Cassels

Cyber Breaches: OSFI Demands the Details

Bernice Karn

April 10, 2019

On January 24, 2019, the Office of the Superintendent of Financial Institutions (OSFI) issued a new advisory on Technology and Cyber Security Incident Reporting (the Advisory). The purpose of the Advisory is to set out the obligations for Federally Regulated Financial Institutions (FRFIs) to report technology and cyber security incidents to OSFI. The Advisory came into effect on March 31, 2019.

Prior to the introduction of the Advisory, OSFI released the Cyber Security Assessment Guideline for FRFIs in late 2013, which allowed FRFIs to assess their level of preparedness and to assist in the implementation of useful cybersecurity practices. The completion of the Cyber Security Assessment was not made a mandatory requirement by OSFI. The Advisory is intended to complement the Cyber Security Assessment Guideline.

The Advisory is in response to OSFI's re-examination in, and approach to, enhancing cyber security at Canadian financial institutions in light of the Government of Canada's plan to create the Canadian Cyber Security Centre. In 2017-2018, OSFI conducted a cyber security cross sector review at select FRFIs to assess their responses to a severe but plausible scenario involving a cyber breach. The review focused on FRFI cyber resilience characteristics and related governance, oversight, and risk management practices. In order to enhance the monitoring of cyber threat and risk levels and trends at FRFIs and to assess systemic impacts to the Canadian financial system, OSFI implemented a cyber security strategy and action plan to identify and manage cyber security incidents as well as reduce risk of data loss and system downtime.

Cyber security has become a major issue for insurers in the US. The National Association of Insurance Commissioners (NAIC) has been working on a model cyber security law for a number of years that would cover a variety of issues. New York has already introduced its own cyber security law for insurers due to concerns over delays in finalizing the NAIC model law.

Initial Notification Requirements

Specifically, firms must notify their OSFI Lead Supervisor, no later than 72 hours after a technology or cyber security incident. FRFIs are also expected to notify OSFI's Technology Risk Division in writing. OSFI defines a technology or cyber security incident as one that has the potential to, or has been assessed to, "materially impact" the normal operations of a FRFI, "including confidentiality, integrity or availability of its systems and information."

Criteria for Reporting

OSFI provides some guidance as to what constitutes a “material” breach of a high level or critical severity to warrant a reportable incident. According to OSFI, the reportable incident may have one or more of the following characteristics:

- Significant operational impact to key/critical information systems or data;
- Material impact to FRFI operational or customer data, including confidentiality, integrity or availability of such data;
- Significant operational impact to internal users that is material to customers or business operations;
- Significant levels of system / service disruptions;
- Extended disruptions to critical business systems/operations;
- Number of external customers impacted is significant or growing;
- Negative reputational impact is imminent;
- Material impact to critical deadlines/obligations in financial market settlement or payment systems;
- Significant impact to a third party deemed material to the FRFI;
- Material consequences to other FRFIs or the Canadian financial system; and
- A FRFI incident has been reported to the Office of the Privacy Commissioner or local/foreign regulatory authorities.

Subsequent Reporting Requirements

Additionally, FRFIs must meet ongoing reporting obligations by providing regular updates as new information becomes available, as well as situational updates, including short term remediation and action plans.

The Advisory also provides a table outlining some examples of reportable incidents, but notes that the list is not to be considered exhaustive.

OSFI notes that prior to the Advisory coming into effect, FRFIs are expected to continue reporting any major incidents in accordance with previous instructions communicated by their Lead Supervisors.

Comparison with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) Requirements

In November 2018, data breach notification requirements were implemented under PIPEDA. The notification requirements require organizations subject to PIPEDA to notify the Office of the Privacy Commissioner (OPC) of any breach of security safeguards involving personal information under the organizations control where it is reasonable to believe that the breach creates a “real risk of significant harm” to an individual.

The Advisory’s reporting requirements differ in a number of ways from the PIPEDA data breach reporting notification requirements. First, the Advisory requirements are broader than the PIPEDA requirements in

that they apply regardless of whether or not the incident involves personal information. Second, the reporting threshold in the Advisory is a material breach of the normal operations of the FRFI that is of a "high or critical severity level" versus any breach that creates a "real risk of significant harm to individuals" pursuant to PIPEDA. The Advisory reporting threshold is thus somewhat broader than the PIPEDA threshold and would require reporting in the event of a breach whether or not individuals or their information were affected by the security incident. Third, the Advisory requires FRFIs to notify the OSFI Lead Supervisor within 72 hours of a breach while PIPEDA lacks any fixed notification period. Finally, the Advisory requires FRFIs to provide daily updates as new information becomes available and until all material details about the incident have been provided whereas PIPEDA is silent with respect to any ongoing reporting requirements.

In light of these differences, FRFIs should consider having designated policies and procedures in place to comply with incident reporting requirements to OSFI, and not rely solely on existing PIPEDA compliance measures.

Summary

In summary, given the existing guidance and the implementation of the new Advisory, FRFIs should:

i. regularly review internal controls and procedures to assess their level of preparedness and ensure that effective cyber-security practices are being maintained;

ii. ensure that business continuity and disaster recovery plans are updated in order to adapt to the advancements in information technology and digitalization;

iii. consider protocols followed by service providers and ensure audits of service providers are also conducted; and

iv. consider whether cyber security is an issue that should be included as a risk factor in the preparation of a FRFI's ORSA.

It is likely that OSFI will introduce revised versions of the Advisory over the next few years as cyber security continues to evolve as a major area of concern for insurance regulators.

For further information regarding this Advisory, please contact any member of the Cassels Insurance & Reinsurance Group.
