OSFI Provides New Guidance on Technology and Cybersecurity

March 08, 2019

Vanessa Coiteux, Stéphane Rousseau, Jérémie Ste-Marie

On January 24, 2019, Canada's Office of the Superintendent of Financial Institutions (OSFI) published the advisory Technology and Cyber Security Incident Reporting, which will be in force as of March 31, 2019. The advisory provides guidance to federally regulated financial institutions (FRFIs) with respect to the timely reporting of technology or cybersecurity incidents to OSFI.

Background

The advisory builds on the Cyber Security Self-Assessment Guidance published in 2013, in which OSFI expressed its expectations with respect to cyber risk management. The overall goal of the reporting requirement is to assist OSFI in the identification of areas where FRFIs can take steps to proactively prevent such incidents or to improve their resiliency in cases where an incident has occurred.

Technology and Cybersecurity Incidents Subject to the Reporting Requirement

The OSFI advisory concerns technology and cybersecurity incidents that affect FRFIs. Under the advisory:

- "Technology and cyber security incident" is defined as an incident having the potential to, or having been assessed to, "**materially impact the normal operations of a FRFI**, including confidentiality, integrity or availability of its systems and information"; and
- FRFIs are **required to report** to OSFI technology or cyber security incidents that they assess as being of "a high or critical severity level".

Guidance on Reportable Incidents

FRFIs are responsible for determining whether a technology or cyber security incident has a level of materiality that justifies its reporting to OSFI. Under the advisory, FRFIs are expected to assess whether an incident is of a high or critical severity level in light of the incident management framework developed pursuant to OSFI's Cyber Security Self-Assessment Guidance.

In this respect, as guidance to FRFIs, the advisory provides the following non-exhaustive list of characteristics associated with reportable incidents:

- 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
- A FRFI incident has been reported to the Office of the Privacy Commissioner or local/foreign regulatory authorities.

To further assist FRFIs in their materiality assessment, the advisory provides some examples of reportable incidents:

- Account takeover botnet campaign targeting online services using new techniques, current defences are failing to prevent customer account compromise;
- Technology failure at data centre;
- A material third party is breached and FRFI is notified that third party is investigating; and
- FRFI has received an extortion message threatening to perpetrate a cyber attack.

Reporting Requirement

A FRFI is required to notify its Lead Supervisor as promptly as possible,[1] but no later than 72 hours after determining that a technology or cyber security incident has happened and is of a high or critical severity level. The advisory sets out a list of information to be communicated in the initial report, including a description of the incident that deals with the type, origin and root cause, date and time, severity, known direct and indirect impacts, number of clients affected, current situation and mitigation actions taken or planned.

After it issues the initial report, OSFI expects the FRFI to provide regular (e.g. daily) updates as new information becomes available and until all material details about the incident have been provided. Where specific details are not yet available, the FRFIs should state that those details are not yet available. Finally, the FRFI should report to OSFI on its post-incident review and lessons learned.

Implications

Cyber security and technology incidents have wide-ranging consequences for FRFIs as they can inflict serious financial, operational and reputational harm. From a legal perspective, such incidents can also have far-reaching implications as they may trigger reporting obligations to regulators. Indeed, with the coming in force of the advisory on Technology and Cyber Security Incident Reporting, FRFIs will become subject to new reporting requirements in addition to the mandatory reporting of privacy breaches to the Privacy Commissioner of Canada, as well as the disclosure obligations under securities regulations.[2] Given that the regulatory regimes have different scope of application, FRFIs will be well-advised to reflect on cyber security and technology incidents reporting as part of their control and management of cyber risk.

[1] The report must also be sent to TRD@osfi-bsif.gc.ca.

[2] See CSA Multilateral Staff Notice 51-347 *Disclosure of cyber security risks and incidents*, January 19, 2017; CSA Staff Notice 11-326 *Cybersecurity*, September 26, 2013.