Bulletin | Cybersecurity, Privacy and Data Protection

April 2020

SEC publishes report on cybersecurity and resiliency practices

In January 2020, the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") published *Cybersecurity and Resiliency Observations* to help market participants and other firms enhance cybersecurity preparedness and operational resiliency. The OCIE's observations are based on its examinations of broker-dealers, investment advisors and other SEC registrants. The observed best practices summarized by the OCIE are useful guidance for organizations of all sizes and in all industries.

Cyber risk management

Cyber risks are risks of loss/harm (e.g. business disruption loss, financial loss, reputational harm, trade secret disclosure and other competitive harm) and costs/liabilities (e.g. incident response and remediation costs, litigation/regulatory proceeding costs, and liabilities to stakeholders, business partners, customers and regulators) suffered or incurred by an organization as a result of a failure or breach of the information technology systems used by or on behalf of the organization or its business partners (e.g. vendors/suppliers and service providers), including incidents involving loss or theft of, or unauthorized access, use, disclosure, modification or deletion of, data in the organization's possession or control. Cyber risks can result from internal sources (e.g. employees, contract workers and system failures) or external sources (e.g. nation-states, terrorists, competitors, hackers, fraudsters and acts of nature).

Cyber risks are relevant to almost any organization, regardless of size or industry, because almost all organizations use or depend on information technology and data to operate their business. Cyber risks appear to be increasing in frequency, intensity and harmful consequences as a result of various circumstances, including: increasing use of, and dependency on, information technology and data; increasing sophistication and complexity of cyber-attacks; and evolving legal requirements and liabilities. Commentators have said 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.

OCIE's observations

The OCIE's observations focus on seven aspects of a successful cyber risk management program: governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness. Following is a summary.

1. **Governance and risk management:** A governance and risk management program to provide structure and oversight to cybersecurity and resiliency activities, including: (a) senior level engagement; (b) risk assessments to identify, analyze, and prioritize relevant cybersecurity risks; (c) written policies and procedures to address identified cybersecurity risks; and (d) effective implementation and enforcement of those policies and procedures, including testing and monitoring, effective communication, and continuous evaluation and adaptation.
2. **Access rights and controls:** Access rights and controls to protect information technology systems and data against unauthorized access and use, including: (a) understanding the location of data throughout an organization; (b) restricting access to systems and data to authorized users based on their legitimate needs; and (c) establishing and effectively implementing appropriate technological measures (including strong passwords and multi-factor authentication) to prevent and monitor for unauthorized access.
3. **Data loss prevention:** Tools and processes to ensure that sensitive data is not lost, misused, or accessed by unauthorized persons, including: (a) vulnerability scanning; (b) perimeter security; (c) detective security; (d) patch management; (e) hardware and software inventory control; (f) encryption and network segmentation; (g) insider threat monitoring; and (h) securing legacy systems and equipment.
4. **Mobile security:** Measures to manage cybersecurity risks associated with mobile devices and mobile applications, including: (a) policies and procedures for the use of mobile devices; (b) mobile device management (MDM) technologies and security measures for all mobile devices (including personal devices used for business purposes); and (c) training relevant individuals on the safe use of mobile devices.
5. **Incident response and resiliency:** An incident response plan for various plausible scenarios that includes: (a) timely notification and response; (b) procedures for internal escalation and communication with key stakeholders; (c) compliance with legal reporting and notification obligations, including reports to regulators and notices to customers and affected individuals; (d) designated incident response team members with assigned roles and responsibilities; and (e) improvements based on testing the plan and lessons learned from post-incident assessments. Practices to improve operational resiliency, including: (1) a prioritized inventory of business services and supporting systems and processes; (2) a strategy for operational resiliency with appropriate risk tolerances; (3) secure offline data backups; and (4) cybersecurity insurance (if appropriate).
6. **Vendor management:** Practices and controls to manage cybersecurity risks resulting from vendor relationships, including: (a) a vendor management program (including appropriate due diligence for vendor selection) to manage risks associated with vendor relationships and to ensure vendors meet security requirements and implement safeguards; (b) procedures for terminating or replacing vendors, including cloud-based service providers; (c) understanding and managing vendor relationships and applicable contracts; and (d) monitoring/overseeing vendors to ensure their compliance with applicable contracts and to identify changes to vendors' services or personnel.
7. **Training and awareness:** Continuously evaluated and updated training and exercises for staff to improve their awareness of cyber threats and understanding of cybersecurity policies/procedures, and to establish a culture of cybersecurity readiness and operational resiliency.

The OCIE encourages market participants to review their practices, policies and procedures against the observed best practices to improve their cybersecurity and resiliency.

Comment

The OCIE's observations provide a helpful summary of some basic cyber risk management best practices that are useful for organizations of all sizes and in all industries, and are consistent with guidance issued by Canadian government agencies, privacy commissioners, financial industry regulators and self-regulatory organizations. For example, see BLG bulletins *Financial Industry Regulator Issues Cybersecurity Guidance*; *Investment Funds Institute of Canada Issues Cybersecurity Guide*; *Cybersecurity Guidance for Small and Medium Organizations*; and *Cybersecurity Guidance from Canadian Securities Administrators*.

An organization's cyber risk management activities can result in sensitive communications and documents that might be subject to mandatory disclosure in regulatory investigations and litigation relating to a cybersecurity incident, unless the communications and documents are protected by legal privilege. Organizations engaged in cyber risk management activities should consider implementing a legal privilege strategy to help establish legal privilege where appropriate, and to help avoid inadvertent and unnecessary disclosures of privileged legal advice. For more information, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*; *Cyber Risk Management – Legal Privilege Strategy (Part 2)*; *Legal Privilege for Data Security Incident Investigation Reports*; and *Loss of Legal Privilege over Cyberattack Investigation Report*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

blg.com | Canada's Law Firm
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.

© 2020 Borden Ladner Gervais LLP. BD9671–04–20

Borden Ladner Gervais