FINANCIAL INSTITUTIONS: OSFI'S HEIGHTENED CYBER SECURITY INCIDENT REPORTING OBLIGATIONS NOW IN EFFECT

Posted on April 8, 2019

Categories: Insights, Publications

On January 24, 2019, the Office of the Superintendent of Financial Institutions ("**OSFI**") published the *Technology and Cyber Security Incident Reporting Advisory*[1] (the "**Advisory**"), which sets out OSFI's expectations for reporting technology and cyber security incidents. The Advisory became effective for all federally regulated financial institutions ("**FRFIs**") on March 31, 2019.

The Advisory requires FRFIs to report technology or cyber security incidents that "have the potential to, or have been assessed to, materially impact the normal operations of a FRFI, including confidentiality, integrity or availability of its systems and information". If a FRFI assesses an incident as being of a "high or critical severity level", the FRFI must notify OSFI as promptly as possible, but no later than 72 hours after the FRFI determines that the incident is reportable. For more details on the reporting process, and how it differs from the breach reporting requirements under *Canada's Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), see our recent publication, "OSFI Boots Up Cyber Safety with its New Advisory on Technology and Cyber Security Incident Reporting".

In order to ensure compliance with the Advisory and OSFI's expectations, we recommend several steps including:

- taking a top-down approach to ensure active participation and buy-in to cybersecurity from the executive and board down through employees;
- conducting periodic risk assessments, security audits, and due diligence on vendor and outsourced workers when contracting with them (as well as including written requirements in the contracts);
- designating a program administrator who is accountable to the organization; and
- developing written policies and procedures, including, critically, an incident response plan, based on the above.

Regularly testing internal controls, conducting staff training programs and updating compliance procedures will increase the effectiveness of these recommendations.

Organizations should consult McMillan's Crisis Response Services for additional guidance, and reach out to a

member of our team with any further questions.

by Darcy Ammerman, Ryan J. Black, Grace Shaw and Alex Tyzuk (Articled Student)

[1] Available at Technology and Cyber Security Incident Reporting[ps2id id='1' 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.