a cyber-attack will be assessed (including the impact on the issuer's operations and reputation, customers, employees and investors) to "determine whether and what, as well as when and how, to disclose in the event of an attack".
- **Registrants:** Remain vigilant in developing, implementing and updating an approach to cyber security hygiene and management. Review and follow guidance issued by self- regulatory organizations (e.g. IIROC and the MFDA).

- **Regulated Entities:** Examine and review compliance with securities laws and recognition, registration or exemption orders, including the need to have internal controls over systems and to report security breaches. Adopt an appropriate cyber security framework provided by a regulatory authority or standard-setting body.

Comment

Cyber risk management guidance issued by domestic and foreign financial industry regulators, while directed to financial market participants, can be helpful for all organizations. The regulatory guidance might also be considered by Canadian courts when determining whether an organization and its directors and management used reasonable care to manage cyber risks. For more information about cyber risk management guidance from financial industry regulators, see the following BLG bulletins: Cybersecurity Guidance From Investment Industry Organization (May 2016), 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).

By

Bradley Freedman

Expertise

Cybersecurity, Privacy & Data Protection

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749