OCTOBER 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Cybersecurity Guidance from Canadian Securities Administrators

On October 19, 2017, the Canadian Securities Administrators ("CSA") published *Staff Notice 33-321 Cyber Security and Social Media* to report on a survey of cybersecurity and social media practices by firms registered to trade securities or to advise clients regarding securities, and to provide firms with detailed guidance regarding their cybersecurity and social media practices. The Staff Notice supplements the CSA's 2016 *Staff Notice 11-332 Cyber Security*. The cybersecurity guidance is useful for all kinds of organizations.

The CSA's 2016 Cyber Security Staff Notice

In September 2016, the Canadian Securities Administrators published *Staff Notice 11-332 Cyber Security* to emphasize the need for firms to follow guidance issued by regulatory authorities and standards organizations to proactively manage cyber risks and prepare for cybersecurity incidents. The Notice highlights the importance of cyber risks for securities market participants, references relevant standards and guidance documents, and sets out general expectations for firms' cyber risk management activities. For more information, see BLG bulletin *Cyber Risk Management – Regulatory Guidance from the Canadian Securities Administrators*.

The CSA's 2017 Cyber Security and Social Media Staff Notice

The CSA's October 2017 *Staff Notice 33-321 Cyber Security and Social Media* reports on the results of a CSA survey of firms' cybersecurity and social media practices. The Staff Notice reminds that securities market participants are a known target of cyber criminals, and emphasizes that all firms, regardless of size or functions outsourced to related entities, should have appropriate cybersecurity policies and procedures. The Staff Notice also provides specific guidance for cybersecurity practices. Following is a summary.

1. Cybersecurity Policies/Procedures

Firms should have cybersecurity policies and procedures designed to safeguard the confidentiality, integrity and availability of the firm's data (including clients' personal information). The policies and procedures should address: use of electronic communications; use of electronic devices; loss or disposal of electronic devices; use of public electronic devices or public internet connections to remotely access the firm's network and data; detecting unauthorized activity on the firm's network or electronic devices; ensuring software is updated in a timely manner; overseeing third-party vendors or service providers with access to the firm's network or data; and reporting cybersecurity incidents to the firm's board of directors (or equivalent). The policies and procedures should be reviewed and updated frequently.

2. Training

Firms should educate and train their employees about cyber risks and the firm's cybersecurity policies and procedures. The training should include: recognizing risks; the types of cyber threats that employees may encounter and how to respond to those threats; handling confidential information; use of passwords; security of electronic devices; and escalating cybersecurity incidents.

3. Risk Assessments

Firms should conduct periodic (at least annual) cybersecurity risk assessments that include: an inventory of the firm's critical assets and confidential data; aspects of the firm's operations that are vulnerable to internal and external cyber threats; how cyber threats and vulnerabilities are identified; the potential consequences of identified cyber threats; and the adequacy of the firm's preventative controls and incident response plan.

4. Incident Response Plan

Firms should have a written cybersecurity incident response plan that includes: the incident response team; a description of the different types of incidents; procedures to stop an incident and eliminate the threat; procedures for recovery of data; investigation of an incident; and incident notification and reporting obligations.

5. Due Diligence of Service Providers

Firms should limit access by third-party vendors, consultants or other service providers to the firm's systems and data. Firms should periodically evaluate the adequacy of safeguards against cybersecurity incidents involving service providers and the handling of those incidents by service providers. Written agreements with service providers should include cybersecurity provisions. Firms should understand the cybersecurity practices of cloud service providers, and have procedures in place if data stored in a cloud service is not accessible.

6. Data Protection

Firms should use encryption and passwords to protect data and sensitive information stored on all computers and other electronic devices, and data that is accessible using communications portals. Firms should back up their data to a secure off-site server and regularly test the back-up process.

7. Insurance

Firms should review their existing insurance policies for cybersecurity coverage, and should consider obtaining additional insurance for coverage gaps.

Comment

The CSA's guidance is generally consistent with similar guidance issued by other regulators and self-regulatory organizations. Cyber risk management guidance issued by securities industry regulators can be helpful for organizations of all kinds. For more information about cyber risk management guidance from securities industry regulators, see the following BLG bulletins: *New York State Cybersecurity Regulation for Financial Services Companies*; *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*; *Cyber Risk Management Guidance for Corporate Directors*; *Cyber-Risk Management Guidance from Financial Institution Regulators*; *Regulatory Guidance for Cyber Risk Self-Assessment*. ■

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's Investment Management Group has experience working with registrants on cybersecurity policies and procedures and would be pleased to assist you and your organization. If you have any questions, please contact the author of this bulletin, your BLG lawyer or the leaders of our Investment Management Group.

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

BLG Investment Management Group – Key Contacts

John E. Hall	Toronto	416.367.6643
Jason J. Brooks	Vancouver	604.640.4102
Jonathan L. Doll	Calgary	403.232.9659
Christian Faribault	Montréal	514.954.2501
Lynn M. McGrade	Toronto	416.367.6115

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com