September 16, 2016

ARTICLE

Cyber Risk Management – New York State Regulation For Financial Institutions

On September 13, 2016, the New York State Department of Financial Services published for comment a proposed cybersecurity regulation for the financial industry. The regulation provides important, detailed guidance for all organizations to help manage cyber risks.

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 sensitive, regulated or protected 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 increasing sophistication and complexity of cyber-attacks, increasing use of information technology and data, increasing regulation and increasing legal liability. Commentators have said that there are only two kinds of organizations – those that have been hacked and know it, and those that have been hacked and don't know it yet.

New York State Regulation

The proposed regulation titled “Cybersecurity Requirements for Financial Services Companies” was issued by the New York State Department of Financial Services to address the ever-growing cyber risk threat to information and financial systems. The regulation is intended to set minimum cybersecurity standards for banks, insurance companies and financial services companies to protect customer information and information technology systems. The regulation requires each regulated institution to implement a robust cybersecurity program designed for the institution's specific risk profile to ensure the safety and soundness of the institution and protect its customers, and to cause the institution's senior management to take cybersecurity seriously and to be responsible for the institution's cybersecurity program. Following is a summary.

A. Cybersecurity Program

A regulated institution will be required to establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of information systems and to perform the following core cybersecurity functions: (1) identify internal and external cyber risks; (2) use defensive infrastructure and implement policies and procedures to protect its information systems and nonpublic information from unauthorized access, use or other malicious acts; (3) detect, respond to and recover from cybersecurity events; and (4) fulfil reporting obligations.

B. Cybersecurity Policy

A regulated institution will be required to establish and maintain a written cybersecurity policy setting out the institution's policies and procedures for the protection of its information systems and nonpublic information. The policy must address, at a minimum: (1) information security; (2) data governance and classification; (3) access controls and identity management; (4) business continuity and disaster recovery planning and resources; (5) capacity and performance planning; (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. As frequently as necessary, and at least annually, the policy must be reviewed by the institution's board of directors or equivalent governing body and approved by a senior officer of the institution.

C. Chief Security Officer

A regulated institution will be required to designate a qualified Chief Information Security Officer (“CISO”) responsible for overseeing and implementing the institution's cybersecurity program and enforcing its cybersecurity policy. At least bi-annually, the CISO must present to the institution's board of directors or equivalent governing body a written report to: (1) assess the confidentiality, integrity and availability of the institution's information systems; (2) detail exceptions to the institution's cybersecurity policies and procedures; (3) identify cyber risks to the institution; (4) assess the effectiveness of the institution's cybersecurity program; (5) propose steps to remediate identified deficiencies; and (6) summarize all material cybersecurity events that affected the institution during the reporting period.

D. Specific Requirements for Cybersecurity Program

A regulated institution's cybersecurity program must include the following:

- Testing/Assessments: Annual penetration testing of the institution's information systems, and quarterly vulnerability assessments of the institution's information systems.
- Audit Trail: Audit trail systems to enable reconstruction of transactions to detect and respond to cyber events, to log privileged user access to critical systems, to protect audit trail data from alteration, to protect hardware integrity, to log system events and to maintain audit data for at least six years.
- Access Privileges: Limited access privileges to the institution's information systems that contain nonpublic information, 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) that are reviewed and updated by the CISO at least annually.
- Risk Assessment: A documented annual risk assessment of the institution's information systems in accordance with written policies and procedures setting out: the criteria for evaluating and categorizing risks; the criteria for assessing the confidentiality, integrity, and availability of the institution's information systems; and requirements for documenting how identified risks will be mitigated or accepted, justifying those decisions, and assigning accountability for the identified risks.

- Personnel/Intelligence: Employment of knowledgeable and trained cybersecurity personnel, or engagement of third party service providers, to manage cybersecurity risks, perform cybersecurity functions and to be aware of changing cybersecurity threats and countermeasures.
- Third Parties: Written policies and procedures to ensure the security of information systems and nonpublic data accessible to, or held by, third parties doing business with the institution. The policies and procedures should address: risk identification and assessment; minimum required cybersecurity practices; due diligence processes; annual reassessments; and preferred contract provisions dealing with use of multi-factor authentication and encryption, notice and response to cybersecurity events, assurances regarding anti-malware protection and audit rights.
- Authentication: The use of multi-factor authentication and risk-based authentication in various circumstances.
- Data Retention: The timely destruction of nonpublic information that is no longer necessary, except where a legal retention requirement applies.
- Monitoring/Training: The monitoring of authorized users to detect misconduct and unauthorized access, and regular cybersecurity awareness training for all personnel.
- Encryption: The protection of all nonpublic information, held or transmitted by the institution, by using encryption or appropriate alternative compensating controls.
- Incident Response Plan: A written incident response plan for the institution to promptly respond to, and recover from, any cybersecurity event.

E. Reporting/Records

A regulated institution will be required to give the regulator prompt notice (within 72 hours) of any cybersecurity event that is reasonably likely to materially affect the normal operation of the institution or that affects nonpublic information.

On an annual basis, a regulated institution will be required to submit to the regulator a written compliance certificate, signed by the chairperson of the institution's board of directors or a senior officer, certifying that the institution is in compliance with the regulation and providing details of planned remedial efforts for identified deficiencies. The institution will also be required to retain all records and data supporting the certificate.

F. Application/Transition/Enforcement

The regulation is effective January 1, 2017, but provides a 180-day transition period. The regulation applies to any person or legal entity regulated by New York state banking, insurance or financial services laws. There is a limited exemption from compliance with a few elements of the regulation for smaller institutions (less than 1,000 customers, and less than $5 million gross annual revenue and less than $10 million in total assets). The regulator may enforce the regulation using the regulator's authority under any applicable laws.

Comment

Cybersecurity regulations and guidance issued by domestic and foreign government agencies, industry organizations and regulators will likely be considered by Canadian courts when determining whether an organization and its directors and management used reasonable care to manage cyber risks. The proposed New York state regulation provides a helpful checklist of some cyber risk management practices and considerations that are useful for all organizations. ulators (March 2015) and Regulatory Guidance for Cyber Risk Self-Assessment (November 2013).

Services: Cybersecurity, Privacy & Data Protection

Related Expertise

Cybersecurity, Privacy & Data Protection