SAFEGUARDING DATA TRANSFERS OF FEDERALLY REGULATED ENTITIES: WITHIN CANADA AND BEYOND

Posted on April 26, 2016

Categories: Insights, Publications

In light of the recent high profile Bangladesh Central Bank theft,[1] it is clear that financial institutions are not immune from cyber security incidents, especially as institutions become more globally interconnected. In an effort to protect data, it is important to focus on prevention of data breaches, but it is also critical that banks and other entities be able to quickly detect any breaches and respond rapidly in order to prevent further loss or damage.

***Personal Information Protection and Electronic Documents Act* ("PIPEDA")**

PIPEDA applies to federally regulated organizations carrying on commercial activity in Canada, including banks, and to many private-sector organizations engaged in commercial activity, including those that collect, use or disclose personal information crossing provincial or national borders. It requires organizations to implement measures to safeguard personal information against loss and theft, and from unauthorized access, disclosure, copying, use, modification or destruction.

Pursuant to PIPEDA, banks and other organizations are responsible for personal information in their possession or control, including information transferred to another party, whether that party is within Canada or outside of Canada's borders.[2] In all cases, transferred data can only be used for the purposes for which it was originally collected (otherwise additional consent may be required).

Under PIPEDA, a third party receiver of data must also provide comparable levels of protection. Banks and other organizations transferring data to third parties should use contractual arrangements and/or other means, such as audits or due diligence of the party's policies, training and security measures, to protect against the unauthorized use or disclosure of data once in the hands of another party.

The federal *Digital Privacy Act* amends PIPEDA. When the relevant sections come into force, banks and other organizations will be required to keep records of every breach of security affecting personal information under their control. Moreover, these entities will also be required to notify both the Privacy Commissioner and affected individuals of any breach reasonably believed to create a real risk of significant harm.

The Role of the Office of the Superintendent of Financial Institutions ("OSFI")

OSFI was established to contribute to the safety and soundness of the Canadian financial system. OSFI has identified cyber security as an aspect of operational risk for banks and other federally regulated entities ("**FREs**").

OSFI's *Cyber Security Self-Assessment Guidance*[3] confirms its expectation that Senior Management review cyber risk management policies and practices to ensure that they remain appropriate and effective in light of changing circumstances and risks. The self-assessment guidance contains a ratings system in six key areas: organization and resources, cyber risk and control assessment, situational awareness, threat and vulnerability risk management, cyber security incident management and cyber security governance.

Additional data and technology risks are governed under OSFI's operational risk management framework more generally (i.e., the risk of loss resulting from people, inadequate or failed internal processes and systems or from external events).[4]

OSFI's Guideline entitled *Outsourcing of Business Activities, Functions and Processes*[5] specifies that FREs retain ultimate accountability for any activities that they choose to outsource to a service provider. FREs are expected to evaluate, monitor and manage the risks of outsourcing arrangements. When outsourcing to a foreign jurisdiction, a FRE's risk management program should be enhanced to address any additional concerns arising from the economic and political environment, the level of technological sophistication and the legal and regulatory risk profile of the foreign jurisdiction.

Insurance Institute of Canada Report

The Insurance Institute of Canada is the premier source of professional education and career development for Canada's property and casualty insurance industry. It has published a research report with respect to cyber security wherein it names cyber security as a "major issue for the insurance industry and society."[6] As attacks become more common and business becomes more interconnected, the report identifies a shift in focus from seeking to entirely eliminate the risk of cyber attacks to minimizing the risk of loss from such incidents.

The report highlights that there is no "one size fits all" approach to security safeguards. That being said, by drawing on several other sources,[7] the report makes certain baseline suggestions that should be adopted by insurance companies (and potentially by other types of organizations). Suggestions include putting a senior executive in charge of security safeguards, setting up a governance framework, prioritizing and protecting critical data, regularly evaluating and addressing vulnerabilities and threats, conducting regular risk assessments, developing an incident management system, requiring strong passwords and regularly changing these passwords, properly training and screening personnel and using application whitelisting to prevent

malicious software and unapproved programs from running.

Recommendations

In general, banks, insurance companies and other organizations should have policies governing outsourcing and should always consider issues of cyber security when selecting third party partners. It is prudent to require assessment and verification of third parties' cyber security infrastructure and to include adequate representations, warranties and covenants in any contract with such third parties. It may also be advisable to inquire about and review the adequacy of a third party's cyber insurance policy and to obtain separate stand-alone cyber security insurance.

Of course, with respect to cross-border data transfers, banks, insurance companies and other organizations must also be aware of and adhere to international standards such as those found in the European Union's Data Protection Directive (DPD),[8] the Trans-Pacific Partnership Agreement (TPP)[9] and the General Data Protection Regulation (once in force).[10]

by Darcy Ammerman and Jasmine Khan, Student-at-Law

1 See, for instance, this article from the *Wall Street Journal*: http://www.wsj.com/articles/hackers-in-bangladesh-bank-account-heist-part-of-larger-breach-1458582678.

2 Note that PIPEDA does not distinguish between domestic and international data transfers.

3 Available at: http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx.

4 See OSFI's draft guideline entitled *Operational Risk Management* available at: http://www.osfi-bsif.gc.ca/Eng/Docs/e21.pdf.

5 Available at: http://www.osfi-bsif.gc.ca/eng/fi-if/rg-ro/gdn-ort/gl-ld/pages/b1 0.aspx.

6 Cyber Risks Research Report: Implications for the Insurance Industry in Canada, available online: http://www.insuranceinstitute.ca/en/resources/insights-research/cyber-risks.aspx.

7 See: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-deloitte-cyber-risk-pov-secure-vigilant-resilient.pdf and http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-eng.aspx.

8 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

9 http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/tpp-

ptp/index.aspx?lang=eng.

10 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011.

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.