Financial Services Flash

Aird & Berlis LLP
Barristers and Solicitors

February 19, 2014

Financial Firewalls: OSFI Issues Cyber Security Self-Assessment Guidance

By Brett Kenworthy and Aisha Ramakrishnan*

On October 28, 2013, the Office of the Superintendent of Financial Institutions Canada ("**OSFI**") issued a memorandum and cyber security self-assessment guidance (the "**Guidance**") for federally regulated financial institutions ("**FRFIs**"). The Guidance was published in response to the increasing frequency and sophistication of FRFI cyber-attacks.

The Guidance provides six primary categories for self-assessment by FRFIs in respect of cyber security practices, each of which are subdivided into various evaluative criteria. Each FRFI must rate its level of cyber security preparedness on a scale of 1 to 4 for each of the criteria in the six categories, with "1" representing a criterion that has not been implemented and "4" representing a criterion that has been fully implemented across its enterprise. Generally, these six categories evaluate:

1. **Organization and Resources:** whether a FRFI has implemented and funded an appropriate internal structure to address cyber security risks across its enterprise.
2. **Cyber Risk and Control Assessment:** whether a FRFI is proactive in the prevention of cyber-attacks by collaborating with its service providers to mitigate risk and engages in regular and ongoing vulnerability testing.
3. **Situational Awareness:** how a FRFI maintains its enterprise-wide knowledge base of users, devices and applications, and how a FRFI analyzes and stores its cyber security-related events.
4. **Threat and Vulnerability Risk Management:** whether a FRFI has implemented controls to prevent the loss of unauthorized data leaving the FRFI, has implemented cyber and software security tools, has protected its network and access to its network, and implemented cyber security management for third party service providers, customers and clients.
5. **Cyber Security Incident Management:** whether a FRFI possesses the ability to protect, monitor, and rapidly analyze and respond to cyber security incidents, and evaluates whether the FRFI implements an effective communications plan and incident management process.
6. **Cyber Security Governance:** whether a FRFI has an effective governance strategy and policies in place to identify and manage cyber security risks, and ensures that these policies are benchmarked against external parties.

OSFI intends that the Guidance will assist FRFIs by providing a framework for an effective self-assessment of their current preparedness in respect of cyber security. The self-assessment process will permit each FRFI to inform OSFI as to the rationale for its rating and provides an opportunity for the FRFI to create an action plan that establishes target milestones in support of achieving full implementation of its cyber security practices.

OSFI states in the Guidance that it does not currently plan to establish specific guidance for the control and management of cyber risk. Due to the manner in which the self-assessment is currently structured, it will be difficult for FRFIs to evaluate cyber security practices objectively. As such, the extent to which the Guidance will be an effective tool in developing FRFI cyber security practices will largely depend upon successful implementation and appropriate guidance and oversight from OSFI. However, this is a step in the right direction, as the Guidance provides an effective governance framework for a high level evaluation of cyber security policies.

The Financial Services Group at Aird & Berlis LLP has experience assisting federally regulated financial institutions. For more information, please contact any member of the Financial Services Group.Details can be found on our Financial Services, Insolvency and Restructuring web page, by clicking on members.

Click here to view our other newsletters
or visit **www.airdberlis.com**

**Aisha Ramakrishnan is an articling student at Aird & Berlis LLP.*