CYBERSECURITY – THE LEGAL LANDSCAPE IN CANADA

Posted on October 25, 2017

Categories: Insights, Publications

In Canada, data protection and cybersecurity are governed by a complex legal and regulatory framework. Failure to understand this framework and take active steps to reduce risks (or the impact of such risks when they materialize) can have serious legal and financial consequences for an organization. Therefore, it is crucial for organizations that operate in Canada (in whole or in part), or that have business partners operating in Canada, to understand this rapidly evolving area of law and governance.

The following paper provides a brief overview of the evolving Canadian landscape governing data protection and cybersecurity. The purpose of this overview is to provide an introduction to the sources of law and governance that would impact organizational decision-making with respect to the development of a plan to address cybersecurity risks. Specifically, this paper introduces the statutory framework of Canadian privacy and data protection laws relevant to cybersecurity, the regulatory and governance framework for certain regulated organizations and institutions, and the current state of the common law. Following a brief review of the legal landscape, we provide recommendations on how to minimize the risk of cyber threats.

Statutory Framework

In the private sector, there are a number of statutes that require organizations to protect personal information within their possession or control. Of particular importance is the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[1], which is the Federal legislation that applies to protection of employee personal information by federally-regulated organizations (such as banks and telecommunications companies), as well as protection of personal information in the course of commercial activities in all jurisdictions that do not have substantially similar legislation.

Currently only Alberta[2], British Columbia[3] and Quebec[4] have substantially similar legislation. Such provincial legislation is applicable in place of PIPEDA within the relevant province, and contains implicit or explicit accountability and security obligations similar to the PIPEDA obligations outlined below (although only the Alberta legislation contains breach reporting requirements)[5].

PIPEDA contains a number of provisions applicable to data protection and cybersecurity, including:

Organizations are responsible for personal information under their control and must designate an

individual or individuals who are accountable for compliance with the principles set out in Schedule 1 of PIPEDA[6].

Personal information must be protected by security safeguards appropriate to the sensitivity of the information[7].

Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, regardless of the format in which it is held[8].

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection[9].

The methods of protection should include *(a) physical measures* – e.g., locked filing cabinets and restricted access to offices; *(b) organizational measures* – e.g., security clearances and limiting access on a "need-to-know" basis; and *(c) technological measures* – e.g., the use of passwords and encryption[10].

In June 2015, PIPEDA was amended to require that organizations notify the Office of the Privacy Commissioner of Canada (the "OPC"), affected individuals, and organizations or government institutions that may be able to reduce or mitigate the risk of harm, if it is reasonable to believe that a breach of the security safeguards protecting personal information[11] poses a "real risk of significant harm"[12] to the affected individuals. Also, organizations will be required to keep a record of all breaches. Knowingly failing to report or record a breach will be an offence punishable by fines of up to C$100,000. These new provisions have not yet come into force, but will become mandatory once the associated regulations have been enacted. As draft regulations were released in September 2017, and the consultation period is now closed, it is expected that the PIPEDA breach reporting obligations may come into force in the near future.

Other relevant statutory requirements/restrictions include:

1.Almost every jurisdiction throughout Canada has specific legislation governing protection of personal health information that is collected[13], used or disclosed by health information custodians, as well as protection of personal information held by government bodies/institutions[14].

2.Certain provinces have also created statutory torts, pursuant to which individuals can bring a claim for breach of their privacy (without proof of damages)[15].

3.Canada's Criminal Code[16] sets out the following offences:

- using a device willfully to intercept a private communication without the express or implied consent of the originators or intended recipient[17]; and

- intercepting fraudulently and without colour of right any function of a computer system[18].

4.*Canada's Anti-Spam Law* ("CASL")[19] contains provisions governing software installation in the course of commercial activities, including provisions aimed at viruses and spyware, such as prohibitions against:

- installation of computer programs on another person's computer system[20] without the express consent of the owner or an authorized user of that system;
- causing a computer program to be installed without consent; and
- having installed a computer program, causing that program to communicate with other electronic devices without the consent of the owner or authorized user.

These prohibitions apply if the installer (or the party directing the installer) is located in Canada, or if the target computer system is located in Canada.

Finally, there are some sector-specific statutes that include provisions relevant to protection of personal information, such as provisions in the *Bank Act*[21] that regulate use and disclosure of personal financial information by federally regulated financial institutions.

Regulatory and Governance Framework

The Office of the Superintendent of Financial Institutions ("OSFI") and the Canadian Securities Administrators ("CSA") each provide guidance to address the cybersecurity risks for organizations subject to their regulation.

1. OSFI Guidance

OSFI regulates Federally Regulated Financial Institutions ("FRFIs"), including banks, most insurance companies and federal pension plans. OSFI does not currently have in place regulations requiring specific actions by FRFIs with respect to cybersecurity. However, Guideline B-10: Outsourcing of Business Activities, Functions and Processes sets out OSFI's expectations with respect to technology-based outsourcing and informs of OSFI's expectations with respect to cybersecurity risk management[22].

In 2013, OSFI released the Cybersecurity Self-Assessment Guidance for FRFIs to assess their level of preparedness and to assist in the implementation of useful cybersecurity practices[23]. The template focuses on six categories for assessment: organization and resources; cyber risk and control assessment; situational awareness; threat and vulnerability risk management; cybersecurity incident management; and cybersecurity governance. In releasing the self-assessment guidance, OSFI identified that it "expects FRFI Senior Management to review cyber risk management policies and practices to ensure that they remain appropriate and effective in light of changing circumstances and risks".

In addition, OSFI released Draft Guideline E-21: Operational Risk Management in August of 2015, which

proposes that FRFIs develop a framework for operational risk management based on the following four principles[24]:

1. Operational risk management should be fully integrated within the FRFIs overall risk management program and appropriately documented;
2. Operational risk management serves to support the overall corporate governance structure of the FRFI;
3. FRFIs should ensure effective accountability for operational risk management, by using, for instance, a 'three lines of defence' approach to separate the key practices of operational risk management and provide adequate independent overview and challenge; and
4. FRFIs should ensure comprehensive identification and assessment of operational risk through the use of appropriate management tools.

2. CSA Guidance

The CSA is an umbrella organization of Canada's provincial and territorial securities regulators whose objective is to improve, coordinate and harmonize regulation of the Canadian capital markets. The CSA has recently identified cybersecurity as a major concern to the Canadian capital markets. On September 26, 2013, the CSA released CSA Staff Notice 11-326 titled "Cyber Security"[25]. The CSA emphasized the need for issuers, registrants and regulated entities to be aware of the challenges of cyber crime and take appropriate measures to safeguard themselves and their clients or stakeholders. In particular, the denial of service attacks and advanced persistent threats were identified as two major types of cyber threats that were increasing in frequency and sophistication.

In particular, in Staff Notice 11-326, the CSA suggested that:

- Issuers, registrants and regulated entities who had not yet considered the risks of cyber crime, give consideration to how best address the risks. Suggested steps included:
    - educating staff with respect to the importance of, and their role in, information and computer security;
    - following guidance and best practices from industry associations and recognized security organizations; and
    - conducting regular third party vulnerability and security tests and assessments.
- Issuers, registrants and regulated entities who had already taken steps to address the issue, should review their cybersecurity risk control measures on a regular basis.
- Issuers should consider whether cyber crime risks, incidents, and related controls constitute matters that need to be disclosed in a prospectus or continuous disclosure filing.
- Registrants should consider whether risk management systems provide for management of cyber crime

risks in accordance with prudent business practices.
- Regulated entities should consider the measures necessary to manage the risks of cyber crime.

Staff Notice 11-326 cautioned that the CSA "will consider these issues in its reviews of issuer disclosure and in its oversight of registrants and regulated entities".

In September 2016, the CSA updated their 2013 notice by way of Staff Notice 11-332. This notice reminds market participants that once they determine that cyber risk is a material risk, they should provide detailed and entity-specific risk disclosure and avoid general, boilerplate disclosure. They advised that cyber attack remediation plans should address how the issuer would assess the materiality of a cyber attack to determine what needs to be disclosed pursuant to applicable securities laws, as well as when and how to make such disclosure. They further reminded registrants to remain vigilant in developing, implementing, and updating their approach to cyber security “hygiene and management” and urged registrants to review and follow guidance issued by self-regulatory organizations.

3. Other Regulators

Various other regulators have also released guidance documents. For example:

- The Investment Industry Regulatory Organization released a Cybersecurity Best Practices Guide and a Cyber Incident Management Planning Guide in December 2015;
- The Mutual Fund Dealers Association of Canada released a Bulletin on Cybersecurity in May 2016; and
- The OPC has published a Security Self-Assessment Tool.

The Common Law (Case Law)

In addition to the statutory and regulatory frameworks described above, there is an evolving body of case law in Canada that is developing in response to individual and class action claims related to privacy and data protection breaches.

For example, in January 2012, the Ontario Court of Appeal recognized a new tort of "intrusion upon seclusion", whereby:

> *One who intentionally [or recklessly] intrudes, physically or otherwise, upon the seclusion of another or his [or her] private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.*[26]

According to the Court, a central rationale for the recognition of this new cause of action was the unprecedented power of organizations to capture and store vast amounts of personal information using modern technology. Highly sensitive personal information can now be accessed and collated with relative ease,

including financial and health information as well as data related to individuals' whereabouts, communications, shopping habits and more. The Court found that the common law must evolve in response to the modern technological environment[27].

In February 2016, the Ontario Court of Appeal recognized yet another privacy-related tort in Jane Doe 464533 v ND[28], whereby:

> *One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.*

In recognizing this tort, the Court acknowledged that the current state of technology enables predators and bullies to victimize individuals on a much larger scale than in the past, and that society is scrambling to catch up to the problem and the law is only beginning to respond.

Given the concerns expressed by the Courts in these two relatively recent cases, there is a real possibility that additional torts may be recognized by Canadian courts going-forward, to respond to particular fact patterns involving privacy breaches.

Lawsuits involving data breaches also include more traditional allegations, such as claims of negligence, breach of contract and statutory breach (e.g., breach of consumer protection legislation).

Although individual lawsuits related to data protection and cybersecurity are possible in Canada, the bigger concern for most organizations is the rise in class action lawsuits. In Canada, these lawsuits tend to fall under three broad categories: (1) employee errors; (2) employee "snooping" and other misconduct; and (3) data breaches. Examples of each are set out below.

1. *Employee Errors*

Some examples of class action lawsuits that involved mistakes by one or more employees of an organization include:

- Class action lawsuits filed in several provinces following the loss of an unencrypted external hard drive containing sensitive personal information of approximately 583,000 individuals who participated in the Canada Student Loans Program, by an employee of Human Resources and Skills Development Canada[29]; and
- Class action lawsuits filed in Ontario and British Columbia after a mailing was sent to approximately 40,000 individuals, which identified them as participants in a federal program for access to medical marihuana[30].

Although none of these class actions have yet been decided on their merits, it is clear that plaintiffs are seeking to hold organizations accountable for mistakes made by employees.

2. Employee "Snooping" and other Misconduct

In addition to cases involving mistaken loss or disclosure of personal information, Canada has seen a number of class actions following intentional unauthorized access to or disclosure of personal information by employees. For example:

- In Newfoundland and Labrador, a class action lawsuit was filed against the Health Authority after an employee allegedly accessed approximately 1,043 medical records without authorization[31];
- In Ontario, a class action has been filed alleging that employees of the Peterborough Regional Health Centre accessed patients' personal health information and distributed it to third parties without their consent[32]; and
- In Ontario, a class action was filed after a mortgage officer gave customers' confidential information to his girlfriend who then distributed it to persons who used it to commit identity theft and fraud[33].

The above is just a sampling of the class actions that have been filed following employee "snooping" or other misconduct. The extent to which courts will hold organizations vicariously liable for this type of employee misconduct is still unsettled law in Canada.

3. Data Breaches

- Class action lawsuits have also been filed following a number of data breaches caused by malicious external parties, including:
- Class actions filed in 2014, in Quebec and Ontario, following data breaches affecting Target and Home Depot[34];
- Class action filed against Ashley Madison's parent companies, Avid Dating and Avid Life, following a high profile breach of the sensitive information collected by the dating site in August 2015;
- Class action filed against Casino Rama and others, following a breach of the casino's employee, customer and vendor data in November 2016; and
- Class action lawsuit filed against Equifax following the highly publicized breach of consumers' personal information in September 2017.

Although none of these cases have yet been decided by a court, the plaintiffs' have alleged causes of action such as breach of contract, breach of consumer protection legislation, negligence, intrusion upon seclusion, breach of privacy, and publicity given to private life. Some of the cases involve massive damage claims (e.g., $760 million in the Ashley Madison case and $550 million in the Equifax case).

Reducing Legal Risk

Liability for insufficient or ineffective cybersecurity practices can arise in a number of ways. Breaches of the various statutes discussed above may result in complaints filed by groups or individuals, as well as audits or investigations initiated by the relevant privacy commissioner or other regulatory body. Penalties under the various statutes vary, but can include substantial fines in some cases, as well as prosecution of individual offenders. In addition, the regulators can disclose the identity of organizations that are prosecuted or investigated, which can result in harm to the organization's reputation. Civil disputes respecting cybersecurity issues may result in lengthy and expensive class action litigation, potentially large damage awards or settlement costs, and significant reputational harm.

Therefore, organizations should conduct an audit of their existing cybersecurity status, including an evaluation of: (i) who and what is connected to their systems and networks; (ii) what is running on their systems and networks; and (iii) whether they have technology in place to prevent most breaches, rapidly detect breaches that do occur, and minimize the damage of such breaches (e.g., automatic shutdown when data leaks are detected).

Organizations should also take into account the advice of cybersecurity experts. For example, the Australian Government's Department of Defence (along with other cyber experts)[35] has suggested the following four mitigation strategies, which have been found to significantly reduce the risk of a cyber intrusion[36]:

1. Application whitelisting
2. Timely patching of applications
3. Timely patching of operating system
4. Minimize administrative privileges

Still, despite an organization's best efforts, it is not possible to entirely eliminate the risk of a successful cyber attack. Therefore, organizations may wish to consider insurance options to mitigate the risk of financial loss as a result of cyber attacks.

Conclusion

With cyber attacks regularly featured in headline news, and class action lawsuits proliferating at an alarming speed, all organizations would be well advised to consider the state of their "cyber hygiene" and takes steps to remedy any deficiencies.

Cybersecurity is an area that requires a multi-disciplinary approach, with input from a variety of experts. Therefore, a cyber audit will necessarily involve an evaluation of an organization's information technology systems, but must also include consideration of applicable legal and regulatory requirements as well as options

to reduce or mitigate risks (including insurance options). Although this will require an initial investment of time and resources, organizations that fail to actively address cyber risk may be exposed to serious reputational, financial and legal repercussions if and when a data breach occurs.

[1] *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5.
[2] *Personal Information Protection Act,* SA 2003, c P-6.5.
[3] *Personal Information Protection Act*, SBC 2003, c 63.
[4] *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c. P-39.1.
[5] Manitoba has also passed *The Personal Information Protection and Identity Theft Prevention Act,* SM2013, C.17, but as at the date of writing this legislation was not yet in force.
[6] PIPEDA Schedule 1, Article 4.1.
[7] PIPEDA Schedule 1, Article 4.7.
[8] PIPEDA Schedule 1, Article 4.7.1.
[9] PIPEDA Schedule 1, Article 4.7.2.
[10] PIPEDA Schedule 1, Article 4.7.3.
[11] "Breach of security safeguards" means "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from failure to establish those safeguards. PIPEDA, s.2(1).
[12] Defined to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. PIPEDA, s.10.1(7).
[13] Every jurisdiction other than Prince Edward Island.
[14] The Federal public sector legislation is the *Privacy Act*, RSC 1985, c P-21.
[15] i.e., British Columbia, Manitoba, Newfoundland and Saskatchewan.
[16] An Act respecting the Criminal Law, R.S.C., 1985, c. C-46 (the "Criminal Code").
[17] Criminal Code, at s.184.
[18] Ibid, at s.342.1.
[19] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio- television and Telecommunications Commission Act*, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act. S.C. 2010, c. 23.
[20] Broadly defined, and would include smartphones, tablets, desktops and laptops, wearable techn*ology, and smart cars and appliances.*

[21] Bank Act, SC 1991, c 46 ("Bank Act").
[22] See *http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/cldcmp.aspx*.
[23] See *http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx*.
[24] See *http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e21.aspx*.
[25] See *https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20130926_11-326_cyber-security.htm*.
[26] *Jones v. Tsige*, 2012 ONCA 32.
[27] Ibid.
[28] 2016 ONSC 541.
[29] See for example *Condon v. Canada*, 2015 FCA 159.
[30] See for example *John Doe and Suzie Jones v. Her Majesty the Queen*., which includes the novel tort "publicity given to private life".
[31] *Hynes v. Western Regional Integrated Health Authority,* 2014 CanLII 67125.
[32] *Hopkins v. Kay,* 2014 ONSC 321.
[33] Evans v. The Bank of Nova Scotia, 2014 ONSC 2135.
[34] See, for example, *Zuckerman c. Target Corporation*, 2015 QCCS 1285 and *Lozanski v. The Home Depot Inc.*, CV-14- 51262400CP (Ont. Sup. Ct.).
[35] These four mitigation strategies have also been emphasized by the Council on Cyber Security, in its paper "The Critical Security Controls for Effective Cyber Defense", as being amongst the "First Five Quick Wins" that will have the most immediate impact on preventing cyber attacks. See: *http://www.councilоncybersecurity.org/critical- controls/reports/*. The fifth "quick win" emphasized by the Council on Cyber Security is "use of standard, secure system configurations".
[36] See *http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm* for more information on these mitigation strategies. These four mitigation strategies have also been emphasized by the Council on Cyber Security, in its paper "The Critical Security Controls for Effective Cyber Defense", as being amongst the "First Five Quick Wins" that will have the most immediate impact on preventing cyber attacks. See: *http://www.councilоncybersecurity.org/critical- controls/reports/*. The fifth "quick win" emphasized by the Council on Cyber Security is "use of standard, secure system configurations".

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.