OSFI BOOTS UP CYBER SAFETY WITH ITS NEW ADVISORY ON TECHNOLOGY AND CYBER SECURITY INCIDENT REPORTING

Posted on February 6, 2019

Categories: Insights, Publications

Canada's ever-evolving cyber security climate welcomes another update with a new advisory for federally regulated financial institutions ("**FRFIs**").

On January 24, 2019, the Office of the Superintendent of Financial Institutions ("**OSFI**") published the *Technology and Cyber Security Incident Reporting Advisory* (the "**Advisory**"), which sets out OSFI's expectations for reporting technology and cyber security incidents. The Advisory is a companion piece to, and should be read in conjunction with, OSFI's *Cyber Security Self-Assessment Guidance* dated October, 2013 (the "**Cyber Guidance**"). The Advisory is applicable to all FRFIs as of March 31, 2019. In the interim, FRFIs are expected to continue reporting any major incidents according to previous instructions communicated to them.

The Advisory reflects OSFI's continued focus on technology and cyber security, as well as the federal government's larger campaign to increase awareness around protecting digital information generally.[1] In fact, the Advisory comes approximately three months after another set of reporting obligations was introduced under Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), which apply to all private sector organizations that experience a security breach involving personal information under their control.[2]

Criteria for Incident Reporting

The Advisory requires FRFIs to report certain technology or cyber security incidents to OSFI. For the purposes of the Advisory, a technology or cyber security incident is defined to "have 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". An incident should be reported to OSFI if it is assessed as having a "high or critical severity level".

Although FRFIs should define incident materiality criteria in their incident management and cyber security framework (which, ultimately, should be assessed by FRFIs pursuant to the requirements under the Cyber Guidance), the Advisory provides the following non-exhaustive list of characteristics that a reportable incident may have:

- 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 (e.g., public/media disclosure);
- material impact to critical deadlines/obligations in financial market settlement or payment systems (e.g., Financial Market Infrastructure);
- significant impact to a third party deemed material to the FRFI;
- material consequences to other FRFIs or the Canadian financial system; and/or
- the incident has been reported to the Office of the Privacy Commissioner or local/foreign regulatory authorities.

Initial Notification Requirements

If an incident meets the characteristics exemplified in, or akin to, those set out in the Advisory, the FRFI must notify OSFI as promptly as possible, but no later than 72 hours after the FRFI determines that the incident is reportable. In addition to notifying the FRFI's Lead Supervisor, the FRFI must also notify OSFI's Technology Risk Division in writing (TRD@osfi-bsif.gc.ca).

The Advisory provides details that FRFIs should include in their incident report. For example, incident descriptions should include the known impacts, whether the breach originated internally or externally, any known or suspected causes, and a mitigation strategy. FRFIs are expected to provide continuous daily updates to the Lead Supervisor while an incident is being contained, as well as submit a post-incident report which is to include lessons learned.

Enforcement

Although the Advisory is not itself law, OSFI has certain legislated enforcement powers. For example, under the *Insurance Companies Act*, OSFI has broad powers to direct insurers to cease or refrain from committing unsafe business practices, or perform acts that OSFI considers necessary to remedy the situation, as the case may be.[3] Such directions are enforceable by court order.[4] Similar provisions can also be found in the *Bank Act*.[5] From a practical perspective, FRFIs should consider the reporting requirements in the Advisory as mandatory obligations and should promptly incorporate the relevant provisions and principles into their respective incident response frameworks.

Comparison with PIPEDA requirements

On November 1, 2018, organizations subject to PIPEDA became required to notify the Privacy Commissioner of Canada and affected individuals of a "breach of security safeguards" involving personal information under the organization's control where it is reasonable to believe the breach creates a "real risk of significant harm" to such individuals.

The Advisory's reporting requirements differ in a few material respects from the breach reporting requirements under PIPEDA. For instance, the Advisory's reporting guidelines are broader than PIPEDA in that they apply regardless of whether or not the incident involves personal information. The reporting threshold in the Advisory is a "high or critical severity level", in contrast to a "real risk of significant harm" pursuant to PIPEDA. While the Advisory sets out a maximum timeline of 72 hours for reporting, PIPEDA lacks specifics, requiring notification "as soon as feasible" after discovering the breach. Finally, a reportable incident under the Advisory has the potential to, or has been assessed to, materially impact the normal operations of an FRFI, whereas there is no similar scope or size component with respect to a reportable breach under PIPEDA.

Outsourcing Arrangements

In preparation for the effective date of the Advisory, FRFIs should review their contracts with third party service providers to ensure that such parties are obligated to assist the FRFI with its compliance obligations pursuant to the Advisory. In addition, and in view of OSFI's keen interest in the outsourcing activities of FRFIs (given that, for instance, third party service providers may have less robust cyber security practices and fewer resources to deal with a breach), FRFIs should take the opportunity to consider their outsourcing risks overall[6] and whether they should contractually mandate their vendors to obtain cyber insurance or take other protective measures.

At a time when the Government of Canada is considering the potential merits and liabilities of open banking (that is, a framework where consumers and businesses can authorize third party financial service providers to access their financial transaction data, using online channels)[7] and amendments to certain acts governing FRFIs' technology-related activities are either recently in force or are pending,[8] it may not be surprising that cyber security and the protection of data are at the forefront of OSFI's mind.

by Darcy Ammerman, Grace Shaw and John Alsbergas (Articled Student)

[1] See, for example, Public Safety Canada's 2019 publication, National Cyber Security Strategy: Canada's Vision For Cyber Security and Prosperity in the Digital Age.[ps2id id='1' target=''/]
[2] The Personal Information Protection and Electronic Documents Act, SC 2000, c 5, ss 10.1, 10.2, 10.3.[ps2id id='2' target=''/]

[3] Insurance Companies Act, SC 1991, c 47, s 676.[ps2id id='3' target='/]
[4] Ibid, s 678.[ps2id id='4' target='/]
[5] Bank Act, SC 1991, c 46, ss 615, 616, 645, 646, 960, 961. [ps2id id='5' target='/]
[6] See OSFI's Outsourcing of Business Activities, Functions and Processes Guideline, dated March 2009, which may be helpful in this regard.[ps2id id='6' target='/]
[7] Department of Finance Canada, Consultation Document: A Review into the Merits of Open Banking, January 2019.[ps2id id='7' target='/]
[8] See the Budget Implementation Act, 2018, No. 1, SC 2018 c 12, which received Royal Assent on June, 21, 2018.[ps2id id='8' target='/]

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.