OCTOBER 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

G-7 Guidelines for Cybersecurity Assessment

On October 13, 2017, the Group of Seven countries, including Canada, the United Kingdom and the United States (the "G-7"), issued a report titled *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector* (the "G7FEA") to provide guidance for effective cybersecurity assessments by financial sector organizations. The G7FEA supplements the cybersecurity guidance in the G-7's 2016 report titled *G7 Fundamental Elements of Cybersecurity for the Financial Sector* (the "G7FEC"). The guidance is useful for organizations of all kinds and sizes.

G-7 Fundamental Elements of Cybersecurity

The G7FEC describe eight basic building blocks for the design and implementation of a cybersecurity strategy and operating framework for financial sector organizations: strategy and framework, governance, risk and control assessment, monitoring, response, recovery, information sharing and continuous learning. For more information, see BLG bulletin *Cyber Risk Management – G7 Cybersecurity Guidelines for the Financial Sector*.

G-7 Fundamental Elements for Effective Assessment

The G7FEA is designed to promote the effective cybersecurity practices outlined in the G7FEC by specifying: (a) desirable cybersecurity outcomes; and (b) assessment components to promote the quality of the assessments and facilitate continuous improvement.

Part A – Desirable Outcomes

The desirable outcomes are broad, demonstrable characteristics of a mature cybersecurity program. The outcomes are as follows:

- The Fundamental Elements are in place: An organization should implement the G7FEC as the foundational elements for its cybersecurity program.
- Cybersecurity influences organizational decision-making: Cybersecurity should be a key strategic consideration when developing new products/services and when assessing business operations. Directors and senior management should have oversight of the design, implementation and effectiveness of cybersecurity programs.
- There is an understanding that disruption will occur: An organization should accept that cybersecurity incidents will occur, and achieve balance across all aspects of the G7FEC to properly prepare for responding to and recovering from cybersecurity incidents.
- An adaptive cybersecurity approach is adopted: A cybersecurity program should foster an environment of continuous improvement and learning so that cybersecurity procedures reflect the ever-changing landscape.
- There is a culture that drives secure behaviors: Effective cybersecurity should be embedded into the fabric of an organization, and should include people, processes and technical solutions. Training and awareness are essential.

Part B – Assessment Components

The assessment components are designed to assist organizations to develop an effective cybersecurity assessment framework and to conduct effective assessments of performance against intended outcomes and provide feedback and identify areas for improvement. The components are as follows:

- Establish clear assessment objectives: Assessments should have clear objectives to confirm the scope of the assessment and provide clarity of motivation and facilitate accountability.
- Set and communicate methodology and expectations: Assessments should be based on clear and measurable expectations and a suitable methodology, all based on consideration of relevant cybersecurity guidance and frameworks.

- Maintain a diverse toolkit and process for tool selection: Assessments should use a diverse portfolio of assessment tools and techniques, which are selected using a defined process and evaluated regularly to ensure that they remain fit for purpose.
- Report clear findings and concrete remedial actions: Assessment reports should have clear conclusions and identify specific remedial measures and actionable findings.
- Ensure assessments are reliable and fair: Assessments should be conducted by competent individuals with appropriate skills and knowledge that are continuously updated. Assessments should be subject to independent review.

Comment

The G7FEA are generally consistent with cyber risk management guidance issued by Canadian government agencies, regulators and self-regulatory organizations. For example, see Office of the Superintendent of Financial Institutions *Cyber Security Self-Assessment Guidance*; Investment Industry Regulatory Organization of Canada *Cybersecurity Best Practices Guide for IIROC Dealer Members* and *Cyber Incident Management Planning Guide for IIROC Dealer Members*, and *Securing Personal Information: A Self-Assessment Tool for Organizations* published jointly by the Privacy Commissioners of Canada, British Columbia and Alberta.

An organization's assessment of its cybersecurity maturity may result in the creation of sensitive communications and documents that may be subject to disclosure in connection with contractual audits, regulatory investigations and proceedings and civil lawsuits, unless the communications and documents are protected by legal privilege. For those reasons, organizations should consider implementing a legal privilege strategy designed to establish legal privilege over communications and documents made in the course of cybersecurity assessments. For more information, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*, *Cyber Risk Management – Legal Privilege Strategy (Part 2)* and *Legal Privilege for Data Security Incident Investigation Reports*. ■

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

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