APRIL 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

New York State Cybersecurity Regulation for Financial Services Companies

On March 1, 2017, the New York State Department of Financial Services' *Cybersecurity Requirements for Financial Services Companies* (the "Regulation") came into effect. The Regulation establishes minimum cybersecurity standards for banks, insurance companies and financial services companies regulated by New York State law to ensure the safety and soundness of regulated entities and to protect their customers. The Regulation is a helpful benchmark for Canadian organizations of all kinds and sizes.

Overview

The stated purpose of the Regulation is to protect New York State's financial services industry and consumers from the "ever-growing threat of cyber-attacks". The Regulation requires each regulated entity to assess its cybersecurity risk profile and design a program that addresses relevant cybersecurity risks in a robust fashion. The Regulation urges regulated entities to "move swiftly and urgently to adopt a cybersecurity program". The Regulation requires a regulated entity's senior management to take cybersecurity seriously and to be responsible for the entity's cybersecurity program, including by filing annual compliance certificates. Regulated entities must also promptly report material cybersecurity events to the superintendent. The Regulation came into effect on March 1, 2017, but there are transition periods (ranging from 180 days to two years) for compliance with certain requirements of the Regulation.

Details

Following is a summary of some key elements of the Regulation.

Cybersecurity Program: A regulated entity must maintain a cybersecurity program, based on the entity's risk assessment, designed to protect the confidentiality, integrity and availability of the entity's information systems and data. The cybersecurity program must perform the following functions: (1) identify and assess internal and external cybersecurity risks to the entity's information systems and data; (2) use defensive infrastructure and implement policies and procedures to protect the entity's information systems and data from unauthorized access, use or other malicious acts; (3) detect, respond to and recover from cybersecurity events and restore normal operations and services; and (4) fulfil applicable reporting obligations.

Cybersecurity Policy: A regulated entity must implement and maintain a written policy setting out the entity's policies and procedures for the protection of its information systems and data. The policy must be based on the entity's risk assessment and must address the following areas to the extent applicable: (1) information security; (2) data governance and classification; (3) asset inventory and device management; (4) access controls and identity management; (5) business continuity and disaster recovery planning and resources; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data privacy; (12) vendor and third party service provider management; (13) risk assessment; and (14) incident response. The policy must be approved by a senior officer of the entity or the entity's board of directors (or appropriate committee) or equivalent governing body.

Chief Information Security Officer: A regulated entity must designate a qualified individual (known as the "CISO") responsible for overseeing and implementing the entity's cybersecurity program and enforcing the entity's cybersecurity policy. The CISO may be employed by an affiliate of the entity or an independent service provider. The CISO must deliver annually a written report on the entity's cybersecurity program and material cybersecurity risks to the entity's board of directors or equivalent governing body or responsible senior officer. The CISO must consider, to the extent applicable: (1) the confidentiality of data and the integrity and security of the entity's information systems; (2) the entity's cybersecurity policies and procedures; (3) material cybersecurity risks to the entity; (4) overall effectiveness of the entity's cybersecurity program; and (5) material cybersecurity events involving the entity during the reporting period.

Risk Assessment: A regulated entity must conduct a periodic risk assessment of the entity's information systems sufficient to inform the design of the entity's cybersecurity program. The risk assessment must be updated as reasonably necessary to address changing circumstances, allow for revision of controls to respond to technological developments and evolving threats, and consider the particular risks to the entity's business operations, data collected or stored, information systems and availability and effectiveness of security controls. The risk assessment must be documented and carried out in accordance with written policies and procedures that include: (1) criteria for evaluating and categorizing relevant cybersecurity risks; (2) criteria for assessing the confidentiality, integrity, security and availability of the entity's information systems and data; and (3) requirements describing how identified risks will be mitigated or accepted and how the entity will address those risks.

Audit Trail: A regulated entity must maintain systems that, to the extent applicable based on its risk assessment, are designed to reconstruct material transactions sufficient to support the entity's normal operations and obligations and include audit trails designed to detect and respond to cybersecurity events that are likely to materially harm the entity's normal operations. The records created by those systems must be maintained for minimum retention periods.

Personnel/Intelligence: A regulated entity must: (1) engage qualified cybersecurity personnel, in addition to its CISO, sufficient to manage the entity's cybersecurity risks and perform or oversee performance of the entity's cybersecurity program; (2) provide its cybersecurity personnel with sufficient cybersecurity updates and training; and (3) verify that its cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. The required cybersecurity personnel may be sourced from an affiliate of the entity or an independent service provider.

Third Party Service Provider Security Policy: A regulated entity must implement written policies and procedures, based on the entity's risk assessment, designed to ensure the security of information systems and data accessible to or held by the entity's third party service providers. The policies and procedures, and related guidelines, must address, to the extent applicable, risk identification and assessment of service providers, minimum required cybersecurity practices to be followed by service providers, due diligence processes for assessing service providers' cybersecurity practices and periodic reassessments of service providers.

Multi-Factor Authentication: Based on a regulated entity's risk assessment, the entity must use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to the entity's information systems or data. The entity must use multi-factor authentication for external access to the entity's internal networks unless the entity's CISO has approved reasonably equivalent or more secure access controls.

Other Requirements: A regulated entity's cybersecurity program must include the following:

- **Testing/Assessments**: Monitoring and testing to assess the effectiveness of the entity's cybersecurity program, including either continuous monitoring or annual penetration testing and bi-annual vulnerability assessments.
- **Access Privileges**: Limited user access privileges to the entity's information systems that contain sensitive data, and periodic review of those access privileges.
- **Application Security**: Written procedures, guidelines and standards for the security of software applications (both internally and externally developed) used by the entity in its technology environment. The procedures, guidelines and standards must be periodically reviewed, assessed and updated.
- **Limited Data Retention**: Secure, periodic disposal of data that is no longer necessary for the entity's business operations or legitimate business purposes, except where a legal retention requirement applies or targeted disposal is not feasible.
- **Monitoring/Training**: Risk-based monitoring of authorized users to detect unauthorized access to or use of data, and regular cybersecurity awareness training for all personnel.
- **Encryption**: Controls (including encryption) to protect data (both in transit over external networks and at rest) held or transmitted by the entity, provided that if encryption is infeasible then the entity may instead secure the information using effective alternative compensating controls reviewed and approved, and annually reassessed, by the CISO.
- **Incident Response Plan**: A written incident response plan designed to enable the entity to promptly respond to, and recover from, any cybersecurity event that materially affects the confidentiality, integrity or availability of the entity's information systems or the continuing functionality of any aspect of the entity's business or operations. The incident response plan must address: (1) internal processes for responding to a cybersecurity event; (2) goals of the incident response plan; (3) roles, responsibilities and levels of decision-making authority; (4) external and internal communications and information sharing; (5) requirements for the remediation of identified weaknesses in information systems and associated controls; (6) documentation and reporting; and (7) evaluation and revision of the incident response plan after a cybersecurity event.

Comment

The Regulation is a helpful summary of current cyber risk management best practices, and provides a useful benchmark for Canadian organizations of all kinds and sizes to assess their cyber risk management program. The cyber risk management practices required by the Regulation are consistent with guidance issued by Canadian financial industry regulators and self-regulatory organizations. For more information, see the following BLG bulletins: *Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents* (January 2017); *G7 Cybersecurity Guidelines for the Financial Sector* (October 2016); *Regulatory Guidance from the Canadian Securities Administrators* (September 2016); *Cybersecurity Guidance from Investment Industry Organization* (May 2016); *Cybersecurity Guidance from Investment Industry Organization* (January 2016); *Regulatory Guidance for Cyber Risk Self-Assessment* (November 2013). ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

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

For more information about cyber risk management and BLG's related legal services, please see the BLG website.

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com