Bulletin | Cybersecurity, Privacy and Data Protection

August 2021

OSFI updates Technology and Cyber Security Incident Reporting Advisory

On August 13, 2021, the Office of the Superintendent of Financial Institutions ("OSFI") released an updated *Technology and Cyber Security Incident Reporting Advisory* (the "Advisory") that imposes enhanced requirements for federally regulated financial institutions ("FRFIs") regarding the prompt (within 24 hours or sooner if possible) reporting of technology and cybersecurity incidents to OSFI. The Advisory is effective immediately and will likely require many FRFIs to update their incident response practices/procedures and agreements with IT service providers and other third parties.

OSFI and cybersecurity

OSFI is an independent agency of the Government of Canada that regulates and supervises FRFIs, including banks, federally incorporated or registered trust and loan companies, insurance companies, and pension plans subject to federal oversight.

For many years, OSFI has emphasized the importance of cybersecurity and issued guidance to help FRFIs implement appropriate policies and practices to manage cyber risks and effectively respond to cyber incidents. OSFI's 2013 *Cyber Security Self-Assessment* provided FRFI's with guidance for the self-assessment of their cybersecurity maturity. OSFI's 2019 *Advisory on Technology and Cyber Security Incident Reporting* (the "2019 Advisory") set out OSFI's expectations for FRFIs' reporting of technology and cybersecurity incidents. See BLG bulletins *Regulatory Guidance for Cyber Risk Self-Assessment* and *OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting*.

On August 13, 2021, OSFI announced the release of the Advisory and an updated Cyber Security Self-Assessment.

The Advisory

The Advisory replaces OSFI's 2019 Advisory and sets out enhanced requirements for FRFIs' reporting of technology and cybersecurity incidents to OSFI. The stated purpose of the Advisory is to support "a coordinated and integrated approach to OSFI's awareness of, and response to, technology and cyber security incidents" at FRFIs. The Advisory explains that timely reporting of technology and cybersecurity incidents "can help identify areas where FRFIs or the industry at large can take steps to proactively prevent ... incidents or improve their resiliency after an incident has occurred".

Key definition – Technology or cyber security incident

The Advisory broadly defines "technology or cyber security incident" as "an incident that has an impact, or the potential to have an impact, on the operations of a FRFI, including its confidentiality, integrity or the availability of its systems and information". The definition is significantly broader than the corresponding definition in the 2019 Advisory, which was limited to incidents assessed to "materially impact the normal operations of a FRFI".

Criteria for reporting

The Advisory does not specify any minimum severity level threshold for the reporting of incidents to OSFI. Unlike the 2019 Advisory, which limited reporting to incidents "assessed by a FRFI to be of a high or critical severity level", the Advisory appears to require the reporting of any incident that has had, or might have, an impact on a FRFI's operations or the confidentiality, integrity or availability of a FRFI's systems or information.

The Advisory provides a revised and expanded list of characteristics of a reportable incident that, if interpreted literally, includes incidents that are relatively minor and limited in both scope and consequences. The Advisory encourages FRFIs to report incidents that do not align with or contain the listed criteria. The Advisory also provides updated examples of reportable incidents.

Reporting – Timing and details

The Advisory requires FRFIs to submit an initial written incident report to OSFI "within 24 hours, or sooner if possible", instead of the 72 hours permitted under the 2019 Advisory. The 24-hour period is the shortest reporting period currently imposed by any Canadian financial industry regulator, and is tighter than reporting requirements under Canadian private sector personal information protection laws.

The initial report to OSFI must be provided using a prescribed form, which requires detailed information about the nature and scope of the incident and the FRFI's incident response activities, including: (1) the incident severity level or priority; (2) the business lines, technologies and locations affected; (3) the current state of the incident and response activities completed; (4) the root causes of the incident; (5) details of internal and external notifications (e.g., notifications and reports to insurers and law enforcement authorities) by the FRFI; and (6) whether the FRFI has engaged external forensics firms, a breach coach or legal counsel (internal or external).

The Advisory explains that OSFI expects FRFIs to provide regular updates (e.g., daily) as new information becomes available and until all details about the incident have been provided to OSFI and the incident has been contained/resolved.

Failure to report

The Advisory warns that a FRFI's failure to report an incident as required by the Advisory "may result in increased supervisory oversight including ... enhanced monitoring activities, watch-listing or staging of the FRFI".

FRFI policies/procedures

The Advisory explains that a FRFI's policies and procedures for dealing with technology and cybersecurity incidents should reflect OSFI's incident reporting requirements.

Comment – Preparing for compliance

FRFIs should assess and update their systems, policies and procedures so they are able to promptly submit incident reports in compliance with the updated Advisory. Following are some suggestions:

- **Policies/procedures – Incident assessment and response:** A FRFI should have written policies and procedures so that each potential technology and cybersecurity incident is assigned to designated and trained personnel for investigation, assessment and response in accordance with a written incident response plan that is consistent with applicable legal requirements, regulatory guidance and relevant best practices. See BLG bulletins *Cyber Incident Response Plans – Test, Train and Exercise* and *Data Security Incident Response Plans – Some Practical Suggestions*.
- **Policies/procedures – Reporting to OSFI:** A FRFI should have written policies and procedures so that designated and trained personnel make and document informed decisions about reporting technology and cybersecurity incidents to OSFI in accordance with the Advisory.

- **Contracts with third parties:** A FRFI should ensure that its contracts with third parties (e.g., cloud service providers and other outsourced service providers) contain appropriate provisions (e.g., obligations to promptly notify the FRFI of all technology and cybersecurity incidents and provide information about each incident) so that the FRFI is able to comply with reporting obligations under the Advisory.
- **Legal privilege:** A FRFI should have an appropriate legal privilege strategy to help avoid inadvertent and unnecessary disclosures of privileged legal advice regarding cybersecurity incidents and inadvertent waivers of legal privilege. See BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*, *Cyber Risk Management – Legal Privilege Strategy (Part 2)*, *Legal Privilege for Data Security Incident Investigation Reports* and *Loss of Legal Privilege over Cyberattack Investigation Report*.
- **Other reporting, notification and disclosure obligations:** A FRFI should be mindful of its other legal obligations to report, notify and disclose technology and cybersecurity incidents imposed by statute (e.g., personal information protection laws and securities laws), contract and common/civil law. See BLG bulletins *Cyber-Risk Management – Data Incident Notification Obligations*, *Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*, *Frequently Asked Questions – Compliance with PIPEDA's Security Breach Obligations*, and *IIROC Imposes Mandatory Reporting of Cybersecurity Incidents for Regulated Investment Firms*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.