Bulletin | Cybersecurity, Privacy and Data Protection

May 2020

Investment industry organization provides additional cybersecurity guidance

In January 2020, the Investment Industry Regulatory Organization of Canada (IIROC) – the national self-regulatory organization that oversees investment dealers and their trading activity in Canadian markets – published a *Cyber Governance Guide* to provide its dealer members with guidance on how to implement, manage and advance a cybersecurity program. The Guide is useful for organizations of all sizes and in all industries.

Cybersecurity and regulatory guidance

Cybersecurity refers to an organization's use of various controls (based on people, processes and technologies) to manage risks of losses, costs and liabilities suffered or incurred as a result of a failure or breach of the information technology systems used by or on behalf of the organization, or other incidents that compromise the confidentiality, integrity or availability of data in the organization's possession or control. Managing cyber risks is important not only for compelling business reasons but also for compliance with various legal obligations (including obligations to protect personal information) and to avoid potentially devastating legal liabilities.

Over the past few years, Canadian investment and financial industry regulators and self-regulatory organizations – the Canadian Securities Administrators, IIROC, the Mutual Fund Dealers Association of Canada and the Office of the Superintendent of Financial Institutions Canada – have emphasized the importance of cybersecurity, and have issued guidance to help regulated firms improve their cybersecurity maturity and manage cyber risks. See BLG bulletins *Investment Funds Institute of Canada Issues Cybersecurity Guide*; *Cybersecurity Guidance from Canadian Securities Administrators*; and *Cybersecurity Guidance from Investment Industry Organization* (January 2016).

In 2015, IIROC published a *Cybersecurity Best Practices Guide* and a *Cyber Incident Management Planning Guide* to help its dealer members manage cybersecurity risks and respond to cyber incidents. The *Cybersecurity Best Practices Guide* sets out a voluntary, risk-based cybersecurity framework, comprised of industry standards and best practices, to manage cyber risks. The *Cyber Incident Management Planning Guide* is designed to assist in the preparation of cyber incident response plans.

IIROC *Cyber Governance Guide*

IIROC's *Cyber Governance Guide* provides IIROC dealer members with guidance on how to implement, manage and advance a cybersecurity program. The Guide incorporates and expands on IIROC's 2015 *Cybersecurity Best Practices Guide*, and provides information and guidance relevant to organizations in other industries. Following is a summary of some key insights and recommendations in the Guide.

1. Threat environment

Firms should understand their cyber threat environment (i.e. threat actors and their tradecraft), identify their vulnerabilities and prioritize their treatment.

2. Security policy and program governance

The Guide notes as follows:

- **Leadership:** There are specific steps that a firm's directors can take to fulfill their legal duty to oversee the firm's security program.
- **Key elements:** Key elements of a cybersecurity program include: (1) asset inventory; (2) threat risk assessments; (3) written information security program; (4) enforced information security policy; (5) cybersecurity training and awareness for personnel; and (6) vendor risk management.
- **Insurance:** Firms should assess the adequacy of their insurance for losses, liabilities and expenses that might result from a cyber incident.
- **Legal obligations:** Legal obligations regarding cybersecurity and data protection include compliance with personal information protection/privacy laws, laws applicable to the financial industry, and IIROC's cybersecurity incident reporting rules.
- **Security policy:** Firms should have an effectively implemented and comprehensive security policy that addresses physical security, personnel security, cybersecurity and business continuity.

3. Operational framework

The Guide provides the following recommendations for a firm's operating tier framework:

- **NIST CSF:** Use the *NIST Cybersecurity Framework* to assess the firm's cybersecurity preparedness.
- **Phased approach:** Take a phased approach to implementing cybersecurity measures, based on an evaluation of the firm's capabilities and security priorities to maximize the impact of the security measures.
- **Prioritization:** Identify and prioritize feasible and cost-effective cybersecurity improvements in the short, medium and long term.

4. Operational program implementation

The Guide provides the following recommendations for implementing an effective cybersecurity program:

- **Basic steps:** Take the following steps to create and implement a cybersecurity plan: (1) identify sensitive data; (2) identify possible threats; (3) analyze security vulnerabilities; (4) assess the level of risk for each vulnerability; and (5) create and execute the plan.
- **Fundamental goals:** Focus on protecting the confidentiality, integrity and availability of information assets and related systems and services, based on the key functions in the *NIST Cybersecurity Framework*: (1) protect assets with safeguards; (2) detect cyber incidents; (3) respond to cyber incidents; and (4) recover from cyber incidents.
- **Due diligence/duty of care:** Document the effective execution of the cybersecurity program (e.g. regularly reviewed and updated inventories, independent reviews, risk assessments and policies) to help demonstrate due diligence and reasonable care to protect valuable assets and satisfy legal requirements.
- **Preparedness:** Cyber preparedness and resilience require: (1) a well-documented and understood incident response plan; (2) secured and tested data backups; (3) regular cyber incident tabletop exercises and the implementation of key findings; and (4) a regularly updated and tested business continuity plan.
- **Threats/vulnerabilities:** Perform proactive assessments of threats and vulnerabilities, and patch information technology system vulnerabilities.
- **Systems thinking:** Use "systems thinking" (i.e. comprehensive program development rather than point or ad hoc solutions) to develop a comprehensive cybersecurity program that addresses specific and likely threats and vulnerabilities.

5. Best practices

The Guide recommends the following best practices for consideration when designing a cybersecurity plan:

- **Insider threats:** Focus on insider threats, including personnel recruitment and behaviour, by implementing appropriate policies and practices, monitoring and responding to suspicious behaviour, anticipating and managing workplace issues, and using access permissions based on the separation of duties and least privilege.
- **Physical/environmental security:** Implement appropriate physical and environmental security, including the clean desktop principle, restricted physical access, visitor management procedures, computer screen locks, power surge protection and regular data backups.
- **Awareness/training:** Require mandatory cybersecurity training for all personnel.
- **Network security:** Implement network security based on a multi-layered defence-in-depth approach, including firewalls, multi-factor authentication, network segmentation, access controls and monitoring.
- **Wi-Fi security:** Implement wireless network security, including access restrictions, vulnerability assessments, intrusion detection systems, advanced encryption and secure authentication protocols.
- **Remote access:** Secure remote access to information technology networks by training personnel, using secure and properly configured VPN technologies and multi-factor authentication for remote access, and monitoring and logging all remote access sessions.
- **Endpoint security:** Secure all devices used to access information technology networks, including by using automatically updated anti-malware solutions and restricting the use of cloud services and removable data storage devices.
- **IT system protection:** Use appropriate technological measures to protect computer systems and data, including secure backup and recovery processes, anti-malware solutions, controls on the use of removable data storage devices, firewalls, application and operating system security updates, system monitoring and secure remote access to systems.
- **BYOD:** Design and implement a bring-your-own-device policy, based on risk assessments and legal advice, to manage the risks associated with the use of personal devices for business purposes.
- **MDM:** Use mobile device management (MDM) software to secure and enforce policies regarding the use of smartphones, tablets and other mobile devices.
- **Backups:** Establish an appropriate data backup plan for all information systems.
- **Account management:** Implement user account management and access controls, including limited privileged accounts, periodic reviews of all accounts, strong passwords and the use of multi-factor authentication for privileged accounts or accounts with access to sensitive data or systems.
- **Asset management:** Identify and manage all computer systems and software applications.

6. Incident response

The Guide emphasizes the importance of planning and preparing for, and effectively responding to, cybersecurity incidents, and explains that incident response plans should include guidance on compliance with data security incident notification obligations. The Guide references the *Government of Canada Cyber Security Event Management Plan*, the *NIST Computer Security Incident Handling Guide* and the Incident Command System incident response model.

7. Other matters

The Guide addresses other important issues:

- **Information sharing:** Information sharing is an essential element of an effective cybersecurity program and an essential tool for mitigating cyber threats.
- **Vendor/outsourcing risk management:** Firms should implement a vendor risk management program, based on a vendor risk management lifecycle model, that includes: (1) risk ranking vendors; (2) mandatory security policies for vendors; (3) explicit provisions in vendor contracts; and (4) verification of vendor performance. Firms should approach vendor risk management in a tiered fashion, starting with the highest risk relationships.
- **Cloud computing:** Firms should consider the risks and threats involved in using cloud computing services.
- **Managed services:** Firms should consider risks when determining whether to outsource security services and selecting a managed service provider.

Comment

IIROC's *Cyber Governance Guide* provides a helpful summary of some basic cyber risk management best practices. While the Guide is directed to IIROC's member dealers, the information and recommendations in the Guide should be useful for organizations in other industries. It is important to note that there is no one-size-fits-all cybersecurity program, and for most organizations the reasonable management of cyber risks will require the organization to make informed risk-based business decisions.

While the Guide recommends that firms obtain legal advice regarding various cybersecurity issues, the Guide does not discuss the importance of protecting the confidentiality of that advice. Organizations engaged in cyber risk management activities should have an appropriate legal privilege strategy to help avoid involuntary and unnecessary disclosures of privileged legal advice or inadvertent waivers of legal privilege. 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

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.