Cyber Risk Management – G7 Cybersecurity Guidelines For The Financial Sector

October 17, 2016

On October 14, 2016, the Government of Canada announced its endorsement of the *G7 Fundamental Elements of Cybersecurity for the Financial Sector* guidelines adopted by the Group of Seven ("G7") to assist financial sector entities to design and implement a suitable cybersecurity strategy and operating framework. The guidelines are 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.

Financial institutions can be particularly vulnerable to cyber risks, due to the pervasive use of information technology systems by financial sector entities and the interconnected nature of global financial systems. Cyber criminals have repeatedly targeted financial institutions around the world, including several recent breaches of the international financial messaging system.

G7 Cybersecurity Guidelines

The *G7 Fundamental Elements of Cybersecurity for the Financial Sector* are non-binding guidelines for financial sector private and public entities to help them design and implement, and regularly review, a cybersecurity strategy and operating framework that

is suitable to their particular circumstances, risk management practices and culture, and thereby improve the cybersecurity and resilience of international financial systems.

The guidelines warn that cyber risks are growing more dangerous and diverse, and threaten to disrupt interconnected global financial systems and the institutions that operate and support those systems.

The guidelines explain that Canadian officials from Department of Finance Canada, Office of the Superintendent of Financial Institutions and Bank of Canada worked with G7 counterparts to identify cybersecurity measures for the financial sector and best practices that could be applied across the G7 countries (Canada, France, Germany, Great Britain, Italy, Japan and the United States).

The guidelines describe eight basic building blocks for a cybersecurity strategy and operating framework. Following is a summary:

- Cybersecurity Strategy and Framework: Establish and maintain a cybersecurity strategy and framework (to specify how to identify, manage and reduce cyber risks effectively in an integrated and comprehensive manner) that is suitable for the entity, tailored to specific cyber risks and appropriately informed by international, national and industry standards and guidelines.
- Governance: Define and facilitate performance of roles and responsibilities (including internal communications, reporting and escalation) for personnel implementing, managing and overseeing the cybersecurity strategy and framework to ensure accountability; and provide adequate resources, appropriate authority and access to the entity's governing authority (e.g. board of directors). The governing authority should establish the entity's cyber risk tolerance and oversee the design, implementation and effectiveness of the cybersecurity program.
- Risk and Control Assessment: Identify and assess relevant cyber risks to all functions, activities, products and services throughout the entity and interconnections, dependencies and third parties, and identify and implement controls (including systems, policies, procedures and training) to protect against and manage those risks within the tolerance set by the governing authority.
- Monitoring: Establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits and exercises.
- Response: Timely assess the nature, scope and impact of a cyber incident; contain the incident and mitigate its impact; notify internal and external stakeholders (e.g. law enforcement, regulators, shareholders, service providers and customers); and coordinate joint response activities. Establish, implement and exercise incident response policies and procedures.
- Recovery: Resume operations responsibly, while allowing for continued remediation and preventative activities. Establish and test contingency plans for essential activities and key processes.
- Information Sharing: Share reliable, actionable cybersecurity information with internal and external stakeholders to enhance defenses, limit damage, increase situational awareness and broaden learning.
- Continuous Learning: Systematically review the cybersecurity strategy and framework regularly and when events warrant to address changes in cyber risks, best practices and technical standards (within the financial industry sector and

other sectors), allocate resources, identify and remediate gaps and incorporate lessons learned.

Comment

The G7 cybersecurity guidelines are consistent with cyber risk management guidance previously issued by Canadian financial industry regulators and self-regulatory organizations, including Canadian Securities Administrators, Mutual Fund Dealers Association of Canada, Investment Industry Regulatory Organization of Canada and Office of the Superintendent of Financial Institutions of Canada. While the G7 cybersecurity guidelines are directed to the financial sector, they provide a helpful summary of some basic cyber risk management practices and considerations that are useful for all organizations.

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

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

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription

preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.