Cyber Security Frameworks and Self-Assessments

Guidance provided by the Financial and Consumer Affairs Authority of Saskatchewan (FCAA) for prudentially regulated entities.

fcaa.gov.sk.ca
April 1, 2021

Financial and Consumer Affairs Authority

Table of Contents

Background

The FCAA is mandated to oversee the activities of a variety of provincially regulated entities. In some cases, this includes ensuring the financial soundness of the entities or ensuring the entities will be financially responsible in carrying out the regulated business activities (“Prudentially Regulated Entities”). The purpose of regulatory oversight of Prudentially Regulated Entities is to assure the government and the public that these organizations are well governed and managed, are achieving their legislative requirements and will be able to meet their financial obligations incurred to consumers in undertaking the regulated business. The FCAA has identified the need to communicate expectations to Prudentially Regulated Entities regarding the measures they employ to address cyber security risk.

Cyber attacks are increasing in frequency and severity. Recent research on industry trends has shown that increased reliance on technology is not being matched by a commensurate level of cyber security within many organizations.

The purpose of this bulletin is to bring awareness of cyber security issues and resources and to provide high-level guidance to Prudentially Regulated Entities of the FCAA’s expectations that cyber security procedures and controls be developed and implemented at an organizational level. The cyber threat environment is continually changing. Cyber threat actors will shift their activities and targets. A robust cyber security framework helps to mitigate this growing risk.

What is Cyber Security?

Cyber security is the protection of data, information, computers, devices and networks against cyber threats and cyber threat actors.

For the purposes of this Bulletin, we will use the following defined terms:

- **Cyber attack:** a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.

- **Cyber security framework:** a complete set of organizational resources including policies, staff, processes, practices and technologies used to assess and mitigate cyber risks and attacks.

- **Cyber security policy:** a set of documented rules issued by an organization that determines how the organization's information systems will be used, managed and protected from cyber threats.

- **Cyber threat:** a potential activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or its information. When the potential activity is taken or launched against the information system of an individual or organization, it is a cyber attack.

- **Cyber threat actors:** states, groups, or individuals with malicious intent, who aim to take advantage of vulnerabilities within a system to obtain unauthorized information.

- **Cyber threat environment:** the online space where malicious cyber threat activity can occur.

Types of Cyber Security Threats

Threats to cyber security can originate from internal or external sources. Examples include:

- Phishing attempts
- Disruption or denial of service (DDoS)
- Malware
- Ransomware

Cyber Security Frameworks

All Prudentially Regulated Entities should have a cyber security framework. An effective cyber security framework will be comprehensive and consider all areas of potential risk to the Prudentially Regulated Entity’s digital environment. For example, the National Institute of Standards and Technology (“NIST”) Framework, version 1.1, includes the following core functions:

- **Identify** – Develop an organizational understanding to manage cyber security risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cyber security event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cyber security event. The Detect Function enables timely discovery of cyber security events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement appropriate activities to take action regarding a detected cyber security incident. The Respond Function supports the ability to contain the impact of a potential cyber security incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cyber security incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

Self-Assessments

Prudentially Regulated Entities should use a self-assessment tool to assess their current level of preparedness, and to develop and maintain an effective cyber security framework. An entity's self-assessment should take into account all relevant areas and aspects of the entity's operations. The framework implemented by a Prudentially Regulated Entity should be appropriately tailored to the entity's business operations, risk management and level of sophistication.

It is a Prudentially Regulated Entity's responsibility to understand their business and establish their expectations of the level of protection their cyber security framework should provide. In tailoring its cyber security framework, an entity should consider its specific business threats, vulnerabilities, and risk tolerances.

The self-assessment is not intended at this time to be a component of the regular reporting requirements of the Prudentially Regulated Entity to our office. Rather, it is meant to serve as an internal assessment and reflection of the cyber security framework currently in place and to aid in identifying potential gaps.

At this time, the FCAA will not be establishing specific guidelines for measuring the level of control and management of cyber risk by a Prudentially Regulated Entity. However, the FCAA may wish to discuss the cyber security framework being utilized by the entity to ensure that cyber security is being appropriately managed.

Some examples of tools that can assist an entity in building a cyber security framework include:

- OSFI – Cyber Security Self-Assessment Guidance (link)
- Cyber security Best Practices Guide for IIROC Dealer Members (link)
- NIST Cyber Security Framework (nist.gov/cyberframework)

Additional Resources

Canadian Centre for Cyber Security – Publications

- Link: https://cyber.gc.ca/en/publications

Bulletin #0690-C – Cyber security from the Mutual Fund Dealers Association of Canada (MFDA)

- Link: https://mfda.ca/bulletin/bulletin0690-c/

Cyber security from the National Institute of Standards and Technology

- https://www.nist.gov/cyber security