Spring 5-20-2019

ARE CANADIAN CYBER SECURITY RELATED LAWS SUFFICIENT TO DEAL WITH THE REALITY OF TODAY'S THREATS

Peter Hanycz
La Salle University, hanyczp1@student.lasalle.edu

ARE CANADIAN CYBER SECURITY RELATED LAWS SUFFICIENT TO DEAL WITH THE REALITY OF TODAY'S THREATS

by Peter Hanycz

A capstone submitted in fulfillment of the requirements
for the degree of Master of Science in Cybersecurity

La Salle University

Philadelphia, Pennsylvania

May 2019

Advisor: Steve Hilkowitz

Abstract

Cyber security is one of the growing concerns across the 21st Century world. For the private sector, proper cyber security allows organizations to protect themselves against the increasing threat of cyber-attacks. These businesses play a critical role by implementing robust security infrastructures that ensure, to the extent possible, the protection of personal and corporate data. At the same time, governments have a major role to play in influencing the decisions that organizations make, especially as it relates to customer data. The current privacy and cybersecurity landscape in Canada has developed over time as a way to hold organizations accountable in protecting the customer information that they collect in the course of their business.

This analysis considers the research question of whether or not the existing legislative/regulatory framework in Canada is sufficient to deal with the cyber threats being faced by individual corporations. There is both a shared interest and, arguably, responsibility in addressing the risks associated with cyber threats among the government, private sector, and individuals. However, sharing a common interest against a shared threat, while important, does not necessarily override the expectations that businesses and citizens have respecting unfettered access to the Internet. As a result, for the government, the dilemma becomes one of balance; balance between achieving the appropriate level of regulation in order to protect users of the internet and their overall individual liberty to operate in the cyber world.

Acknowledgements

This project would not have been possible without the support of many!

I cannot express my gratitude adequately to the many professors who I have worked with at La Salle University, including my Faculty Advisor, Dr. Hilkowitz. Their wisdom and commitment to my success supported this work at many stages along the way. I am especially grateful to Professor Margaret McCoey, Program Director, for her ongoing support and encouragement during these last two years. Thank you Peggy!

I remain grateful, also, to my peers in the program. As we travelled this journey together, I learned a great deal from their insights and experience, and benefited from their collegial encouragement and interactions.

Of course, nobody has been more important to me in the completion of this project than my family. Most importantly, I wish to thank my beautiful wife, Colleen, for always offering her love and support, and also for her gentle guidance along the way. I wish to thank each of my three wonderful children, Erik, Emily and Claire. Emily strongly encouraged me to undertake this program at the outset and since her sudden death, she has continued to encourage me in a very different way. I am grateful to all of you!

I would also like to acknowledge all readers of this work. And finally, for all those bereaved parents who are struggling to find a way through their grief, I offer this project to you as proof that there are, indeed, brighter days ahead and that it is possible to survive the unimaginable.

Introduction

> *"The first gasoline-powered vehicle driven on the streets of Detroit was built by engineer Charles Brady King in 1896. It went as fast as 20 miles per hour, which was described in the newspaper as "tearing along the street at a lively rate, dodging people and teams". By 1909, there were 200,000 motor vehicles in the United States, and by 1916, that number had expanded to 2.25 million.*
>
> *While the arrival of the motorized vehicle saw various cities implementing safety measures such as stop signs, rudimentary lane markings, one-way streets and traffic signals, there were significant numbers of serious injuries and fatalities. It was not until the mid-1920s, almost 30 years after the arrival of that first vehicle in Detroit, that a uniform approach to highway safety emerged, including licensing requirements for all drivers". (Loomis, 2016)*

Since the late 1980s, technological advances and growing global activities have combined to place significant focus and pressure around the question of how best to regulate the cyber world. We have witnessed the evolution of teenage hackers breaking into computer networks on a dare, through a growing incidence of disrupted and defaced websites, through increasing concerns around the malicious spread of viruses and worms and the major risk to business operations that they carry. We have seen an intensive increase in the cyber theft of personal identity, and most recently, we are experiencing the growing criminal focus of individuals and groups on espionage against governments and major corporate organizations. The media regularly reports on large-scale data losses, service outages and cyber breaches that are experienced with growing frequency and impact.

Addressing the issue of the introduction of gasoline powered vehicles eventually moved beyond reactive scrambling to installing simple stop signs and traffic lights to instituting a comprehensive system of highway safety legislation and regulation that is continually refined as threats shift and evolve. We now face a similar evolutionary dilemma with our digital superhighways operating in cyberspace. The risks are simply too great to allow full individual and organizational freedom in how the Internet is harnessed as we are beginning to see unacceptable levels of harm that result. It is time to develop and implement a comprehensive scheme for the acceptable regulation of cyber security in the interests of protecting all users.

The problem appears not so much in recognizing that computer-based threats and vulnerabilities *exist,* but rather in identifying the nature of those threats as a precursor to creating the optimal prevention and reaction strategies. There is significant motivation to address these matters, given that the victims of the growing cyber damage range from national governments through various corporations to single individuals. There is a growing and shared interest in addressing this problem, among the government, private sector, and individuals, all of whom benefit from ensuring the implementation and regulation of the cyber world.

It is not as simple as identifying a common interest against a shared threat, however. In a liberal democracy such as Canada, businesses and citizens also expect unfettered access to the Internet, for both personal and business purposes. Any proposed limits on this freedom are given serious consideration and critique, as elected officials debate whether the necessity of regulation outweighs the restriction of freedom in a capitalist society. The dilemma becomes one of balance: how far should a government go to achieve the appropriate level of regulation so as to protect users of the Internet, without unnecessarily infringing on individual liberties? When does

a legitimate focus on safety creep into unjustified overreach? For individuals and organizations engaged in the digital world, these are critical questions.

As cyber issues continue to evolve and threats increase, there will be heightened expectations on the Government of Canada to play a strong leadership role and coordinate efforts across both the public and private sectors in the country. However, as the government directs its immediate attention to the hostile actions of other nation-states, crime rings, and individual hackers, we need to ask if the current laws and regulations in place related to cyber-security for private corporations are sufficient to manage the inherent and growing risks associated with cyber security. The test is to achieve a level where the government's role in providing effective checks and balances exists so that security can be enhanced while intrusions into individual liberties are minimized.

Governments, businesses, and individuals are all vulnerable to attack. The private sector, however, is being targeted on an exponentially increasing basis. Typically, hackers appear to be one step ahead of organizations, despite the various security measures in place. Admittedly, responding to these incidents requires a significant investment that is often as much, if not more, than the costs associated with proactive efforts to secure IT related network systems. Even with these increasing investments, there is a growing regulatory and consumer impatience that both the proactive and reactive measures amount to 'too little, too late'.

At face value, the status quo cannot be considered sufficiently robust to handle existing and emerging threats, especially given the ever-evolving sophistication of attackers. There remains an ongoing need to continue to revisit the cyber strategies that exist, and the Government of Canada, working with the private sector, needs to ensure that more is being done at the federal, provincial, and even local levels. This was all but admitted in the Executive

Summary of a recent report from the country's Senate Committee on Banking, Trade and Commerce, in which it was made clear that Canada "has offered only limp responses to this real and rising threat," and that the "federal government should be leading efforts to make Canadians' information more secure…" (Canada, Standing Senate Committee on Banking, Trade and Commerce, 2018, p.1).

At the same time, the changing cyber landscape is being influenced by the growth of new types of digital business and technology. Digitized commodities will expand and increasingly be provided as automated products and systems in business-to-business and business-to-consumer relationships, impacting all facets of consumer life. Is the government keeping up to the changing world? With recent innovations like Internet of Things (IoT), and even cryptocurrency, Canada's challenge is also to find the right balance between oversight and innovation, recognizing that it may no longer be sufficient to rely upon existing legislative frameworks. Laws and regulations designed to protect Canadians have been slow to adjust to these emerging technologies.

This paper will:

(1) analyze the challenges and inherent risks associated with the overall use of technology related to the protection of customer information;

(2) review the current Canadian statutory framework related to the regulation of privacy and data management practices affecting cybersecurity and the regulatory and governance framework for specific federally regulated financial institutions (FRFIs)[1];

[1] FRFIs include banks, federally incorporated trust and loan companies, life insurance companies, fraternal benefit societies and property and casualty insurance companies.

(3) review the regulatory due diligence required of these organizations, by federal regulators, in their handling of the personal information of their customers, whether within their possession or after having been outsourced to a third-party provider; and,

(4) determine whether the current standards, policies, and practices in place are sufficient to address the sophisticated level of current cyber threats.

Cyber related Challenges

The Office of the Privacy Commissioner (OPC) of Canada is a non-partisan, Ombudsman Office reporting to the Parliament of Canada. It oversees the country's *Privacy Act* and provides advice and information to the federal government, businesses, and individuals on the topic of protecting personal information. The OPC outlines various challenges related to cybersecurity (Canada. Office of the Privacy Commissioner of Canada, 2014, sec. 1), including:

1. The continuing evolution of cyberspace, with its various interconnected networks, holds an enormous, and increasing, amount of data. Financial institutions have relied on information technology for decades, and some might argue, are fully dependent, on the digital data they have in their possession, including data that can be accessed in a cloud environment.

2. With the advent of distributed and multiple processing systems, these interconnected networks are inherently vulnerable. New revelations of vulnerability will continue to surface as more complex and interconnected technological and communication systems become available.
3. The unparalleled flexibility of Cloud Computing, that also promises to reduce costs, provides organizations an irresistible proposition especially in highly competitive industries, like financial services, especially during difficult economic periods. Uses of Cloud Computing services will only likely increase as more and more organizations become comfortable moving their data outside of their perimeters. According to Dupont (2013), within the foreseeable future, one-third of all computer data will be stored in, and will transmit through, systems administered in the Cloud.
4. The heavy reliance on mobile devices, by both individuals and corporations, in itself increases the cyber threats that exists. For many businesses, mobile devices are becoming the central access device to company data and many users do not appreciate the security shortcomings of their phones and fail to enable the available software security. For some, there remains a belief that 'surfing the net' on their phones being as safe, or even safer, than using their personal computers (Khan, Abbas, & Al-Muhtadi, 2015, p. 377).
5. The insight, through data analytics, that companies can develop from 'big data' has been touted as the future to customer interactions. The ever-increasing amount of information and data collected, stored, and produced by the vast machines that are connected to the internet requires a continuous and regular review of security techniques used by businesses. However, the general thinking is, the bigger your data, the greater the opportunity it presents to hackers.

6. Privacy breaches continue to garner attention in the press. And while there may well be more focus on the overall issue in Canada, as well as throughout the rest of the world, organizations appear to still be unprepared for cyber threats and breaches.
7. Finally, while companies are nonetheless required to comply with the various laws and regulations that impact them, when it comes to security, many succumb to a mechanical approach to overall compliance when responding to regulatory requirements. Using a checklist mentality wherein an organization ticks off a box to indicate that an issue has been addressed, does not in itself demonstrate that an organization is secure.

From a business perspective, what seems missing from their analysis, especially in light of the insights from the OPC, is an appreciation for the ongoing need to reevaluate the risks they face, and the overall security approach being taken. There does not appear to exist the need to either push for a 'reboot' of cyber security measures or at least the idea of revisiting their comprehensive strategy to address how cyber threats are managed. Instead, there appears to be a disconnect between the real challenges, threats and risks that organizations face and how best to address them. According to Craigen, Walsh & Whyte (2013), "it is impossible for any one organization, no matter how well informed, to fully grasp the challenges…" (p. 17) they face.

Threat/Risk Assessment

To varying degrees, countries are combatting cyber threats as almost all societies have become dependent on the Internet. While the public face of the cyber-attacks that confront Canadian society seems to continue to grow and evolve, does the Canadian government, corporations or individual citizens truly appreciate the breadth and depth of the dangerous threats currently in play? Potential adversaries are located throughout the world and, according to Lakomy (2013), there are several key reasons why Canadian organizations and Canadian citizens should take particular note of the intensifying cyberthreats they specifically face, including:

1. International commitments - Canada has a strong legacy of effective engagement in peacekeeping and other related global security efforts. For example, Canada is partnering with the European Union (EU), in a *Police Mission for the Palestinian Territories*, assisting in the effort to establish effective and sustainable civilian police forces in the territories. Similarly, Canada is also engaged with the EU's effort in assisting Ukraine in reforming its overall civil security, including police and the rule of law. Finally, after the 2001 terror attacks on the United States, Canada was part of the international coalition that was created to deal with the ongoing threats related to the al-Qaeda terrorist network, and the Taliban regime in Afghanistan. Terrorist groups in each of these areas have evolved in their cyber capabilities and it should not be underestimated that Canadian organizations could be victims of either direct or indirect attacks because of the country's international commitments.
2. Geography – Canada and the United States have historically maintained a key strategic alliance and economic partnership. This has been heavily influenced by the physical proximity of these two nations. However, this same proximity exposes Canada to the harm caused by direct and indirect cyber-attacks on the United States. Many corporations have

head offices in the U.S., with one or more branch offices or operations located in Canada. As such, it is not uncommon for a successful cyber-attack on the systems of the main operation in the US having significant impacts on Canadian customers. And the multidimensional cooperation between the two countries both at the governmental and business levels may encourage both state and non-state actors to exploit cyberspace to target Canada.

3. Past commitments to cybersecurity - there is also those who claim that Canada was relatively slow to adopt and implement its first official cyber-security strategy (Rosenzweig, 2012). Playing 'catch up' on the international stage in dealing with cyber threats puts the country at a disadvantage, enhances its vulnerabilities, and places the country as a potentially easy target for cyber-attacks.

Scott Jones, head of the newly created Canadian Centre for Cyber Security (the Cyber Centre) at the Canadian Security Establishment (CSE), the government agency now overseeing cyber issues in the country, in a recent speech indicated that “[e]very day, the CSE blocks hundreds of millions of malicious activities directed at the government of Canada” (Anonymous, Canadian Government is Improving its Cybersecurity, 2018, p 11).

Jones indicated that the CSE “decided to break the cycle and make it harder for people to discover our vulnerabilities" (Anonymous, Canadian Government is Improving its Cybersecurity, 2018, p 11), claiming that the CSE is making it more difficult for attackers penetrate government networks, depriving them of any potential vulnerabilities in the software and services running on their networks. He suggests that organizations similarly harden their

operating systems and applications (Anonymous, Canadian Government is Improving its Cybersecurity, 2018, p 11).

This advice is especially prudent for financial institutions in Canada and his comments are likely an indication that he feels more can be done. Their heavy reliance on informational technology and overall dependency on the interconnectivity of the global financial systems that they use makes them particularly vulnerable. Cyber criminals continue to target financial institutions not only in North America but around the world. These attacks embody both internal and external attacks using such techniques as ransomware, Distribution Denial of Service (DDoS) and sophisticated phishing campaigns.

While the Canadian rate of cyber breaches might be considered relatively low when compared to, for example, the United States, the average organization still faces 96 targeted attacks each year, one-third of which result in a successful security breach (Thomas, 2017). Over twenty percent of Canadian businesses reported being impacted by a cyber security incident which affected their overall operations and, after a breach, 49 percent of business lost customers, 43 percent reported damage to their brand, 41 percent had increased expenses and 37 percent lost revenue (Statistics Canada, 2017). Given the arguable disincentive to draw attention to cyber related attacks and losses, it is easy to imagine that this data is underreported.

More recently, the U.S. watchdog, *Risk Based Security*, reported that Canada ranked third on its list of countries most impacted by cybercrime (Contant, 2018), perhaps not as surprising in Canada's context as one of the "most wired" countries in the world, according to the Canadian Internet Registration Authority. In fact, "Canada has more computers per capita than any other

country….and Canadians are the heaviest Internet users in the world". (Canada, Department of Finance, 2016, p. 1)

Many large organizations rely on internal IT resources to help combat the threats that they face. Small to medium-sized businesses, challenged in their resource capacity, regularly turn to external experts for assistance, with many 'outsourcing' this function to cybersecurity consultants (CIRA, 2018). Admittedly, whether using internal or third-party resources, no organization can ever be 100% secure; the threat environment that businesses operate in is simply moving too rapidly for a full and complete defense. In fact, "[c]urrent approaches to cybersecurity are ill-suited to detecting or anticipating threats, which increasingly rely on hybrid socio-technical vectors" (Craigen, Walsh & White, 2013, p. 14), including such things as phishing attacks because they combine both a technical and psychological component to entice a user.

Despite this, most Canadian organizations indicate continued confidence that cybersecurity is being managed correctly (Stockburger, 2018). They argue that the objective of implementing comprehensive, risk-based, layered approaches to secure their systems is appropriately balanced with the overall customer experience they are looking to provide. To the extent that cyber breaches occur, they are being dealt with adequately. It is apparent that, instead of attempting to fully secure their network systems, the approaches that businesses increasingly adopt are to make it a 'more trouble than it is worth' approach for prospective criminals to breach their systems, so that those would-be hackers will look elsewhere for easier targets.

While Scott Jones summarized the general steps the CSE is taking to combat the threats the Government of Canada faces, at face value a far more active and aggressive strategy than has been taken in the past to defend the government's networks from cyber-attacks, he has also taken

his message a step further by highlighting that organizations could benefit from a similar approach, suggesting a need for better all-around security measures. However, no hint has been made that the Canadian Government is sharing information on the type of malicious attacks they face, and/or the specific steps they have taken as way of assisting private organizations in their efforts.

It is interesting that the Canadian Government has endorsed the *G7 Fundamental Elements of. Cybersecurity for the Financial Sector Guidelines (2016)* meant to assist financial institutions in their overall efforts to design and implement appropriate cybersecurity strategies. These guidelines address issues ranging from 'Governance' to 'Risk Assessment' and from 'Monitoring' to 'Responding' to cyber-attacks. Of note is the recommendation that financial organizations "share reliable, actionable cybersecurity information with internal and external stakeholders to enhance defenses, limit damage, increase situational awareness and broaden learning" (G7, 2016).

The guidelines are not mandatory on the financial sector in Canada but if the Canadian Government's goal is for individual businesses to step up in this area it would be helpful if they first led by example. The exchange of information requires a two-way street and there is currently no indication that the government has taken the necessary steps to share cybersecurity information with any stakeholders, especially those in the private sector.

My recommendation to address this issue

Private organizations could benefit from better collaboration and information sharing with the Canadian government. Something as 'simple' as sharing information on the perpetrators behind the malicious attacks each are experiencing could result in a better strategic and structured approach to defending against attacks. The Government, through its various agencies, should lead by example and initiate the process of information sharing.

Canadian Landscape - Data Protection and Cybersecurity

At the national level, only recently was the Cyber Centre established as a way to strengthen the national security regime in Canada and to allow for more focus on appropriate governmental responses to cyber threats and better coordination between various stakeholders engaged in similar efforts. Prior to this framework, which remains in its infancy, the agency responsible for coordinating the implementation of the nation's cybersecurity strategy was Public Safety Canada, given its overall mandate in coordinating the country's national security and public safety efforts.

Within Public Safety Canada, a specific department, namely the Canadian Cyber Incident Response (CCIR), oversaw cybersecurity nationally. Two other agencies, the Canadian Security Intelligence Service (CSIS), the equivalent of the CIA in the U.S., and the Royal Canadian Mounted Police (RCMP), worked with the CCIR and reported to the same federal government minister. This approach made it much more challenging to develop a coordinated strategy since no one agency was responsible for overseeing the country's national cybersecurity policies and laws. Instead, the Canadian Government had to defer to various governmental agencies and private sectors to develop the programs, recommendations, guidelines, and publications aimed at meeting cybersecurity requirements, including best practices for various industries.

As of November 1, 2018, in an acknowledgement that a more coordinated approach was needed, the Cyber Centre was charged with moving towards strengthening the country's protection and defenses against cyber-attacks. According to the Canadian Centre for Cyber Security, their mandate is to become the "primary centralized voice and resource for senior leadership in Government on cyber security operational matters, including incident management,

situational awareness, and technical advice and guidance" (Canadian Centre for Cyber Security, 2018, para. 4).

While the Cyber Centre is not expected to have full operational capabilities until the spring of 2020, its creation should be seen as a step in the right direction especially given that it has been suggested by Rosenzweig (2012) that based on *Canada's Cybersecurity Strategy,* first introduced and approved in 2010, Canada has not done as much work as the United States in developing a domestic government infrastructure for operationalizing cybersecurity. Only time will tell if the establishment of the Cyber Centre has any impact as it works toward its overall objective of developing "stronger cyber protection, defense, and security for the Government, the private sector, and all Canadians" (Canadian Centre for Cyber Security, 2018, p. 1).

That said, there are no authorities or public administrative agencies specifically charged with regulating the conduct of businesses engaged in cyber activity. Rather, the authorities that oversee specific sectors are generally responsible for determining policy and/or taking appropriate action for those that fall under their purview. As a result, the current legal and regulatory framework that exists in Canada to govern customer data and cyber security for private industry has developed over time, responding to issues as they arise, depending on the political will that existed at the time.

The framework admittedly is fluid and will continue to change and evolve. Organizations that interact directly with consumers, regardless of size, are expected to adapt to this shifting framework, bearing in mind the various laws, programs, recommendations, guidelines, and regulatory expectations. Included in this framework are:

- Personal Information Protection and Electronic Act (PIPEDA),
- Criminal Code of Canada (CCC),

- Canada's Anti-Spam Law (CASL),
- Case Law, and
- U.S. Patriot Act

The Personal Information Protection and Electronic Act (PIPEDA) – while not specific to FRFIs, there are many statutes that require organizations to protect personal information that they collect and within their possession or control, most notably PIPEDA. PIPEDA, as well as the various provincial privacy laws that exist, is intended to protect the individual privacy rights of consumers by requiring that organizations implement "appropriate security protocols" (Sirivar & Wolch, 2017) in order to protect the data they collect. It is meant to protect the use and storage of employee personal information by federally-regulated organizations (such as banks, insurance companies, and telecommunications companies), as well as protection of personal information of customers collected in the course of commercial activities federally (and in any provincial jurisdictions that do not have substantially similar legislation). PIPEDA applies within the geographical borders of Canada but also to all personal information that flows across national borders.

Of note, however, is that PIPEDA does not apply in those provinces that have substantially similar legislation, a group that currently includes the provinces of Alberta, British Columbia, and Quebec. To avoid any overlap in laws, those three provinces each have provincial legislation that applies in place of PIPEDA for residents in those provinces. This becomes complicated, as a result, for those companies that operate across various provincial jurisdictions, or for organizations that transfer personal information into a cloud environment; in both situations, a clear understanding of the applicable laws would be required in order to avoid any conflicts caused by gaps or overlaps in the regulatory frameworks.

The *Criminal Code of Canada (*the CCC) defines the following activities to be criminal in nature as they relate to ‘unauthorized access’ of computers and computer networks:

- using a device willfully to intercept a private communication without the express or implied consent of the originators or intended recipient (Criminal Code, 1985, s 184(i)), and
- 'intercepting fraudulently.... any function of a computer system' (Criminal Code, 1985, s. 342(i)).

Every G8 nation has a similar criminal framework that regulates ‘unauthorized access’, resulting in the criminalization of hacking activity. Canada has a far broader application of its unauthorized access laws by simply referring to ‘‘everyone [who] commits mischief” (Craig, Shackelford, & Hiller, 2015). This is significantly broader than the corresponding criminal standards in either the United Kingdom or the United States.

As well, Canada is one of a few countries that also has no specific provision mandating the required level of security or protection for the breached computer system or data. Other nations, such as Germany and Italy, require a specified degree of protective steps to be taken by the ‘owner’ of the computer. If these proactive steps cannot be demonstrated, the criminal law framework is not triggered (Craig, Shackelford, & Hiller, 2015). While any level of 'victim blaming' is distasteful in criminal contexts, this approach certainly serves to communicate the importance of all computer users engaging in safe, preventive practices.

Canada’s Parliament has previously considered amending the CCC to authorize greater government access to, and control of, private internet communications to support their overall cybersecurity obligations. Each attempt has failed, however, to win the necessary approval, perhaps signaling a strong view in Canada that any governmental regulation should be limited to only the most necessary and basic settings.

My recommendation to address this issue

Canada passed the relevant provisions of its CCC over 40 years ago, shortly following the introduction of the 1986 U.S. Computer Fraud and Abuse Act (CFAA), but prior to most other G8 members—including Germany, Russia, and the United Kingdom—passing similar laws in the 1990s, while the remainder—including France, Italy, and Japan—did not regulate this behavior until the 2000s.

A formal review of Canada's Criminal Code should be undertaken once again to take advantage of what other countries have been doing to address hacking activity and cyber security. At the very least, a targeted, more specific approach in such an undertaking would assist in the overall objective of dealing with cyber-attacks. It can also be used to demonstrate increased expectations of private organizations and highlight the need for them to have in place a specified level of security before criminal charges could be brought to bear on those perpetrators behind breaches.

Canada's Anti-Spam Law (CASL) is considered by many to perhaps be the toughest anti-spam legislation in the world. The first phase of CASL, implemented in 2014, imposed requirements related to the sending of commercial electronic messages. A year later, strict consent and notice rules came into place. The administrative penalties for violating CASL are severe, with non-compliance risking financial penalties of up to $10 million dollars for corporations, as well as statutory damages of up to $1 million a day. Once again, these rules do not stop at the border of Canada. CASL also contains provisions governing software installation, including aspects aimed at viruses and spyware.

Case Law – privacy and data protection breach related claims in Canada, both individual and class action, continues to evolve and develop. It is incumbent on financial institutions to monitor both OPC and court decisions to determine if any appropriate changes to their overall efforts in both securing data and in response to breaches need to be made.

U.S. Patriot Act - interestingly enough, one of the laws that impact organizations in Canada is not a law passed by Canadian authorities. The *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (The Patriot Act)*, is a piece of U.S. legislation that has provoked significant concerns from Canadian businesses, stemming largely from a deep uncertainty, and arguably a lack of trust, as to its application and interpretation. Multinational companies, with operations located in both the United States and Canada, fall under this law as does, more importantly, the customer data coming from Canada as it flows across borders.

Canadian companies remain wary of their accountability to their customers if, due to the application of the Patriot Act, their 'parent' U.S. organization proceeds to disclose personal customer information without the consent of the Canadian individuals involved. This could result in the Canadian organization that transferred the information violating Canadian privacy legislation in order to comply with the Patriot Act. This could be addressed through ensuring the customer understands that their information could end up being shared with the company's US counterpart but does not necessarily eliminate confusion around its applicability and raises various competitive concerns. The issue for our purposes would similarly apply if a cyber breach occurred to the U.S. organization and Canadian customer information was accessed.

Perhaps more importantly, personal customer information held by the Canadian office of a multinational insurance company, for example, on a shared network system, and accessible to colleagues in its U.S. operation, may constitute custody by the U.S. company and could lead to an order, under the Patriot Act, to produce that information to U.S. authorities. Taken to a

possible conclusion, if a cyber breach occurs, while this information is in the possession of a U.S. organization or even the U.S. authorities, what are the repercussions to the Canadian organization and its customers?

As a result, the possible implication of the Patriot Act on businesses and individuals in Canada remain quite relevant but still relatively unknown. At this point, no existing federal law in Canada addresses this issue. But because some Canadians have become so worried about the flow of their private information into the hands of U.S. authorities, several provinces in the country (currently Nova Scotia, Quebec, and British Columbia) have passed laws governing the demands for information by U.S. authorities (Siegel, Denny & Poff, 2019).

My recommendation to address this issue

There remains much uncertainty surrounding the US Patriot Act as it relates to responding to foreign orders and the Canadian Government needs to provide clarity, at the federal level, to Canadian organizations, especially on the interaction between PIPEDA and the Patriot Act.

Clarification directly from the Office of the Privacy Commissioner, or through amendments to PIPEDA, is needed.

Statutory and Regulatory Framework

In Canada, failure to understand the complex legal and regulatory framework, which has developed over time, around the collection and protection of customer data has its risks.

Companies need to take active steps to reduce risks (or the impact of these risks when they materialize) as they can have serious legal and financial consequences. So, it is crucial for organizations that operate fully or partially in Canada, or that even have business partners operating in Canada, to truly appreciate and understand the applicable laws and regulations.

As mentioned previously, both federal and provincial privacy laws (at least in those provinces where they exist) dictate how businesses are expected to collect, use, and disclose the personal information of their customers. While the intent is to protect the individual privacy rights of Canadian citizens, the laws, as they stand currently, only require that organizations take ‘appropriate’ steps in establishing and implementing security measures and controls to protect their customer information. While the measure of what constitutes 'appropriate’ steps is subject to continued interpretation by both the courts and the OPC, it does not communicate an objectively high standard to organizations operating in Canada.

This is clearly illustrated in PIPEDA Report of Findings #2018-001. Stemming from a complaint made to the OPC that VTech failed to adequately protect personal information of customers, or in other words, that they did not take the ‘appropriate’ steps, it was determined that the company suffered a privacy breach, impacting over 550,000 Canadians.

The report highlights that VTech did not have any of the following safeguards in place:

- A program of regular testing to identify common vulnerabilities
- No security monitoring and login to detect potential threats
- Poor administrative access controls, and
- No comprehensive security management program

To most observers, implementing strong information system controls, or identifying existing vulnerabilities and testing controls, would be considered basic steps to any effective

approach to cyber security, let alone to be considered 'appropriate' steps. However, since the term remains subjective it is up to each organization to determine what it deems to be appropriate.

My recommendation to address this issue

Administrative, cybersecurity and physical safeguards should form the basis of every organizations privacy protection regime as they look to protect the sensitive and personal information of their customers. Such measures go a long way in helping an organization demonstrate their overall commitment to data privacy.

If the OPC continues to believe that 'appropriate steps' should be the measure of what a company should have in place, there is a need to at least demonstrate and require the basic steps that should be part of any regime. For example, with the recently implemented GDPR legislation in Europe, it includes prescriptive responsibilities when it comes to security rather than leaving it up to each organization to determine what might be appropriate. It is really this type of clarification, either directly from the Office of the Privacy Commissioner, or through amendments to PIPEDA that is needed to demonstrate their expectations and in turn to hold organizations responsible and accountable for what they do, or do not do, in securing their computer networks.

As a result, the private sector, while playing a crucial role in implementing robust security measures to combat cyber threats, is initially only driven to meet the minimal steps as required by laws and regulations. Perhaps more importantly, as way to demonstrate to stakeholders that they are sufficiently capable of safeguarding the personal and corporate data that is being captured and warehoused, some organizations may strive for more than simply implementing the 'appropriate' steps required of them. This can lead to targeted cyber-attacks against those companies deemed to be more vulnerable as a result.

Organizations face even greater challenges in managing third-party vendors providing cloud-located services if they decide to 'outsource' this function as there is no contractual relationship between those vendors and the ultimate customer. In the absence of such a direct

contractual relationship between the ‘customer’ of the business and the ‘vendor’ of the business, the intermediary organization that initially collects the information actually has a higher duty of care to ensure that the necessary safeguards are in place by the ‘vendor’ to secure this information. This is not only the expectation of their customers but also the government as well

Statutory Framework – PIPEDA:

Personal Information Protection and Electronics Documents Act

PIPEDA is considered by many to be the single most important legislation in Canada that directly addresses the issue of collecting, controlling and storing of personal information, containing various provisions applicable to data protection and cybersecurity.

While this statute is quite extensive, it is important to highlight the following items from the Act as they relate to the various privacy practices of commercial organizations (PIPEDA, 2000):

1. As mentioned previously, organizations are ultimately responsible for the personal information they collect and/or is under their control;
2. Organizations must designate an individual who is accountable for overall compliance with PIPEDA;
3. Personal information is given a broad definition and includes “any factual or subjective information, recorded or not, about an identifiable individual” (PIPEDA, 2000, sec.3). Some common examples include items like age, name, ID numbers, income, ethnic origin or blood type. However, it encompasses much more, including opinions, evaluations, comments, social

status, or disciplinary actions. All are considered sensitive or "Personally Identifiable Information" (PII) and is explicitly protected under the law;

4. PII must be protected by security safeguards. The protective safeguards companies establish, both physical and digital, must be able to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, regardless of where or the format in which the information is held;

5. The nature of the safeguards is driven by the overall sensitivity of the information in question; the more sensitive the information the higher level of protection is required; and,

6. The methods of protection are to include physical measures (ex. restricted access to offices), organizational measures (ex. security clearances and limiting access), and technological measures (ex. passwords and encryption).

PIPEDA is similar to other privacy laws in other jurisdictions in that organizations "must obtain an individual's consent when they collect, use or disclose that individual's personal information. People have the right to access their personal information held by an organization. They also have the right to challenge its accuracy" (PIPEDA, 2000, c5).

Recent amendments to PIPEDA, effective in late 2018 although passed in 2015, now require very specific security breach notification requirements be met by businesses. Not only are they required to inform affected individuals as well as the Office of the Privacy Commissioner (OPC) but also keep all records dealing with the issue related to the breach. Canada has been looked as a leader in establishing guidelines on data breach notification and reporting. Canada's approach has in fact helped shape similar guidelines to those that exist in New Zealand and Australia (Siegel, Denny and Poff, 2019). While notification and reporting are important parts of any countries breach notification process, is this the area that a country wants

to be seen as a leader in? Does this not demonstrate an emphasis on reacting after a breach occurs rather than on ensuring that the necessary protocols are in place to avoid a breach from occurring to begin with?

Penalties, however, appear to be much smaller for PIPEDA violations when compared to other privacy regulations like those in the U.S. or the current General Data Protection Requirements (GDPR)[2] for Europe. For example, failure to report a breach to both the OPC and to the affected customers, and cases where no record of total data breaches are kept can cost organizations fines only up to $100,000.

My recommendation to address this issue

The Canadian Government could consider increasing the level of fines given when privacy breaches occur to match those of other countries like the U.S., and those in the European Union. Perhaps they should be more in line with the administrate penalties attached to CASL, which requires that organizations receive consent from customers before sending messages, where penalties of up to $1,000,000 per violation for individuals and $10,000,000 for organizations exist. This would demonstrate that protecting the personal information of their customers is as important as seeking their permission before sharing such information.

As well, if the Canadian Government is truly serious about ensuring organizations have invested properly in cybersecurity an, alternative would be for the OPC to 'incentivize' rather than simply apply fines. The amount of any fine could instead be required to be re-investing back into company's IT efforts to better secure their systems. This would necessitate perhaps that the OPC work closely with the appropriate government regulatory agency, and the organization in question, to ensure that the amount of the 'fines' are used appropriately and in addition to normal budgeted expenses, but such an approach would tie in nicely with the federal governments stated objective of partnership and collaboration.

Outside of some slight amendments, there have been no substantive changes to PIPEDA since it was introduced in 2000. At that time, nearly twenty years ago, the European

[2] The fine framework for a violation under GDPR can be as much as 20 million euros (equivalent to more than 30 million Cdn$)

Commission formally highlighted that Canada's federal privacy law provided an *adequate level of protection for personal data* from the European Union (EU) to residents in Canada (European Commission, 2002, p.13-16).

PIPEDA, however, was recognized recently by the former Privacy Commissioner of Canada, Jennifer Stoddart, as outdated. (Hammond, 2010) In her opinion, Canada's privacy laws are in need of a major overhaul. The privacy issues the country currently faces are much more complex than they were at the turn of the century. Canadian privacy laws were introduced with a principles-based approach, providing organizations more flexibility than the more prescriptive privacy laws that exist in some other jurisdictions. However, privacy and security challenges have evolved over time and the privacy framework that was initially created can be seen as largely insufficient to deal with today's challenges.

My recommendation to address this issue

The OPC should undertake a substantive, formal review of PIPEDA, with appropriate recommendations to be made to the Canadian Government, looking at best practices that other countries use related to cybersecurity. Such changes should be implemented in an appropriate and timely manner. The piecemeal approach of dealing with different issues and different times is disconcerting.

For example, PIPEDA was amended in 2015 and gave company's three years to adjust to the new mandatory breach reporting requirements implemented as of November 1, 2018. The EU's General Data Protection Regulations (GDPR) came into force in May of 2018 and could likely lead to revisions to Canadian privacy laws depending on what comes of the EUs expectations of personal data of EU residents that is stored and processed in Canada.

PIPEDA does not require complete and total impenetrability against cyber breaches. Whether theoretically possible or not, there is a need though to move beyond the current requirements that organizations simply meet the 'reasonableness' standard in terms of the security safeguards in place or that the security safeguards be 'appropriate' given the sensitivity of the information in question.

Regulatory Framework

A complex corporate regulatory framework has evolved over time in Canada that partners with statutory laws to collectively look to ensure the protection of consumer data and to address related issues of cyber security. Although many attackers are targeting larger, high-profile companies, all businesses should be prepared for such events, regardless of their size or complexity. As organizations consider how best to optimize for profit the use of the data that they collect from their customers, an equally serious level of attention needs to be given to best practices for *protecting* that critical data. The importance of addressing cyber security at the all levels of government and at the highest levels of corporate leadership cannot be understated. The increasing sophistication of cyber hackers (and hacktivists[3]), along with the expanding scope and frequency of data breaches should demonstrate the stakes that exist for national governments around the world as their respective citizens look to them to combat the risks.

Two key pieces to the regulatory and governance framework in Canada include:

1. The Office of the Superintendent of Financial Institutions (OSFI), a federal regulatory body that oversee Federal Regulated Financial Institutions (FRFIs), including all banks, insurance companies and federal pension plans, and
2. The Canadian Securities Administrators (CSA), an umbrella organization of Canada's provincial and territorial securities regulators.

[3] A recent phenomenon involving individual or collective groups of hackers targeting corporations and government bodies alike, penetrating and wreaking havoc on computer systems motivated by ideological beliefs rather than personal financial gain.

Concentrating on OSFI, given its oversight on Federal Regulated Financial Institutions, it is still important to highlight that there are rules and regulations that apply to the securities' sector as well. However, unlike any other major federation, Canada lacks a securities regulatory authority at the federal government level, instead relying on the individual provinces and territories to regulate the securities industry.

For Federal Regulated Financial Institutions, OSFI "regulates by developing rules, interpreting legislation and regulations and providing regulatory approvals for certain types of transactions" (Canada, OSFI, 2009, p.1). Through various "Guidelines" OSFI has provided "best" or "prudent" practices that they expect federally regulated financial institutions to follow. These Guidelines set standards for industry activities and behavior.

However, there are currently no guidelines or regulatory requirements with respect to cybersecurity specifically. Instead, OSFI's B-10 Guideline *Outsourcing of Business Activities, Functions and Processes* sets out their expectations with respect to "financial institutions…[who]…outsource business activities, functions and processes to meet the challenges of technological innovation, increased specialization, cost control, and heightened competition" (Canada, OSFI, 2009, para. 1). While OSFI has recognized the benefits that new technology-based services, such as Cloud Computing, can provide to organizations, they have nonetheless raised concerns about the unique features and inherent risks associated with these services.

Cloud Computing

Looking more closely at offsite cloud computing, it helps to return to the requirements of PIPEDA, including the clear accountability that any organization assumes once it begins to collect data, regardless of its jurisdiction, industry or the type of data involved. These organizations are deemed immediately to be "*fully accountable and responsible for the protection of said data. Organizations are responsible for personal information in its possession or custody, including information that has been transferred to a third party for handling and/or processing"* (PIPEDA, 2000, c 5).

It is this last part that is important for these purposes. It would be far easier (and tempting) to simply rely on a third-party, cloud provider to manage all the inherent risks and regulatory accountability associated with protecting personal information within the possession of the provider. However, that is not where the responsibility lies within PIPEDA. Similarly, OSFI has made it equally clear that all FRFIs falling under their jurisdiction are responsible for ensuring that all laws and regulations are being met related to the protection of personal information, notwithstanding whether that service is outsourced or not. As referenced in their B-10 Guideline, OSFI operates on the premise that FRFI's "retain ultimate accountability for all outsourced activities" (Canada, Office of the Superintendent of Financial Institutions [OSIF], 2009).

Even before considering moving to a cloud environment, organizations are expected to take the following due diligence steps (Canada, OSFI, 2009):

1. assess and define the scope of the services they are considered, based on their specific needs,
2. review and evaluate the different laws and regulations the organization needs to comply with as this may well define the type of service that can be used,

3. gauge, and then rate, any services they deploy to a third part cloud provider with respect to how critical it is to their business.

Guideline B-10 does stress that organizations are, prior to outsourcing any business, required to determine whether the agreement is ‘material’ to its operation by considering the following questions (Canada, OSFI, 2009):

- What is the impact of the outsourcing arrangement on the overall business of the organization?
- Will the organization be able to implement internal controls should the service provider fail?
- Is it difficult and/or costly to find an alternative provider in a reasonable period of time?
- Can the function or service be brought back in-house if necessary?

The type and level of materiality is to dictate the risk management program which organizations are expected to have in place, and should include the evaluation of items like:

- Confidentiality, security, and separation of property,
- Contingency planning,
- Location of records,
- Access and audit rights,
- Subcontracting, and
- Monitoring the material outsourcing arrangements.

The process includes the need to perform appropriate due diligence, assess each service provider being considered, document the ultimate decision made, and have the appropriate contracts in place.

Guideline B-10 is not binding on firms though and there is no current requirement that FRFIs provide OSFI with any formal notification if they enter into any contractual arrangement. The question that begs to be asked is why, if these are truly prudent practices and/or standards, OSFI does not require they be followed and why it is not more heavily engaged in the verification process if an outsourcing activity, like Cloud Computer, is being considered.

Appreciating that there was a need for some level of clarity, OSFI, in 2012, supplemented Guideline B-10 with a *Memorandum re: New Technology-Based Outsourcing Arrangements* (Canada, OSFI, 2012). Intended to specifically address the issues raised by cloud computing, the memo states that FRFIs should recognize the unique features of these new technology-based services, consider the associated risks and abide by the expectations contained in Guideline B-10.

However, to be clear, OSFI does not look, or even ask, for prior approval before such agreements are entered into by individual corporations. Instead, they have emphasized the importance of FRFIs ensuring that the outsourcing provider regularly tests their business recovery systems. With reasonable notice, OSFI can request a summary of these tests. This reactive approach though, again likely requested after a breach may have occurred, is insufficient to overcome concerns raised by many (Hammond, 2010).

A Canadian Privacy report found a range of "privacy-specific issues inherent in the cloud infrastructure", specific to such issues as data ownership, data "permanence", misuse of data, data intrusions, and security (Hammond 2010, para. 2). Perhaps of most importance is the Privacy Commissioners (OPC) concerns with Cloud Computing in general and specifically as it relates to cyber security. The OPC has questioned that while the users, in our case FRFIs, pay

for such a service, they are not provided with either "the expertise or control over the technology infrastructure that provides these services" (Hammond, 2010, para. 6).

My recommendation to address this issue

OSFI should conduct audits of all cloud computer providers who would like to offer their services to Canadian customers (ex. FRFIs) to determine if they meet current guidelines, with the corresponding costs to be incorporated in the annual fees that companies are already charged by OSFI. This proactive approach to 'screening' Cloud Computing providers would go a long way in demonstrated the overall desire for the partnership that the Canadian Government professes to want and can also ensure a higher level of protection is being met for all companies involved.

In 2013, OSFI released their *Cyber-Security Self-Assessment Guidance* (Canada, OSFI, 2013) document, including a template risk assessment tool, to assist FRFIs. Businesses are "encouraged" to use the template or similar assessment tools to gauge their overall readiness and implement additional cyber security measures, if necessary.

That said, written memorandums to the financial services' industry noted that they, OSFI, may request companies complete the self-assessment template during upcoming and future supervisory reviews and assessments. However, again this suggests a preference to a reactive approach in dealing with the issue, i.e., occurring after a breach has occurred.

My recommendation to address this issue

OSFI should not only require, rather than simply 'encourage', federally regulated financial institutions to complete the self-assessment (using the recommended tool or similar tool) but companies should have to file these self-assessments with OSFI on an annual basis, including any additional steps that need to be taken to maintain acceptable levels of cyber-security preparedness.

The template calls for a self-assessment rating from 1 to 4 (“Not Implemented” through to “Fully Implemented”) for each of several criteria grouped within six categories, including:

- Organization and Resources
- Cyber Risk and Control
- Situation Awareness
- Threat and Vulnerability Risk Management
- Cybersecurity Incident Management
- Cybersecurity Governance

What is noteworthy as it pertains to governance is that it is clear OSFI holds boards as ultimately responsible for overseeing the management of cybersecurity for the organization they oversee, for even the most highly technical matters. However, is this feasible? Do board members have enough education or corporate information to make appropriate decisions around cybersecurity? Some might argue that given the expense involved in protecting an organization against cyber-attacks there may indeed be a conflict given the board of directors financially motivated objectives as well. And while CEOs typically pay the price after a major breach occurs, board members “who should be front and center in cybersecurity discussions stay silently in the background” (Zimmerman, 2018).

My recommendation to address this issue

OSFI should require mandatory annual training for all board members in the area of cyber security. The curriculum should be developed and/or approved by OSFI to guarantee it meets the

necessary criteria to ensure board members gain an appreciation for the risks associated with cyber-attacks, the overall need for security, and the responsibilities that board members have in their oversight capacity.

OSFI recently announced, via an advisory letter (Canada, OSFI, 2019), that as of March 31st, all FRFI's are required to begin reporting all technology and cybersecurity incidents directly to OSFI, marking a very similar approach being taken by the OPC, given its recent revisions in reporting requirements. OSFIs new requirements, however, appear to be somewhat more stringent. For example, notification is required regardless of whether the incident involves personal information, and an FRFI must notify OSFI of an incident as "promptly as possible but no later than 72 hours" after determining a breach occurred.

OSFI's fixed notification period of 72 hours differs in PIPEDA's approach, which mandates all companies to notify appropriate parties, including the OPC, individuals and third-party organizations of breaches of security safeguards "as soon as feasible" after it has determined that the breach creates a real risk of significant harm to an individual. There is an understanding, if not an appreciation, that it takes some time for organizations to investigate possible breaches to determine possible impacts.

Only time will tell if OSFI and the OPC move towards a similar reporting process which will likely alleviate concerns that organizations may well end up having as a result of such duplicate and yet differing requirements. Suffice to say it again appears that more effort is being spent to deal with issues after the fact rather than on the front end to ensure that companies have the necessary processes and frameworks in place to prevent breaches from occurring.

Finally, the global financial crisis of 2007-2008 did result in the financial service's regulatory landscape in Canada, the U.S., as well as other countries around the world, moving

into a constant state of flux. More and more regulators are leaving less and less to interpretation and moving away from principles-based regulation to an ever more prescriptive rule making approach. In order to keep up with new requirements, firms are increasingly forced to direct resources from strategic initiatives towards non-discretionary spending on compliance and supporting technology. However, OSFI has seemed to have gone 'against the grain' by maintaining a less prescriptive approach than some other regulators. OSFI has in fact emphasized in past statements that it did not 'plan to establish specific guidance for the control and management of cyber risk', whether the 'service' is outsourced or not.

Conclusion

This paper has analyzed the current threats and challenges that organizations face in securing their networks against cyber-attacks and protecting the customer information they collect during their course of their operation. As it stands, and without revisions to current standards, policies and practices, the current regulatory and legal framework that exists in Canada is not nearly strong enough to address the sophisticated level of threats, protect consumers, and oversee the financial institutions that operate in the country. While the recommendations highlighted in this paper are but a sampling, rather than a comprehensive assessment, they provide a roadmap to begin to address the ways in which organizations can be

assisted by legislative frameworks in ensuring that the necessary security measures are being implemented.

The Canadian Government has made a number of strong indications that more needs to be done. The most recent Canadian federal budget from early in 2018, for example, proposed various cybersecurity-related commitments, most notably over $155 million set aside over a five-year period so that the Communications Security Establishment can create a new "Canadian Centre for Cyber Security." This is important as it would result in a single source of expertise, "providing Canadian citizens and businesses with a clear and trusted place in turn to for cyber security advice" (Canadian Centre for Cyber Security, 2018, p. 1).

This was quickly followed in the summer of 2018 by another positive move when Canadian Government renewed its overall commitment to implementing a strong cyber security regime when it published its new *National Cyber Security Strategy*. Reference was made that Canada recognizes "evolving threats, emerging opportunities, and the need for collaborative action" (Canada, Public Safety Canada, 2018, p. 1). Three themes were consistently raised in its strategy document focusing on: (1) privacy, (2) collaboration, and (3) using skilled cyber security personnel. Of particularly note is the goal that the "federal government, in close collaboration with provinces, territories, and the private sector, will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favor" (Canada, Public Safety Canada, 2018, p. 1).

While all might be considered important and necessary steps in laying the proper foundation in moving forward, they fall short in implementing new regulatory and legal

requirements for federally regulated financial institutions that operate in the country. There is a level of urgency in beginning such an effort sooner rather than later as it takes time to move from one regime to another.

For example, the European Commission acknowledged back in 2010 that their privacy regime, at the time known as the Data Protection Directive (DPD), was no longer affective or appropriate given the rising technological developments experienced around the world. At the time, they indicated that personal data must be 'effectively' protected, whatever the technology used to process their data'. Even though the DPD was for all intents and purposes repealed n 2012, it took an additional six years for their new regulation, the GDPR, to be implemented (European Commission, Communication from the Commission to the European Parliament, 2010).

As well, regulators and corporations in Canada were slow to respond to things like Big Data and Cloud Computing (Dupont, 2013). Should Canadian society feel confident that these same regulators and corporations in turn are addressing the new security challenges posed by additional items like the Internet of Things (IoT), brain-computer interfaces, near field communication payments systems or mobile robots? Each result in an increase in the overall amount of data collected by organizations, an increase in the connection points across the Internet, as well as the speed and velocity that this information flows throughout these interconnected systems.

The use of smart home devices, for example, has been growing in Canada. It is estimated that within the next 5 years over 35% of Canadians will use a smart device in their home (Canada, Statistics Canada, 2018). These devices pose both a privacy risk and cybersecurity risk

given their connection to the internet. No specific law in Canada currently exists addressing this emerging risk and there are no indications that one will be forthcoming. Existing laws offer little protection and PIPEDA is in no way strong enough to regulate companies, either manufacturers, retailers or users. If the Canadian Government took the initiative and responded to the Privacy Commissioner's concerns, then we may see news laws and regulations that must be followed.

The G7 Cybersecurity Guidelines for the Financial Sector laid out best practices that could be applied across the member countries. Canada can do more to learn from the other G7 countries, i.e. France, Germany, Great Britain, Italy, Japan, and the United States, including incorporating some of the recommendations already highlighted in this paper that they are engaged in.

And while Canada's new National Cyber Security Strategy highlights their goal in the area of cyber innovation 'by supporting advanced research, fostering digital innovation, and developing cyber skills and knowledge' this may be more of a panacea given that, according to McLeod (2018), Canada is already facing a talent shortage as it relates to cybersecurity experts. Current projections indicate that the demand for cyber experts is growing by 7 percent each year, according to a report from Deloitte. This not only provides a challenge to Canada's objective of leading the world in cyber innovation but puts companies at risk in not having the necessary resources to deal with both existing and new emerging risks in the future.

As we struggle with the global phenomenon of appropriate cybersecurity frameworks that adequately balance individual freedoms with protection, it is time to recognize that installing haphazard stop signs and traffic lights is no longer an acceptable method of addressing the

information superhighway. Rather, we must push to be thoughtful, strategic and proactive in developing a comprehensive legislative model that will last into the future.

References

(December 13, 2016 Tuesday). New data from the Canadian Internet Registration Authority shows Canadians embracing mobile and Internet-connected devices, despite concerns about cyber-security. *Canada NewsWire.* Retrieved from Nexis Uni.

An Act respecting the Criminal Law, R.S.C., 1985., c. C-46 (the "Criminal Code"). Retrieved from: http://canlii.ca/t/53jff

Anonymous. (2018). Canadian Government is improving its cybersecurity. *Information Management, 52*(6), 11.

Beardwood, J., & Bowman, M. (2016). *Cybersecurity evolves. Understanding what constitutes reasonable and appropriate privacy safeguards post-ashley madison*. Cologne: Verlag Dr. Otto Schmidt. doi:10.9785/cri-2016-0603

Bodrov, S. (2018). The new and improved PIPEDA. *Mondaq Business Briefing*. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV07T8MwELagLGxFvEoBZYEtqHFixxkYCm1pEUMFRWKrHPtSMRBK0_5_7vJoKFMZWKzoHFvy3cU-O-fvY8znNx3315ygQishxtXIhsYjkDcRayWAG7BR7OcwBoOhfHhWvafwsSYxq2X_aniUoenpIu0fjL_uFAX4jC6AJToBllu7AeUwdintNz9AwAhzPBr3e92fcSl-2lZ_1Wnwd7iDTqpVrcgmxKZFWpjeOCrwVH5nTq6NW3ZVpQttYE-_jcJNYYGJS9yZGKPJzjUhkX_Yd7O8hdR9fdlle9wPI1HAd9bohoKooxpVYmG5Ok2arElz9lzPYeF0C10csB1ID1kb9eBgpYN6cCo9OIUejthk0J_cD92SF8KdYXjmQoK-o0XMk0AC7qiAS2uJl9DGPAoCE-GeV0WJIbaGDvAglBjXgbLaaBOIIPGPWSP9TOGUOZ4fciutoP-D1DICDr6SnpHSSgGixa5oKNOSEBSLjI5MspleZdm01k6LneTvkV8sF9pM1zVnW_bQZvu1xc5ZY7lYwQXBkGVEqXOZa_kboyoFeg

Campeau, M. (2018). Rules tighten for reporting data breaches. *Canadian HR Reporter, 31*(11), 8. Retrieved

from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1NS8NAEB1s CuLJb6zVsnjzEE1212ZzklabFhWRoFRPpclOLkqqtv3_zm43KhV68ZIcAmHIbt68dh5AIK fBf4SJoQyy3guKBxBFBTMxWGRqawQWuaiiG3cmAza_VRd30U3rrnQHI1xy12hpIVuPc lN1vycQDeWoVF4vHz_8I2OlKm3OlGNGtS5GQfmQb3TfRr2v9GZCIGtXyr60TlXz38w2 DqWZBNeKxu0k0ogNmvkTWz-T0qxNLbxX9ZuQYNck0b2K1fHOoutsw1rWO7AetUIvwun6fwNp2xmoncsGZFbtigwkLN jprGUUTRtxkFP9-Ak6T1eDfzKpJGrRIx-zBH74JWTEg-AYRDzSAd5EGkt2zhWKMYyjJFfZBExubwBzRUvOlz5tAkbxDXU4hjfEXizzzkemzlb9q O2oBYNX-iqktuWWzK6d3v3D-kXWpmuBA

Canada. Communications Security Establishment. (2018). Canadian Centre for Cyber Security. Retrieved from: https://www.cse-cst.gc.ca/en/backgrounder-fiche-information

Canada. Department of Finance. (2016). *Canada Supports G7 Work on Cyber Security.* Retrieved from: https://www.fin.gc.ca/n16/16-133-eng.asp

Canada. Office of Superintendent of Financial Institutions. 2013. Cyber security self- assessment guidance. Retrieved from OSFI website: http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx

Canada. Office of the Superintendent of Financial Institutions. (2009). OSFI *Guideline outsourcing of business activities, functions and processes.* Retrieved from OSFI website: http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx

Canada. Office of the Superintendent of Financial Institutions. 2019. Technology and cyber security incident reporting. Retrieved from OSFI website: http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx

Canada. Parliament. Standing Senate Committee on Banking, Trade and Commerce (2018). *Cyber assault. It should keep you up at nights*. Retrieved from https://sencanada.ca/en/info-page/parl-42-1/banc-cyber-security/

Canada. Office of the Privacy Commissioner of Canada (2014). Report on *Privacy and Cyber Security: Emphasizing privacy protection in cyber security activities.* Retrieved from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/exploreprivacyresearch/2014/cs_201412/

Canada. Office of the Privacy Commissioner of Canada (2018). PIPEDA Report of #2018-001. Connected toy manufacturer improves safeguards to adequately protect children's information. Retrieved from: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-001/

Cloud computing and Canadian federally regulated financial institutions. (2011). *Mondaq Business Briefing* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV1LT4NAEN5ovXir8VVf2YteDKZAd5Y9eNAqrcbEROu52Vcbkwq1tP_fWSjQmpjowcsGBtiEbya7M8PwDSFhcNX2vq0JETdgFe5GhmvfkbwxJSNmA22NUGFOYxD3ofcS3T3xx7p7Yi37V8WjDFXvfqT9g_KrSVGAx2gCOKIR4PgrM-hO0oW5LHo35BmQBM9KRoLYMUnIycT54XlLevQ-4xUKjqKOoMrolY2fUgzjP-uS-VuMtkflDmhWM6LtOtxcPlQWEa0xUj88x-vCgik3AFwJBBdw4fjJP8y7nl_bxHt73SRbQcgFK0g9a85D5hpKNcpyw3KfGzRJ0y3lUzm1M3pTQLRDNmyyS3o5PLSChyI8tISHVvDQCh5awUNX4dkjg_h-0O17y9YS3hgjNi-yNuqokCuF3rKvGFh00yJQMgTHzy9A-iABRSwQlmPEq9BvVmBGkTBao9e8TxpJmthDQv2QBwYMc58YOx0thA0sTuVrAAPM

shY5d-
89XPYUxSFzWZdsLBdZNqyhbJGD_D5nWvOZ1MPqytGPV47Jdq3QE9KYzxb21HGXZ
a4Pz1muhC8rmxs9

Cloud computing market in Canada 2014-2018: Key vendors are Amazon, Google, IBM, Microsoft, Rackspace and Salesforce.com (2014). PR Newswire Association LLC. Retrieved
from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwxV1LT8JAEJ4gX
DypUSOiZOK5aF-01YQYQAqKGENU4okUdktMsKtFEh-
_x__p7JaqAcPVS5tmk3Z3ujvzzc7OfACWeaiX5nRCOHQ8mxmh7g1c5jplAv307FoBIWCj
PJABXr_lNLve2aV7kYGPNDVm9rtTLalUNxNDuWt-
JLGKLLKrO6dPzyXJIyXjrSmpxneWWXIchKCo5CZZqFUbjyvBjJaBVQyZk78COfIaXLl
C3N79gopWdsdfg8-
0i399wbatuaqO_zSYdciTzWMcf20CYjWZkxuQ4dEmvNbHYsowIZEgc4kdlW6NDxGqA
gkBEkawaTUZ3gm2-
Rve8YiJeIJBzLH6GLyLSMOmEKMx1_C81tGwI48STsiKaNiVhQLI-
ecYRAyp11xi8YQ6ZQsO_MZNvVVKBdKfhUn6P8KwtiEbiYjvAOosIP2iOzTpQtvWh8ch
ITHH4eSCcS90zTwUlrxod2lrAVbVIMkmmeYeZF_iKd-
XRcCUnItqJtDV89tFyFVrt70m3WuNq-vuF-3I5ns

Contant, J (2018). Where Canada ranks worldwide in cyber breaches. *Canadian Underwriter.* Retrieved from:https://www.canadianunderwriter.ca/technology/canada-ranks-worldwide-cyber-breaches-1004136764/

Craig, A. N., Shackelford, S. J., & Hiller, J. S. (2015). Proactive cybersecurity: A comparative industry and regulatory analysis. *American Business Law Journal, 52*(4), 721-787. doi:10.1111/ablj.12055

Craigen, D., Walsh, D., & Whyte, D. (2013). Securing Canada's information-technology infrastructure: Context, principles, and focus areas of cybersecurity research. *Technology Innovation Management Review, 3*(7), 12-18 doi.org/10.22215/timreview/704

Dave Kearns. (2010). *Document offers gloomy view of cloud: A report by the office of the privacy commissioner of Canada is critical of cloud computing, but seems confused about what it actually is*. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwxV1LT8JAEJgXPSCokYQSQ9eq6W73S0HYkApBB8xBEM8kb7WC6HI46C_xx_qTGkrAePVS5vuHtrdnX47O7P7fQDMvDL0LUxQvrB5UFeG7clACgudfnyWzEUPuG55lOB1eqI7sO8eZD8Hn-nRmGS4U5SMoTuIfIqaX-PEJolMxb6ZveskI0Xp1lRTIztktt4Ngp4oSZPsUNXOJ003UWUImnU6kr8HBVw0SPpB5Og1A3UiOt-B6xhynSJ8pZ_72-s4Z1sMj__TsEMo4_QXhNpGPFBrrc3zCHLhtATFVElCS4ClBAcbtIj49JhxyS6O4RLnwRXFMLWItFwW2tsEnf0PjRqBRZo_iVbBCQydzvC2pyfaDvoM10i6CLF9VuAxxl2XmQ1S_6CcqOSuZwpf2b7X8N3QMFUDTcdCJ5OoERkXtlK4JmDsFPLTaBqegWYELuKOIdAYFeeG31DooQkR4tIstJU0y1BNe3nsehQ_8peLcdbHZahk1Uma5qey8lflOeyvtxJw3RBVyC_nq_CCmMPiEanF9oNX27mvQaHVfhl18d7uPD0PsNQZ9L8BoYvypw

Equifax says 100,000 Canadians impacted by cybersecurity breach (2017). Toronto: Canadian Broadcasting Corporation. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1LS8QwEB7c

7WVPKio-S7x5sJpt09dpcbXdRUVkUTwuaZKiCK1rLdh_7yS2KOtBwXtIhiR83zyS-QA894Q6S5ggeTbMaKzyHKGSUeGHOXryUoUxRYJWOlOQToPJLLq4Di_bx4X6a0x73B1KGuiWpdBZ81MMv90QJ4uj0cvC0TpSut7aimr0wEJq8_DmW-Pk5nb2vRLmsTD4Ab2GT9JVeO6Wlq1CAjqxWtXEpP0Y85a6Nf7LyDUYGEYy-LAOK6rYgFGyqJ9y_k4q3lRkSOkx2ky6VgUV-fw8qSTJGiKaDH3EVueOYAjNxeMmHKXJ3fnU6cyZ433RRQBeqLKu5l8GeVvQL8pCbQOhIs48X0o_4zkbMpcHKlcUYz8R6458bAcOf51u9w9j9mDgalrUEgzxPvTfXmt1oJttmS22oRelVzZYZ-P7h4ndntwHOcexOg

European Commission. (2010). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, ‘A comprehensive approach on personal data protection in the European Union’ COM (2010). Retrieved from https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

European Commission. (2002). 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C (2001) 4539) Official Journal L 002, 13 – 16. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002D0002

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security, 13*(2), 113-170. doi:10.1007/s10207-013-0208-7

G7 (2016), G7 Fundamental Elements of Cybersecurity in the Financial Sector, Retrieved from: https://www.fin.gc.ca/n16/docs/g7-1014-eng.pdf

Harold Gallagher, Wade McMahon, & Ron Morrow. (2014). Cyber security: Protecting the resilience of Canada's financial system. *Financial System Review,* , 47. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV3PS8MwFH64DsSLv0WdjuDFU7UmWdp6kW2uGyoyquJxtEkKQ2l104P_vUmaKEzYxVMPgfLIC9_7ePnyPQCCzwJ_ARO4VlNJzggmUl5QHgiaE4FZQSJBBTVPiUdsmEbXd-GNFRfqpzE23Q4lDXSLiuuu-bki-qrYMBrRq7d3X8-R0vetdqhGA5pYu5d70Oz2np6HP32XoBMplmJ096E24cRx8AeGTW1JNuDFhSHstARFaPWEE9MCpJQsODf-K-BNWLcUFHXrM7MFK7LchlWngN-BpP-Vyxl6sJPtLtG49nJQRQ4puohSOZ--GkRAVYGMvUF2OkeJ8-5AtQv6Lpwkg8f-yHdRTuz9xOQ3QrIHXlmVch8QyTo54TzMM5JRkcU55ip_jMUSF4rAFAfQWvKjw6WrLVhTDITW-pAj8D5mn_JYu2-ZfW5DI0pu2zaF6tsb3I_Tb6AVtLE

Hammond, Brian. (2010). *Canadian privacy report offers skeptical view of 'cloud computing'* Aspen Publishers, Inc. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2AwNtIz0EUrE9KSzSxMUgzTDCySzFPMzUyBjX4g39w4EdgCNjRNAk3wunmYuQdZuPiYezExVMG2xkCjG1ZKgovulPxk0Ki5vpEh-NoIA0v7gkJd0DVSoOlW2J0a8E1mkNUgwJYo6GoSjKNqi3JsE6G3MqTYGoK25DMzsAI7DeagDGIeHolRQoNLUTcBhiUwF2KzwcTEGO1Qx4HxiyCDJLDGS0lVQBoCVHCEpEghBqbUPBEGJ2dHP0cXT0c_hYAgzzBH50iFINcA_6AQBX83N9egYIVgb9eAENDJDAqgtRpAUQV1Zx__UBcFZ3_fgNAQTz93dVEGRTfXEGcPXZjP4qHTHfFwXxmLMbDk5e

elSjAoGKQkAosJAzNg2kkzMTFItkwDNqjMzFKBPalUizRzI0kGKdzmSOGTlGbggkztm-gamMowsJQUlabKgk7yAgeXHDg-5RhYnVz9AoIAg7XMHA

International cybersecurity law. (2017),339-359. doi:10.1002/9781119231899.ch10 Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV1LT8MwDLZYd0FceIo3_QF0tM2StAdOsDEhTjDOFU0iwYEisXHYv8d5qCErQuqBS1RFrqPUke249mcAko_SZE0nFFwyVaM1klxkGuSN1i8FVblQsqyJgTGYztjdY3H7wO99yyI_96-CxzkUvS6k7SH8lilO4DMeARzxEOC45h-HkVgLPbCq0btzHep8vNonr_tY4O-kLhyAJqZNvrOquptvEyZV2osjajjt2dG0_KG8iIUVcnaQWKTujoq1kK2eB17YRuLV5aaG0NV_kmto83f5JpbXqkmenwYwRO8hpREM0SBP2pBLbt5093cTOOO6qKU0XZ_cJrjD7mo35aqjcO2r7srhNcSYx_k2bOnaklgXfeAOdmBDNbswwK-9BxeBPOJAHjFS7AOZTuY3s8RwrcxP7kVl4aDzKli_0uubgRxA1Hw06hDijPBcMkn1T8rxWJSlyhUpWCYYk4wqegSXfTgf9yM_gU1_jE4hWn5-qTONf7bQvXzOnTS-AaPGHMY

Jackson, E. (2018). *Canada's privacy watchdog asks Facebook for info on data misuse that raises 'serious concerns'*. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1LSwMxEB5sexEPKio-y3iql0r34aZ7EqvdFhWRovRmSXZTWwq7ddMq_ntnwi5CPSh4DJtsBmb4MpkvMwPgueet5gomuCJshUIlnlbk4o-Vr4OxGCtHBIknHZsjFvWD3qB9cy9ui8eFnBpTqLtESQvdSRZz1Jyu7dzzpu07_uX8rcl9pJhvLZpqVKBG3z2y_Fqn-_A4-AG19vyINmFWbpUUHRHIaeUuJjbM5_veSnXGfwm1BRtDrbAMzG_Dmk534MXWIZANg_N8-i7jT_wgFJ4k2StKMzMYydgSp0heLLLZYZYivx9FsoSl0biYyAXmzDQZbLDhZkuDMWc

95qlp7MJZ1H267jdLeUe0jFkBmWqaOPqW2NuDapqleh9QCTrLBTP0UvkhXZmEq5KYlOUGwruQrQM4_fV3h3-YcwTrNLBJfk54DNVFvtQnXH3L6qAOlXZ0V4faVed52KsXqvwC8k65UA

Karn, B. (2013). Cyber security: OSFI issues self-assessment questionnaire. *Mondaq Business Briefing* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV1LS8NAEF60XrxVfNUXuehFIkk2m80KHtpqbUUo2HouSXa2CJrWJD34753NkxYEPXhZwuyyJN8MO5lh9htCqHNjmRtngs-lByF6I8kjW5O8sTDwGTgRSBHSnMZgMPQeX_z7Z_7U9NNqZP-qeJSh6vVF2j8ov94UBfiMJoAjGgGOvzKD_lcISZlVz3J2p_FkMCqb7qH8XZndmpzzOk9_4rvEQVUUWzV7WmDo_tmUyfcwwlaV19PndVkU3IMkLqvpqlyCTctLdXU9UbFXVU-0Rk49Gg_WhQVpLnW5h0ETt640VfmHfIuyO4jN18k22XEoF6zg92zoD5nuLdWqKg9LdzZtk7Y-1JfBEhKjW4C1R7Yg3iciB8qogLo1NExGAZOxAZOxBtMBmQ4epv2hWbaVMOf4d2e66LIDHgkpMZRTAlQUCs5sakOggCoJIVOKCx2oCiZEIPCP1gqd0PIBV9s2PSSteBHDMTFsyh3pSaaXum4kBDhAfc-OPE96DFiHXOoPnZX9RHFIdcYlnQerNJ012HXIUb5Om1WWBNGsnjn5ceaU7DYaPCOtLFnBueYtS3UPnosc9W_pVBlJ

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science, 56*, 376-383. doi:10.1016/j.procs.2015.07.223

Lakomy, Miron. Cyberspace in Canadian Security Policy, Central European Journal of International & Security Studies, 01/2013, Volume 7, Issue 2, 102-119

Lemieux, M. (2015). Cyber crime, governance and liabilities in the banking and payment industries. *Banking & Finance Law Review, 31*(1), 113.

Li, L. (2018). US privacy laws in a global context: Predictions for the next year. *Computer and Internet Lawyer, 35*(9), 42. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwxV3JTsMwEB0VuHBih1JAvnAMxI7bOEgIsbQghBBiEeIUTeykqoRaaFoW8T38J-MspWK7cskhY0Vxxh4_z8TvAXhiy3W-xAQCyZGSiYsYidhg3bKw-UHsGomRqzM1t9ZJ4_hSHZ35pxV4K4_GFO4uo2QWuk1P26z5Nm1WlLJpFL738OhYHSlbby1FNUanzPLfQQiKWm2Sb1y1_ftdLGQZzC63Z_InYIp2DcpOcv_2blSRoJXZzblXac8VSPlbCM_WpdYMvJdd-OkNpPS-sD7-U2dnoUproonZWJKQ7edjdg4qcXceJs7weQEObq7YRb_zhPqV0Y2UdboMWa5LwDIirZfBDrWw1aVswjDC3IwwLDsnC7ujri3CTat5fXjiFCoPTpsT3HQaNIyEMJ5BP1EiMLRqe4EnA46RJc1FJdFwLdzIsiUaHicuxe-Eq0QniRBaeksw2e114xVgJiH0xVUDA-QyknUV0MMa9OG0EojSr8Km9VlY6HvSJbUZkLSNwzQN9wlZ-UFdufUqLGft7Bwf9FGHY5b10j0hRjYZpQdp-OmcKtRG9qLoM2Zd_dNag2lCYyr_gW0NJgf9YbxumcgyZ25kw3EDpg6a5xeXH1UiBvQ

Libicki, M. C., & Rand Corporation. (2007). *Conquest in cyberspace: National security and information warfare*. New York, NY: Cambridge University Press. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwdV1BS8MwFH7ovAgenFrq3GZO3jqypG2a45huY6gH8V6aNAUvFcRL_70vb7ETocfwICEhL-97H-97AZBiwZN_b0JtMY0wqcyXVti0Vpn2gU2lxlgpmooE37t8-1Y8Pqv9sWuOPRR7dAtEkv5rkb6yxrMXCDQQO5wiJioEoaFVT65wgWmFyoI2NdcCQX8Y-

ASBy9B659eYHsdk59QBipb8E202lzDyCoQxnLj2CuIX6qP91bEH9lrhvWDBHa8hWn-29Kyzj5bZznjdZGXdDdxvnt7XuyTMXQaKpgx7USKCi8pXtrffpICrY2BL6bgUWe2aAqMtZrNaFsqgqxmjrM70LcRD002GTXdwfmApPZkwhbMGL7ub9bue03n-AKA0dtw

Liu, J. (2014). New study on cybersecurity calls for increased awareness and protection for Canadian companies. *Inside Counsel. Breaking News*, Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1NS8NAEB1sevGkomKtlsF7NM1uPjxJq02LikhRihfLJrsBUbZqFfHfOxM3KBV68ZIcNmyGzO6byezMGwARHgb-AibEZZxHpSzLXAgVCmVUGXVTo6I418oIrnfORvFwnJ5dJucuuZBLY5y6a5SsoFvPCo6aH9FeJWBlA3Xy_OJzHyk-b3VNNRrQDJkOzINmr387Gf6B2sp-ZGvwWL9Ku44I5LRyF5MqzCelWGBn_JdQ69AiC6QN_grJYe97hWzAirGbcE_YhhWzLNJY8ZmTE-ga2SEp7WmO5Mvig2WXcm40qg-uGSNQRGU1Om4HnpYfqwkOsMpnt_TrvQUH2eDmdOTXwk_d0cT0R3CxDZ6dWbMDyIWzQa5kQpqWUqljLtEKhNZJocO4kC1oL5lod-loG1bJ-ZCcdtVN98B7e303-0y8VX3-DjSSyR1d0-yi43RI9_7g6nr8Ba8cux4

Loomis, Bill, " 1900-1930: The years of driving dangerously", The Detroit News, April 26, 2015. Retrieved from https://www.detroitnews.com/story/news/local/michigan-history/2015/04/26/auto-traffic-history-detroit/26312107/

McHardie, D. (2001). Internet privacy law now on-line: Affects federally regulated groups at first but will cover most e-businesses by 2004. *The Globe and Mail (1936-Current)* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1LS8QwEB509-LJFd-PJX-gavNqexIfWxcRkcX70iYDipLWsrr47-

2krUJlT0JugcwwGb4MM5NvAAQ_PQ96mBBHVmNev0Y2MiGRvKk8ixVygzbJhacxSKf6dhbf3Ed3bXMhfY1pr7tDSQ_dtjCUNT-rIwVit1I6vijfA5ojRfXWdqjGOgy5kFHtcOrycPj7Key8PfzTg-DPW6mm_Da6WDbUQl1NEvjTXz-T0rRo238l7YjGBGmlVmJFbtsXGYL1tBtA2syg7hgZfXymZkv9pYtmSuWrHABRaIE4nT9fToBM7f3bl_Fec2IWBKxzuAwtFxK22isphUpokQY4i1qHR2mqF6gD2VhxyuHLnCDaatqx68WMYLKoPPCH-LG-scWv-b3LemnQ

McLeod, J. (2018). *Canada facing a talent crunch when it comes to cybersecurity experts - and things look likely to get worse*. Toronto: Postmedia Network Inc. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1LS8NAEB60vYgHFRWfZbx5ieaxefQkVvtARaQoPZZNdmpra6JtSum_d3ZJEOpBwVNYyGYHvjDfx-zufACee2FbKzlhQAFFThB6rh2rKEhC8p1EqNBRdV_6gblK3Ana3ej2IbwrDhfqqzEF3GWWNKlbZYmuml_qxuOuoZirj09L-0jp_dbCVGMdqq5WNxWoXjdeeu0fqdbwR2sLxuVSqnBEYNGqXUxMmU8Ib6U747-C2obNHsVYFuZ3YI3SXXgzfQgkDmTCbIUSWXUz4WAyZWYb4mJIKY54mL3TDMMk2XMyrBwt0NjBJDP0EKZKsyN2SdOWKDjZDSmyVLPeKUcFxnP2YPzVvP5pmOVsff5Z9I7BDKlbD7rf0fv7UMlzVI6AHRCspWQrGzigfBjNyblMHDStYVDKhaHcPbr 547-8M4xbDBkkTkLWz-BSj6d06nuxGXwqMF61LqvFXDys9F8fOp-ATjWvtw

Mee, W. (2018). What to expect come November 2018: Privacy commissioner's final guidelines on mandatory breach reporting under PIPEDA. *Mondaq Business Briefing* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV1NT9wwELVguXCjaqHQUs2l7SEKSuI4H0g9QGH5EGJXNFWPK6_trPZAlia7_P7O2NkEkCrRQy9W5E

RW_Mbx2JPxe4zx6CjwX8wJWaoTM0VvpFMVEsmbmMpMmEgZnU-5pTEYXiYXd9nZTXrdS3z2df_V8FiHpqeDtP9g_K5RrMBrHAJY4iDA8lXDgKi5vWJhKY3Vkj5_490uHg3pgHjoljMKCYzr-SPJvtNpkXljJXdcIH9oNbMuVsSFRfnx3qiihBntfs2f1pSK2a7hKeRgRZS88dX4_Ozk6aoXJw4tf_dJ9qe4Py_XPtOy_9qw6i9TtVS3bRgizNrzeF0qkmtonYr0jNf6ajR8Xun4dnGtlcbEQvqFWM7v9Vwtv5nK__ljk21FPM2FowbtmRMFyVIN1kmLrccrdtgO-YMH-WBqOHE4v2EbpnrLVoQxFAtwGANhDGuMgXpxDC3C8BThrw1YfKHHF0YVdPiCwxc6fMHiCw7fd6wYnhffL_1WzcKfYUf9XCrcaQoZ5FyHQa6mOopynZU8M6kMTBmX2tD6ORGR0CGxQPK4DGIVBoHUuKvlu2xQ4cu9ZxDyNNKJFvRXM45VnpvI8CwJVZLoRBixzz4TSJNWxhSLhgI9zUyummbS477P9uxzNJqXtVST7s7BX-98YNu99T-ywbJemUOiS2tI-ueTtdgf6EhAJQ

New Canadian cybersecurity era? (2018). *Mondaq Business Briefing* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV07T8MwELagLGxFvMozC2xBsZ049oAQFEpBSEhQ5sqOnYqBtDTtwL_nLo9GrYQEA4sV3SWRLnc5n63z9xHC2UXgr-QEIw0zTJk0ggmJBzYRgVZM0wTZ4WVBRNfri_sXefsUPzbEmY3sXx0PMnA9HqT9g_MXLwUBXEMIwAhBAOOvwgD7FxcIBN0vA9VexVgHKVCvtPXBD271Z9MMfwPr6LSe26qtAYpQ0355srNsDyofqtuDlrCmH557y8ISAxfWK1AzxEqeI_L4h31PZpcu899e18kG47GKSrjOBs0wQqqoVt1IWE3LgzZpY46e6Imbetel7VtkzWXb5BQUXm23t2S3B3Zf7ZBB727Q7fsVF4Q_EmCVTZ2iOlVWU0iInEmjoPLRLEiFs3EUJSqUNo24osoILS0PBcOzYFBv6YIXaZe0snHm9olHtaIsAU0gTOgSKzVHCB7JTYjIALRDztCcYUUCCkOO2yT5SM_zfNh8oQ7ZK-7DWJhNdTJcaA5-1BySzcZPR6Q1m87dMYKN5Uicc1J8228PRPv5

Office of the Privacy Commissioner of Canada. (2014). *Privacy and Cyber Security: Emphasizing privacy protection in cyber security activities,* from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/

Over half of Canadian firms reported cybersecurity incident last year. (2017). Hamilton: CNW Group Inc. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1NT8LXYekEcAAHiswo3LoWlKW1zQgzaTYAATaAdp7RNBAJa2Mdh_x67pEIaB5C4V-1T7djOS-wHIPzjjrcQEwKdF7HgCstlXysTYuKJVBai_UUQmQ61P6f9sDeIL2-iK3u5kFpjrLmbKFmH7qLKiTU_4ZKmiQnhy7P3D490pOi81YpqtMDB1CbQ851ucns_BFq6_yRrsJL86nCKiJg0UoqJjXNFwRiYTrjv0CtwcpQZ6wh5tdhSZcbkNyh07In9WpYZVgzlICZ5_HbhH2dHOiC5fMM60GraceIh6dGXoZop2yOgDbhKE0eLvpeA2uEfkLkvyp1NZuMvoGJLWiXVam3gXGpJS94LiOuAolbr1PcpRpa07hMozDcgcNfX7f7h2f2YNmndEg3QeQ-tKfjmT6gIVv1r3ahFafXLjjn3cdhz7UW-wSHVrBX

Parliamentary committee recommends substantial revisions to PIPEDA. (2018). *Mondaq Business Briefing* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV07T8MwELagLGwgXuUlL7CgoCTOc2BoaUuLkKggzNUltqsOTUuS_n98Tpq0SEgwsFjROQ_lu8v5kbv7CGH2vWl88wmMewL80Iq5awsBTsCdwLS554EPID1Mfx4Mvae3oPfiPzc0hI3sXxWvZEr1mEj7B-XXN1UCdaxMQLXKCFT7KzMYQ4b7KRghnumvfz4rCk3WoJ421_Gw6DuQS3hW1dnPdWxctLgbj8b9Xmdz-qo8AIfPJlq-qxbacj34VXsHlk6mK0lmy_ih8qJ1_NBWMerR62BbWBbJdZnOf3L8WyxNPuezpHgQqfH

xvkv2bOaHblnPsyl36CKXVGsdaViN29EBOUAnvoSlyGinBOeQ7Ij0iHS3gKE1MLQBhm4AQ2tgaLSgJTDHJBr0o8ehUfFJGFPP9A2wLSk9y-KhnjTGyvOwxAnBNEGCiZXoOJiJms64oXKC3AzVUirG5aQDgSO5x05IK12k4oxQP9a_L-NQAncAWAhOwhLpCo7gcNYmN_jGk4pIVDU5brXkU1jl-aQBsU1O9XloT0UGyaTuOf-x54LsN6q8JK0iW4krLFiWI_nOtYb_C6nHGBs

Personal Information Protection and Electronic Documents Act. (SC 2000). c 5. Retrieved from: http://canlii.ca/t/53h4m

Privacy dealt with in the open. (2007). *Winnipeg Free Press* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1NT8JAEJ0IXDyJ8QsV0j9QZdv9PBlQC1FjCMF4bNrdrcFDwYom_nt3SksMifHgqUl72c5038687b4HEAYXfX8LE6Qw3KZuNTJCExR5Y2kimQ20NSoNSxmDaMxHU3nzIO5-HOqv0l2jZAndZqGRNb8UDD1ZmepfLd98tJHC7dbKU6MBrQDPeTehNRg-PY82PZhia9rFNRo-GtP_jsS4vkR78FoPxVSOCa6oRZeTkgakNNxSb_zPoNvQRmRbJktbeIP1h7MPOzY_gN6kmH8m-ssz-FeYhxytN889VyN66LJ1CLPodnY99isDBf-Fua6Q2JBKxpV2ZZniMiNKmMT1c4ozlrl71CqRGTcBhUyoywqVxqJ8XGqNURnLwiNo5ovcnoBHQhEYbhhupFGqlbKBDSUnmnPDmWUdOMYwxjgrVkWiY8IDLN4C1YFuHYg4r9_uPd7E4fSP52ewu6ZTqU_4OTRXxYftoj5XmYUeNGR036uy7K7D28fJ9Buqordb

Rosenzweig, Paul. (2012). The international governance framework for cybersecurity. *Canada-States Law Journal, 37*(2), 405.

Shackelford, S. J., & Bohm, Z. (2016). Securing North American critical infrastructure: A comparative case study in cybersecurity regulation. *Canada-United States Law Journal, 40*(1), 61.

Shecter, B. (2018). *Market watchdogs eye new rules on how companies disclose 'material' risks like climate change, cyber attacks*. Toronto: Infomart, a division of Postmedia Network Inc. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1LS8NAEB5sexEPKio-y3iqBys2j016EqtNiy-kKD2WZnewpSGrTUvpv3dnTRDqQcFLDpuQHZjh29mZ-WYAXOfisr6CCWGgBMXmNFKBbHCTNz8ehj45klQzdm0bg6grOr3w9iG4y4sLmRqTq7tASQvdSkuOmvO1nfuFmRPs6v2jznOkON-aD9UoQcW8cI3lV1rtp-feD6i1cBhtwqTYSuUTEYzTylNMbJjP89yV7oz_EmoLNvoUYxGY34Y1SncgebT8ZlwY7B0p_ZYhLQmNU43TeUIZ6hRHeoG2Jj0112dkvm6iM8KacWqtndaQC9EzTMYTQpmMeR2_mMPnKJcxTXE4mzFpfxfOovbLTbdeSD8w5sQ5gmFKep4NvuV396Cc6pT2ARtu4CihfE6jeZ5sNskhNxQNKYQSPvkHcPrr7w7_8M0RrJtnaAtj_GMoz6ZzOuFeXFYjVSiF0X0VKtet136nmiv2E2yJvoc

Shein, M. M. (2017). Fraud, cybersecurity and banking in Canada. *Security*, *54*(9), 77. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwxV3PT8IwFH5BuHhCUSOCpCcPRhTbrhsHYgD5ETXGEAzxRLp2TYxkIJGD8e_x__S1bGLAePWyJdth2-vb977X9r0PgNHzWnUNE5gONMfIIDE70CHFoBwo30TMCIMOErqC777oDYLrO_8mAx9paUwy3ClKOujWU2VnzS8wWUHnY5zzq9lr1epI2fXWVFTju8psuR0EqajVJtnoVTufNGQiy6Abl7YmfwtymDX49g_xR0-r7SLC6erWAlt6HVCxgd0uIHXz8Jm--2-P5pyttXv8p6_cgSIGQx2RH7ODpLl01l3IRHEB8qmuBElgpgDlZc0wGUUTI-cROSHphen8ZQ9OkWwv9Blpv4fIXRP9PSJjTVrSCUGQ55i4rgtyH4bdzrDdryaSD9WZJzgGhMjjvjBI83Sdhkj865hxGeELT1NZ00Iyn1FPhZTWtappxhXST0WVYRwzS8YOIBtP4-gQSF0iuPieTcAoD4SS6KyWO0klAm2oKUIptfc4WZ4Zr2x99OfdEmxTG93dVrMyZN_mi-jY9gxz1q84x8Fj0L2tQK7Zehz18Nzq3D8MvgAEL-zJ

Siegel, A., Denny, W., Poff, K. W., Larose, C., Hale, R., & Hintze, M. (2009). Survey of Privacy Law Developments in 2009: United States, Canada, and the European Union, The Business Lawyer, 65(1), 285-307. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwxV1NT9wwEB3xcemlLVDUpRT5gnohbdZJbAcJVUvLggqqEC1CnCLHdhBSlaUJS0V_T38oM46zaqHiysVREkuJNePnNx7PDEDC38fRPUyojFCpHVaxKqWVIkPSj_cy0ciAh1lJDt7xgdg_UZ-P5Jc5-N2HxgRx9yjpodtODO2af-Cc1k4khx-vfkZURorcrX1NjVmQWXcaBJkolSZ5kKq2-bGjQ1UGuzOkkPx5WESjQdIEkWfnM1BHGA9F2WQkFGWKDQjenWJ8gOQehccv4E8_kv_9SZom95I_Ps2YX8LzQH_ZqNPXJZhz9TLMH-lfK3D-bdrcuFs2qdhxc3mjzS3D5-yvU00tu6wZ-Vm2WUeVWUeVt5jPsaC3mK4tQ0bLeh8D9ZvUr-B0vPf900EUCj9EF7SSRpnJpBVGO505tNdijTYadwItS15aqWNeoklfIjJya2xeVcbk2giT5EZzwZVLVmGhntTuNbDYakSlWKCqVmkam7xC_iaEQ8PNqUryAWySHItQ8hObljZF2gs9bdtihIQIDVSl1ADe-X407a8bbXSIXsCvUAKtf3quepUorrp0IUVKdX0ylQ9grZdpERxCxUyea4-9fAPPvBPLh0Cuw8J1M3VvKUeZF_CG11Rs1fhwAxZHu6dn-3jd3ft6fHIHn7QSaQ

Sirivar, J., & Wolch, S. (2017). A look at Canadian privacy and anti-spam laws. *Defense Counsel Journal, 84*(4), 1-23. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1JT8JAFH4RuHhxX1AkczGeqtN9OJmiVKLEEJQQT820nRJiLEiLxn_vmzIEIcaLl2mambSTWb73ZnnfB2Aal1Rbw4QkcpgV6wlloRu7jo1OP767JkcPWLdDecDrt527HrvtuPfqcqEMjVHdvUDJArrjcSR3za_0OXmaSdn15F2TOlLyvFWJapSgUvAJlaHiNfuDuyU6m2zO_ikjk6mUOf8digv49LfhdVGVWCkmoFMrVU6KbUDLMtfYG_9V6R3YUm4o8ebjZhc2RLoHpQ7_3AfNIx30vAnPyYK6gHSnow8efRGexsRL85H2NOFvBItnB9D3W883bU2JKmhD3cAVI5pvjvhGuU

CrZDVEGDZCPWZmKJhj88g1bVfYHBdJtkGTmCVY04jhu5DE7YbBzUMop-NUHAOhMccZTx0cBoll0aiRoG_kOAIXRYIlrlGFc9m0gZLTxCSTGw7ZkM-yLPBkyKzN0IBW4agoJ6dUPuVR8CPnYiWHq5gB_L-krVr5Rm3R3oGahVmwbOyTv7NPYdOQ5rq4pFeDcj6diTNJAlZ0dR1K7uAFU-Y_1NV4wmez9djtfQN589iW

Statistics Canada. Impact of cybercrime on Canadian business. (2017). Retrieved from https://www150.statcan.gc.ca/n1/en/daily-quotidien/181015/dq181015a-eng.pdf?st=A8sTXxGy

Stacey, R. D. (2011). *Libicki, martin C.: Conquest in cyberspace: National security and information warfare* American Library Association CHOICE.

Russell Thomas. (2017). Rebooting cybersecurity. *Ivey Business Journal (Online)*, Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2AwNtIz0ErE1JSjZOMLcwsTIEVmklSokFamlGyYZqhQUpqSrKFAXirlZuHmXuQhYuPuRd0cSFoaww0umGlJLjoTslPBo2a6wObHsBOOLCwtbAvKNQF3SMFmm-FXqrBzMBqBNpEysLA6ugUGu4O74RZmJtbYpS74MrETYAhG2ZvCvR6BGALFnSlCXjMz8TEGO2oRopcKMjAD21zKjhCEokQA1NqngiDeBBonhS06FnBuTIJ2AiEXmQnyqDk5hri7KELsyseOq0Qj7DHWIyBJS8_L1WCQcEgzSjVzNTcPA0Y3iagit_CMsUgKTU12cg41TI1zVSSQRqPQVJ4ZaUZuIxA1Rt44Z8MA0tJUWmqLOjQLHBoyTEwm4HAkkLN285aPgDaSdXv4AgAIp2nxQ

Zimmerman, K. (2018). Survey: Cybersecurity leading corporate board directors' concerns. *Westchester County Business Journal, 54*(18), 28. Retrieved from

https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2039835622?accountid=11999