OSLER

OSFI outlines technology and cyber security incident reporting expectations

MARCH 19, 2019 4 MIN READ

Related Expertise

- Banking and Financial Services
- Commercial Technology Transactions
- Cybersecurity and Security Incident Response
- Financial Services
- Technology

Authors: Wendy Gross, Jessica Robyn Lumière

The Office of the Superintendent of Financial Institutions Canada (OSFI) recently issued the *Technology and Cyber Security Incident Reporting Advisory*, which comes into effect on March 31, 2019 (Advisory).[1]

The Advisory sets out OSFI's expectations for federally regulated financial institutions (FRFIs) with respect to the reporting of technology and cyber security incidents affecting FRFI operations. The Advisory defines a technology or cyber security incident as one that materially impacts, or could potentially materially impact, the normal operations of an FRFI, including confidentiality, integrity or availability of its systems or information (Incident). The Advisory further indicates that the FRFI must report the Incident to OSFI (by notifying its Lead Supervisor as well as TRD@osfi-bsif.gc.ca), *in writing and as promptly as possible, but no later than 72 hours, after determining an Incident meets the incident characteristics*. These are listed in the Advisory as:

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

The Advisory further advises that materiality should be defined in an FRFI's incident management framework and that an FRFI should report high or critical severity level Incidents to OSFI. A list of information to include in the initial Incident report is provided, and the Advisory also notes that OSFI should be provided with regular updates (including any short- or long-term remediation), the method and frequency of which may be changed by OSFI.

Clients should take into account the following considerations when evaluating the impact of this Advisory:

- Although the language in the Advisory would benefit from added clarity, the characteristics appear to be symptoms or examples of an event that has had or could potentially have a material impact on the normal operations of an FRFI. If the definition of an Incident is already met, then very likely one of the characteristics is also present.
- Internal policies and protocols should be reviewed to ensure alignment between FRFI incident severity level ratings and OSFI expectations, including with respect to these new reporting obligations.
- The characteristics of a reportable incident are relatively broad and vague — note for instance that the obligation to report extends as far as "significant levels of system/service disruptions"; this may be broader than what typical internal protocols or service provider language addresses, which can sometimes be limited to privacy or other security incidents.
- The FRFI should consider addressing the following in its current and future agreements with service providers: (i) the service provider's obligation to notify the FRFI of Incidents; (ii) the service provider's obligation to provide the FRFI with sufficient details to meet the initial report and subsequent situation update requirements set out in the Advisory; and (iii) the right for the FRFI to share the Incident-related information and reports with OSFI, and potentially also with any third parties retained by the FRFI to assist in managing or investigating the Incident.
- Further, while most arrangements that meet the OSFI B-10 Guideline "material outsourcing" threshold would likely be within the scope of such a review, note that the application of the Advisory is not limited to material outsourcing arrangements and includes all service provider incidents where the impact on the FRFI meets the criteria in the Advisory.

The appendix to the Advisory provides helpful examples to guide an FRFI in determining whether a technology or cyber event is reportable to OSFI pursuant to the Advisory. However, if you have any questions about whether to report such an event, do not hesitate to reach out to the Osler Technology Group.

---

[1] OSFI expects FRFIs to continue reporting any major incidents according to previous instructions communicated by their Lead Supervisors until the Advisory becomes effective on March 31, 2019, from which point forward the Advisory takes precedence over any prior instructions in respect of the reporting of technology and cyber incidents.