January 12, 2016

ARTICLE

Cybersecurity Guidance From Investment Industry Organization

Cyber risk management is an increasingly important challenge for organizations of all kinds. The Investment Industry Regulatory Organization of Canada (IIROC), the national self-regulatory organization that oversees investment dealers and their trading activity in Canadian markets, has published detailed guidance to help investment dealer firms manage cybersecurity risks. The guidance provides useful checklists and helpful summaries of industry standards and best practices. The guidance emphasizes the need for organizations to proactively manage cyber risks and to prepare for cybersecurity incidents.

Cyber Risks

Cyber risks are the risks of harm, loss and liability (e.g. business disruption, trade secret disclosure, financial loss, loss to stakeholder value, reputational 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 organization's information technology systems. 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 appear to be 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.

Cybersecurity Best Practices Guide

IIROC's *Cybersecurity Best Practices Guide* sets out a voluntary, risk-based cybersecurity framework, comprised of industry standards and best practices, to manage cyber risks. The Guide's stated purpose is to provide an understanding of standards-based security controls that make up a best practices cybersecurity program. The Guide emphasizes that cybersecurity is a multi-faceted challenge that requires an enterprise-wide, interdisciplinary approach to implement a comprehensive strategy to avoid, mitigate, accept or transfer cyber risks.

The Guide discusses best practices relating to governance and risk management, insider risk, physical and environmental security, awareness and training, threat assessment, network security, information system protection, user management and access controls, asset management, incident response, information sharing and breach reporting, cyber insurance, vendor risk management and cybersecurity policies. The Guide includes a Cybersecurity Incident Checklist and a Sample Vendor Assessment form.

The Guide identifies the following key points:

- Governance: A sound governance framework — strong leadership, board and senior management engagement and a clear accountability — are essential for a successful cybersecurity program.
- Training: Effective training of personnel can significantly reduce the likelihood of successful cyber-attacks.
- Technical Controls: A cyber risk management program should include technical controls appropriate for the organization's particular circumstances.
- Service Providers: An organization should exercise strong due diligence and implement clear performance and verification policies to manage cyber risks that arise from relationships with service providers who have access to the organization's sensitive firm or client information or information technology systems.

Cyber Incident Management Planning Guide

IIROC's *Cyber Incident Management Planning Guide* is designed to assist in the preparation of cyber-incident response plans. The Guide emphasizes that an organization must be able to respond to cybersecurity incidents in a consistent, coordinated and timely manner. The Guide explains the five phases of cybersecurity incident management: plan and prepare, detect and report, assess and decide, respond and post-incident activity. The Guide includes recommendations (based on the National Institute of Standards and Technology *Computer Security Incident Handling Guide*) for implementing a cybersecurity incident response plan. The Guide also includes a simple, ten-step guide for how an organization should respond to a cybersecurity incident when the organization is not prepared.

Comment

IIROC's cyber risk management guidance is described as "voluntary", and "not intended to create new legal or regulatory obligations". Nevertheless, guidance issued by IIROC and other financial industry organizations and regulators (e.g. SEC, FINRA, CSA and OSFI) will likely be considered by courts and regulators when determining the reasonable standard of care required of an investment dealer firm that is the victim of a cybersecurity incident. IIROC's guidance, while directed to investment dealer firms, can be helpful for organizations of all kinds.

By: Bradley Freedman

Services: Cybersecurity, Privacy & Data Protection, Technology

---

Related Contacts & Expertise

Bradley Freedman
Senior Counsel

Vancouver

BFreedman@blg.com

604.640.4129

Related Expertise

Cybersecurity, Privacy & Data Protection

Technology