Cassels

OSFI Updates Cyberbreach Advisory and Self-Assessment Tool

Bernice Karn, Gordon Goodman

August 19, 2021

Over the last number of years cyber breaches have occurred with unfortunate regularity throughout the world. Statistics abound as to the frequency of cyber attacks on organizations, and of those intrusions, ransomware attacks are becoming more and more prevalent. According to a 2020 report by the Canadian Centre for Cyber Security,[1] Canada "often ranks among the top countries impacted by ransomware" and "it is almost certain that a majority of ransomware attacks against Canadian victims are unreported to authorities." The report goes on to say that, over the prior two years, ransomware attacks have impacted hundreds of Canadian businesses and critical infrastructure providers, including hospitals, police departments and various levels of government. This trend towards the deployment of ransomware on unsuspecting organizations has evolved towards attacking high value targets, and this has not gone unnoticed by the Office of the Superintendent of Financial Institutions (OSFI).

In May of 2021, in its *Near-Term Plan of Prudential Policy for Federally Regulated Financial Institutions and Federally Regulated Private Pension Plans*,[2] OSFI signaled that, as part of its strategic plan, it was looking at preparing federally regulated financial institutions (FRFIs) to improve their preparedness and resilience not only for financial risks, but against non-financial risks before these risks negatively affect their financial condition. To this end, we can expect new OSFI guidance later this year on OSFI's expectations for technology and cyber risk management by FRFIs. In the meantime, on August 13, 2021, OSFI updated its 2019 Technology and Cyber Security Incident Reporting Advisory (Advisory)[3] along with its 2013 Cyber Security Self-Assessment tool.[4] The updated Advisory lays out expanded rules about when FRFIs should report technology and cyber security incidents to OSFI.

OSFI has identified cyber security as a key risk that is increasing as FRFIs continue to rely on technology. The updated Advisory supports a coordinated and integrated response to technology and cyber security incidents at FRFIs.

The following are notable updates in the new Advisory:

- **Timing of Notification**: While the 2019 Advisory listed a number of different criteria to describe a reportable incident, it was silent on timing of the reporting obligation. Now the expectation is that reportable incidents must be reported to OSFI"s Technology Risk Division as well as the FRFI's Lead Supervisor within 24 hours, or sooner if possible. Presumably the 24 hours runs from the discovery of the event, but that is not explicit in the new Advisory. Where specific details are

unavailable at the time of the initial report, the FRFI must indicate “information not yet available” and must provide best estimates and details available at the time.

- **Expanded Notification Criteria**: The notification criteria provide more specific information around what “impact” of a cyber breach incident means in terms of the FRFI’s operations. Reportable events have been expanded to include a broader range of situations in which the incident must be reported, including the following:
    - Incidents that affect the FRFI’s financial market settlement systems, confirmations or payments systems, payment services, utility or data centre disruptions or outages and loss/degradation of connectivity;
    - Incidents where there has been an operational impact to key/critical systems, infrastructure or data and incidents that affect the confidentiality, integrity or availability of data generally, including customer information;
    - Incidents impacting a third party that affects the FRFI (note that the materiality qualifier in respect of the third party set out in the 2019 Advisory has been dropped);
    - Situations in which disaster recovery teams or plans have been activated or a disaster declaration has been made by a third party vendor that impacts the FRFI;
    - Incidents for which the FRFI's technology or cyber incident management team or protocols have been activated;
    - Incidents that have been reported to the Board of Directors or Senior/Executive Management;
    - Incidents that have been reported to various government institutions such as the Office of the Privacy Commissioner (a requirement of the prior Advisory), another federal government department (e.g., the Canadian Center for Cyber Security), other local or foreign supervisory or regulatory organizations or agencies, or any law enforcement agencies;
    - Incidents that have caused the FRFI to engage internal or external counsel;
    - An incident for which a cyber insurance claim has been initiated;
    - An incident assessed by a FRFI to be of a high or critical severity, level or ranked priority/severity/tier 1 or 2 based on the FRFI's internal assessment;
    - Technology or cyber security incidents that breach internal risk appetite or thresholds.

An incident may be considered reportable if it possesses at least one of the updated characteristics listed in the new Advisory. When in doubt, the FRFI is encouraged to report the incident, and the new Advisory supplies a template form of report specifically for this purpose.

- **A New “Failure to Report” Section**: If an FRFI does not report a cyber incident, it could be subject to increased supervisory oversight by OSFI, including but not limited to enhanced monitoring activities, watch-listing or staged intervention by OSFI in the FRFI’s operations.

Cyber security and technology incidents can have extensive adverse consequences for FRFIs, inflicting serious financial and reputational harm. To help FRFIs measure and possibly improve their current state of

readiness against emerging and growing cyber threats, as mentioned above OSFI has issued an updated Cyber Security Self-Assessment concurrently with the new Advisory. This tool examines a FRFI's current level of cyber preparedness and assists the FRFI in developing and maintaining effective cyber security practices.

With the updated Advisory, FRFIs will be subject to cyber breach reporting requirements that arguably are more onerous than the reporting obligations for privacy breaches under the *Personal Information Protection and Electronic Documents Act,* which is only to report those breaches where there is a "real risk of significant harm" to an individual. In light of these changes, prudent FRFIs must have designated policies and procedures in place to deal with these incidents as and when they occur and to comply with the updated reporting requirements of OSFI.

---

[1] Online: https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-modern-ransomware-and-its-evolution.

[2] Online: https://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/prupol-let.aspx.

[3] Online: https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx.

[4] Online: https://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/cbrsk.aspx.
