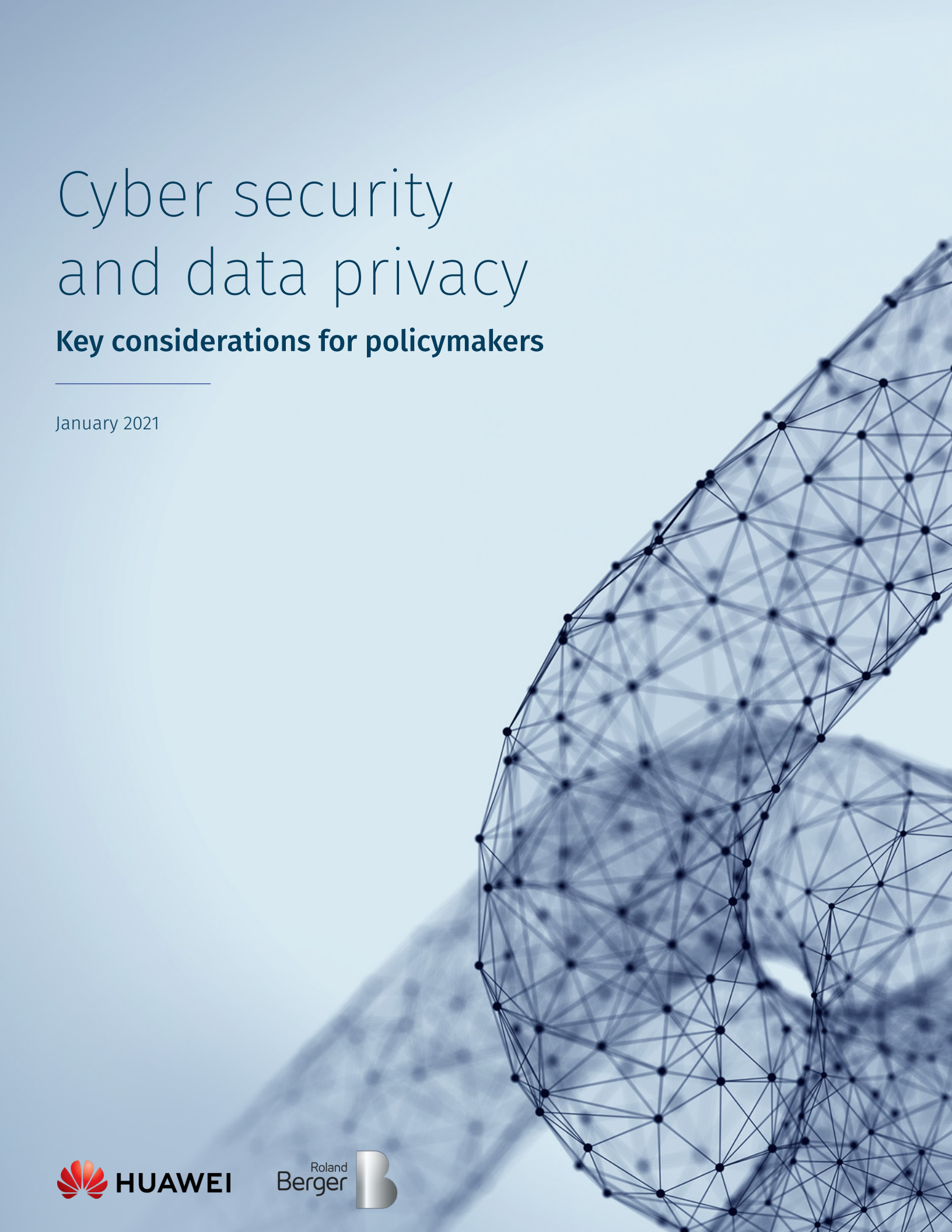
Cyber security and data privacy

Key considerations for policymakers

January 2021



HUAWEI

Roland Berger

TABLE OF CONTENT

EXECUTIVE SUMMARY

With the emergence of digital infrastructure, numerous economic and social transactions are increasingly being digitized. Online banking, social networking, smart grids and industrial networks are examples of activities now relying heavily on digital data. The amount and speed at which digital data is generated and stored keeps increasing exponentially. While most data are trivial, a significant amount will contain sensitive information or personal identifiable information (PII) and needs to be protected. This requires clear physical and digital cyber security defences to ensure data remain private.

From a cyber security perspective, threats will come from both external and internal actors whose capabilities are rapidly improving. As organizations adopt digital transactions, they will embark on a digital journey to transform their business model. In many cases, they don't have the experts in-house to protect customer and transaction data. Canadians have never been so affected by cyber criminality as the reported rates of cyber crimes, including fraud and identity theft, are increasing dramatically. Critical infrastructure such as water supply and electricity are also facing increasing risk.

From the data privacy point of view, the increased digitalization of business and social transactions is creating new opportunities for cyber criminals to breach the data integrity of organizations, allowing them to exploit personal or critical information for fraud, espionage and sabotage. Although data privacy regulations must be modernized to adapt with new technologies, they must not hinder digital innovation or block the implementation of those new technologies. This dichotomy between digital innovation and data protection thus fuels the debate around the required amount of regulation in the cyber space.

COVID and trends such as the never-ending search for ease of transactions will continue to drive the uptake of digital technology in consumers' everyday transactions and institutions' business operations. This, in turn, will increase the economy's exposure to potential cyber crimes. In fact, the total worldwide cost of cyber criminality is currently estimated to be 525 billion USD, representing about 0.7% of the world's GDP, and is expected to grow if appropriate measures are not taken. This ratio is higher in developed regions and is indicative of the need for countries such as Canada to take forceful actions on this issue.

The policymakers cannot overlook the importance of their role in providing a safe digital environment to preserve confidence in new technologies and support the growth of the digital economy. Most industries are benefiting from the efficiency gains arising from digitalization, and thus, safeguarding businesses' and individuals' data is essential to developing a competitive economy.

Cyber security and data privacy are complex by nature. However, by increasing its efforts in the resolution of the following seven key challenges, the policymakers would address most significant issues related to cyber security and data privacy and provide better conditions to grow the digital economy:

CYBERSECURITY

1. Improving the general public's digital literacy
2. Supporting small institutions in their digital transformation
3. Securing critical infrastructure and governmental networks
4. Keeping up with a changing technological environment
5. Strengthening policing efforts against cyber criminality

DATA PRIVACY

6. Balancing of data privacy and digital economy growth
7. Navigating the complexity of the international legislative landscape

CYBER SECURITY ECOSYSTEM

As most components of modern society now rely heavily on online services, individuals and institutions alike become more exposed to the risks of cyber criminality. As such, the amount of data generated and stored online every year increases exponentially and represents an ever-growing opportunity for cyber criminals. Reliance on online services such as social networks, e-commerce platforms and digital banking radically increases the number of potential entry points into IT systems and thus enables increases in data theft, fraud and extortion.

Canada, along with the United States, is among the most targeted countries in the world when it comes to online record theft. The cost of cyber crimes in North America represents 0.8% of the GDP, higher relative to the world average of 0.7% (Gemalto, 2018). Large potential financial gains, combined with a low success rate of law enforcement in identifying and prosecuting cyber criminals, are fuelling the worldwide increase in cyber criminal activities.

Although governments have taken actions to improve Canada's general cyber security, the situation requires constant attention. Large and highly publicized data breaches, such as those at Capital One and Desjardins, are frequently occurring. Furthermore, numerous cyber attacks on small businesses, large institutions and critical infrastructure providers often remain undetected, unreported or unpublicized.

Securing digital infrastructure is thus of the utmost importance to provide confidence and drive adoption. It is a crucial pillar to support the growth of Canada's digital economy. As most industries benefit from the efficiency gains stemming from digital transactions, safeguarding businesses' and individuals' data is essential to ensure Canada's future competitiveness.

Cyber security needs to be addressed on multiple fronts. To mitigate the impact of future cyber criminality, we believe that Canadian policymakers should focus on five main challenges:

1. Improving the general public's digital literacy;
2. Supporting small institutions in their digital transformation;
3. Securing critical infrastructure and governmental networks;
4. Keeping up with a changing technological environment;
5. Strengthening policing efforts against cyber criminality.

By upping its game on these five challenges, policymakers will address most key issues in the cyber security environment and provide better conditions to support the growth of the digital economy. These challenges were established based on the current state of cyber criminality and Canada's policy landscape supporting cyber security efforts.

2.1 PORTRAIT OF CYBER CRIMINALITY

The typical cyber attack has evolved over time. Understanding the present state of cyber criminality by identifying the actors behind attacks as well as their motives, tactics and targets is required to put into context the threats currently faced by Canada.

2.1.1 Actors

Cyber attacks on organizations generally come from external actors (see figure 2.1). However, breaches originating from internal actors, such as employees and business partners, are disproportionally frequent in North America when compared with the rest of the world. They represent approximately 30% of reported data breaches in the United States and Canada compared to only 16% in the rest of the world (Verizon, 2020).

Internal actors sometimes have nefarious intentions, but there are also many circumstances in which internal actors are unaware of the repercussions of their actions due to a lack of training and general digital literacy. Regularly, employees

fall for simple phishing scams and inadvertently share information with the wrong people. The higher level of data breach occurrences in Canada due to internal actors is indicative of poor digital hygiene practices by employees handling or having access to sensitive information.

On the other hand, external actors are increasingly sophisticated and are often backed by criminal organizations or states. Organized crime and nation states represent respectively roughly 70% and 10% of reported external actors, although this distinction is sometimes difficult to establish due to the cooperation of state and non-state actors. The remaining 20% consists predominantly of unaffiliated actors whose motivations often remain unclear (Verizon, 2020).

Figure 2.1 – Description of key threat actors

	Actors	Description	Illustrative objective
External actors	**Cyberterrorists**	**Extremist groups** using cyber techniques to intimidate an audience, force a political change or cause fear or physical harm	› Disrupt critical infrastructure › Modify or delete intelligence records of known terrorists
	State-sponsored actors	**Highly sophisticated groups** receiving guidance, funding or technical assistance from nation states	› Build profiles of targets for espionage campaigns › Use information as leverage to gain other types of intelligence
	Cybercriminals	**Malicious individuals or organized groups** accessing personal, financial or health data to monetize it	› Conduct identity theft, tax, or medical fraud › Use credentials and harvest contact lists for phishing attacks
	Hacktivists	**Organized groups** seeking to bring awareness to a cause or to exercise free speech	› Publicize a breach to highlight vulnerabilities in a particular organization › Gather personal information of a specific target
	Thrill-seekers	**Cynical opportunistic individuals** accessing protected systems for the challenge it represents	› Claim ownership of a successful cyber attack › Gain credibility among the cyber community
Internal actors	**Insider threats**	**Individuals already operating within organizations** perpetrating a cyber attack, sometimes unintentionally (e.g., disgruntled employees, partners and untrained workforce)	› Sell confidential client data or intellectual property to outside buyers › Disclose private company executives messages

Source: Canadian Centre for Cyber Security, RAND Corporation, desk research, Roland Berger

2.1.2 Motives

Financial gain is the main motive behind the vast majority of cyber attacks on individuals and institutions alike. For businesses, around 90% of data breaches are motivated by direct financial gain. The rest is mostly linked to industrial espionage targeting highly technical sectors (Verizon, 2020). Other marginal motivations may include activism, personal satisfaction, and notoriety.

For individuals, phishing or hacking of personal credentials is usually performed with the aim of financial gain. Other motives for stealing an individual's credentials include attempts to damage reputation and gain notoriety on social media during state-sponsored election meddling attacks.

2.1.3 Tactics

The most common tactics used by cyber criminals can be categorized into four major groups: hacking, social engineering, exploitation of user errors and malware.

- **Hacking** often refers to brute force attacks, during which cyber criminals attempt to find password combinations or hidden web pages by trial and error. Hacking also refers to the simple usage of stolen credentials obtained on Dark Web marketplaces or other cyber attack tactics. About 80% of hacking attacks use either brute force or stolen credentials, while the rest uses vulnerability with various levels of sophistication (Verizon, 2020).
- **Social engineering** tactics mostly refer to phishing campaigns during which cyber criminals send mass e-mails or text messages, pretending to be a legitimate institution and asking for credentials or other sensitive information. For example, during the COVID-19 lockdown, cyber criminals have impersonated the Canadian Revenue Agency and lured people into divulging personal and banking information to obtain Canadian Emergency Response Benefit (CERB) payments.
- **Exploitation of user errors** relies on the misconfiguration of cloud-based storage and other tools accessible by the public, or on the misdelivery of sensitive information, usually through e-mails sent to the wrong recipients.
- **Malware** exists in many forms but generally consists of programs inadvertently installed on users' devices, often through malicious e-mail attachments or links. Unnoticeable programs designed to capture and transmit passwords or other sensitive information are the most prevalent forms of malware. Ransomware is another common type of malware. It threatens to publish or destroy data unless a ransom is paid. Ransomware has flourished with the rise of cryptocurrencies as they allow for untraceable payment methods and facilitate the laundering of cyber criminality profits.

User error exploitation and social engineering tactics are becoming the most prevalent tactics, slowly replacing malware. This change is driven by the growing number of unsuspecting end users caused by the wider adoption of digital technologies. Additionally, improvements of cyber security standards have rendered ineffective many older and simpler malware codes.

2.1.4 Targets

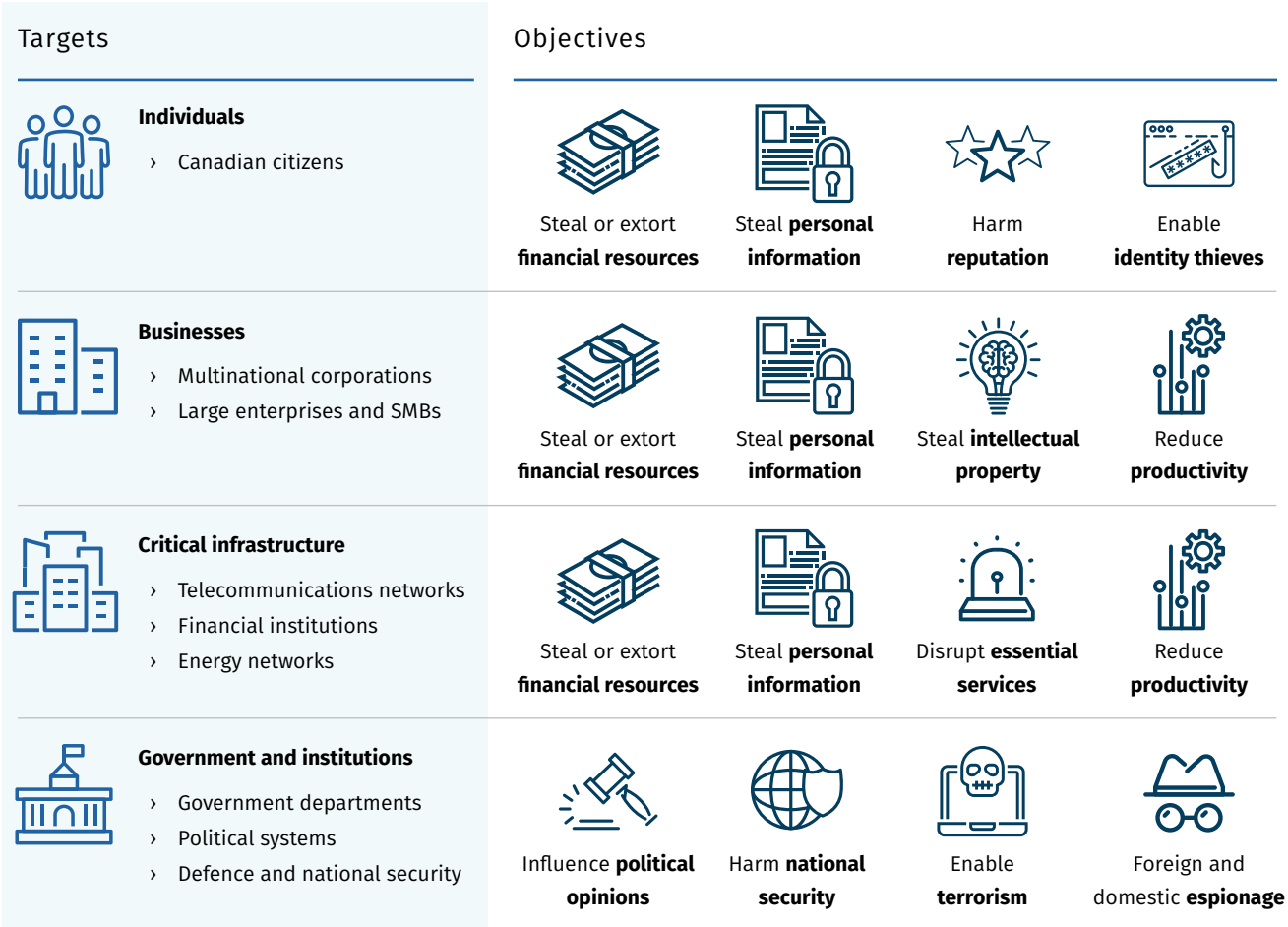
Cyber criminality targets all participants of the digital society, from individuals and businesses all the way to critical infrastructure and governmental networks.

- **Canadian individuals** are increasingly targeted by cyber criminals. Reported cyber crimes have grown at more than 20% per year since 2014 (Statistic Canada, 2019). The vast number of records stolen in recent years makes it quite simple for cyber criminals to amass enough personal data points on individuals to commit fraud or identity theft. Poor user knowledge surrounding cyber security also allows criminals to use unsophisticated social engineering tactics and user error to obtain credentials and other sensitive information.
- For **Canadian businesses**, the average cost of a breach is estimated to be around 6 million CAD, about 15% higher than the global average of 5.3 million CAD (IBM Security / Ponemon Institute, 2019). The average cost per stolen record is higher in Canada, despite a lower number of stolen records per breach. It is important to note that although companies of all sizes are affected by cyber crimes, smaller businesses are often more vulnerable given their lack of resources dedicated to cyber security.

› The digitalization effort of many **critical infrastructure** providers[1] to gain efficiency and additional capabilities is opening the door to cyber attacks. Attacks are often conducted by either confirmed or suspected state-sponsored actors, compounding the threat of coordinated cyber warfare. Compared to other countries, Canada's critical infrastructure has not been the most successfully targeted. Nevertheless, its healthcare industry has been put to test in recent years, suffering multiple ransomware attacks and security breaches. The total number of attacks on critical infrastructure remains unknown. Failed attacks are only disclosed to the relevant authorities as public disclosure would be counterproductive.

› **Governmental networks** are a prime target for data theft. They often store large amounts of high-quality data and, as their operations are often essential and backed by public funds, they can be particularly attractive for ransomware. Governmental institutions in Canada have taken important steps in recent years to protect their networks, but the rapid evolution of cyber threats requires constant and demanding updates of security measures. Smaller public institutions, such as mid-size and rural municipalities, become especially vulnerable due to their lack of resources in cyber security.

Figure 2.2 – Overview of targets and typical objectives



Source: Roland Berger

1. Critical infrastructure providers include utilities, telecommunication, finance, healthcare, water, food, transportation, public safety and essential manufacturing.

2.2 OVERVIEW OF CANADA'S CYBER SECURITY POLICY LANDSCAPE

Cyber security mostly falls under federal jurisdiction due to its national and often international nature. Provinces operating their own police service – Ontario, Quebec and Newfoundland and Labrador – are responsible for the law enforcement of cyber crime legislation, as long as the case does not cross provincial or national borders. Considering cyber attacks spread easily across provincial and international boarders, it is easy to understand why investigations of any larger cyber crime most of the time fall under the responsibilities of the RCMP.

In Canada, cyber security is regulated and governed by a complex framework of federal departments and agencies. As seen in figure 2.3, three different departments (Public Safety Canada, Treasury Board and National Defence) oversee agencies responsible for the fight against cyber crime.

Figure 2.3 – Current federal separation of cyber security responsibilities

Public Safety Canada

- Formulates and supports the implementation of the national cyber security strategy
- Coordinates cyber security efforts with national and international stakeholders

Royal Canadian Mounted Police

- Investigates and prosecutes cyber crimes on the national level
- Coordinates with international law enforcement partners

Treasury Board

- Oversees the government-wide development and implementation of proper cyber security measures

Shared Services Canada

- Consolidates and manages most IT infrastructure of the federal government's departments

National Defence

- Supports research and development efforts of the public and private sectors in the cyber protection of critical infrastructure

Canadian Security Establishment

- Operates the CCCS

Canadian Security Intelligence Service

- Assesses national and international cyber threats

Canadian Centre for Cyber Security (CCCS)

- Unites most federal expertise in cyber security under a single organization
- Prevents, identifies and mitigates the impact of cyber security attacks on governmental networks, critical infrastructures, businesses and citizens
- Supports the RCMP in the operation of the National Cybercrime Cooperation Unit (NC3)

The structure above does not include entities active in data privacy, such as the Office of the Privacy Commissioner. Details of the data privacy framework at the federal level are presented in section 3.

Overview of the cyber security strategy

The current strategy and action plan of the federal government, released respectively in 2018 and 2019, are articulated around three main axes: the security and resilience of Canadian networks, the support of cyber innovation, and the leadership role of the federal government.

- The first axis focuses mainly on the protection of the federal government's networks and those of critical infrastructure providers, namely in the financial and energy sectors. The government aims to improve its detection and intelligence gathering capabilities and to increase collaboration with critical infrastructure providers. RCMP capabilities was also enhanced with additional resources and by creating the National Cybercrime Cooperation Unit (NC3) in collaboration with the Canadian Centre for Cyber Security (CCCS).
- To support cyber innovation, the federal government focuses on the development of the necessary workforce in cyber security (through a financed work placement program), and on the support of SMBs' security measures (by implementing a new certification program dedicated to SMBs). Canada also supports research efforts, both in public institutions and in the private sector, through funding provided by the new Cyber Security Cooperation Program and through conventional research funding organisations such as the National Research Council (NRC) and the Natural Sciences and Engineering Research Council (NSERC) under the Innovation, Science and Economic Development (ISED).
- Lastly, the action plan aims to improve Canada's leadership position on the national and international stage.
  - At the national level, the government unified its expertise into one organization in 2018 through the creation of the Canadian Centre for Cyber Security (CCCS). The CCCS coordinates all efforts in cyber security. It monitors Canadian and international networks for cyber criminality, informs public institutions, companies and citizens on cyber threats, and provides recommendations to stakeholders of the digital economy. CCCS is the authority on technical matters and the point of contact for all agencies and partners to coordinate incident response.
  - On the international stage, Canada aims to cooperate specifically with the United States by establishing a global framework for the fight against cyber crime. Canada also intends to increase collaboration with them when setting up cyber security defences, especially for common critical infrastructure (for example in the energy sector).

The current Canadian strategy addresses many issues of cyber security, but several challenges remain. The following five key challenges have been identified through the analysis of the Canadian cyber security landscape. Properly addressing these challenges would allow better protection of Canada's digital environment.

2.3 CHALLENGE 1 – IMPROVING THE PUBLIC'S DIGITAL LITERACY IN CYBER SECURITY

2.3.1 Context

Cyber criminals are increasingly relying on the lack of cyber security knowledge of the general public to perpetrate their attacks. When trying to infiltrate a company network, they often only require a single-entry point, potentially offered by an employee falling for a phishing scam or inadvertently downloading malware. In recent years, cyber criminals have mastered the exploitation of these soft targets. As discussed in section 2.1, about 30% of cyber security breaches of North American companies originate from internal actors. These breaches are most often unintentional and are made possible by the lack of digital literacy in cyber security. In fact, poor digital literacy is a major cause of the ever-increasing level of fraud, extortion and identity theft committed against private citizens.

2.3.2 Key considerations for future policy

The lack of knowledge regarding cyber security issues and best practices among the public should be tackled along two different axes: awareness campaigns and training.

Far-reaching media campaigns should aim to inform the public of cyber security best practices. The effectiveness of these campaigns should be measured and monitored to ensure they are impactful. Since 2011, the CCCS operates the GetCyberSafe campaign, which communicates advice and information on recent cyber threats affecting Canadians. It could be expanded to truly improve the cyber security hygiene of larger portions of the population. For example, the existing Cyber Security Awareness Month is an opportunity that brings cyber security to the forefront through major awareness campaigns and media presence of cyber security experts. This initiative should be further expanded to reach more people and expand literacy. Teaming up with private sector associations (e.g. financial sector) to expose the consequences of negligent cyber security behaviours and highlight best practices would help in reach and effectiveness.

On another note, training regarding employee handling of sensitive information should be supported in both the public and private sectors. In the public sector, this training should go beyond the federal government and target smaller institutions, such as municipal governments and health agencies. In the private sector, tools should be offered to employers, especially SMBs, to enable them to improve the cyber security knowledge of their workforce. The CCCS, who already possesses the necessary expertise and provides high-level advice to public and private institutions, is an ideal candidate to lead these initiatives.

Various associations already support efforts in cyber security literacy. For example, the Anti Phishing Working Group (APWG), an international industry association of large ICT companies and cyber security service providers, already supports the Cyber Security Awareness Month and could be involved in larger campaigns. The APWG includes companies involved in online payment services, such as Interac and PayPal, and in e-commerce, such as Amazon, that would greatly benefit from improved online cyber security behaviours.

THE CASE OF THE UNITED KINGDOM
SUPPORTING EMPLOYEE TRAINING THROUGH A COURSE CERTIFICATION PROGRAM AND BASIC FREE TRAINING

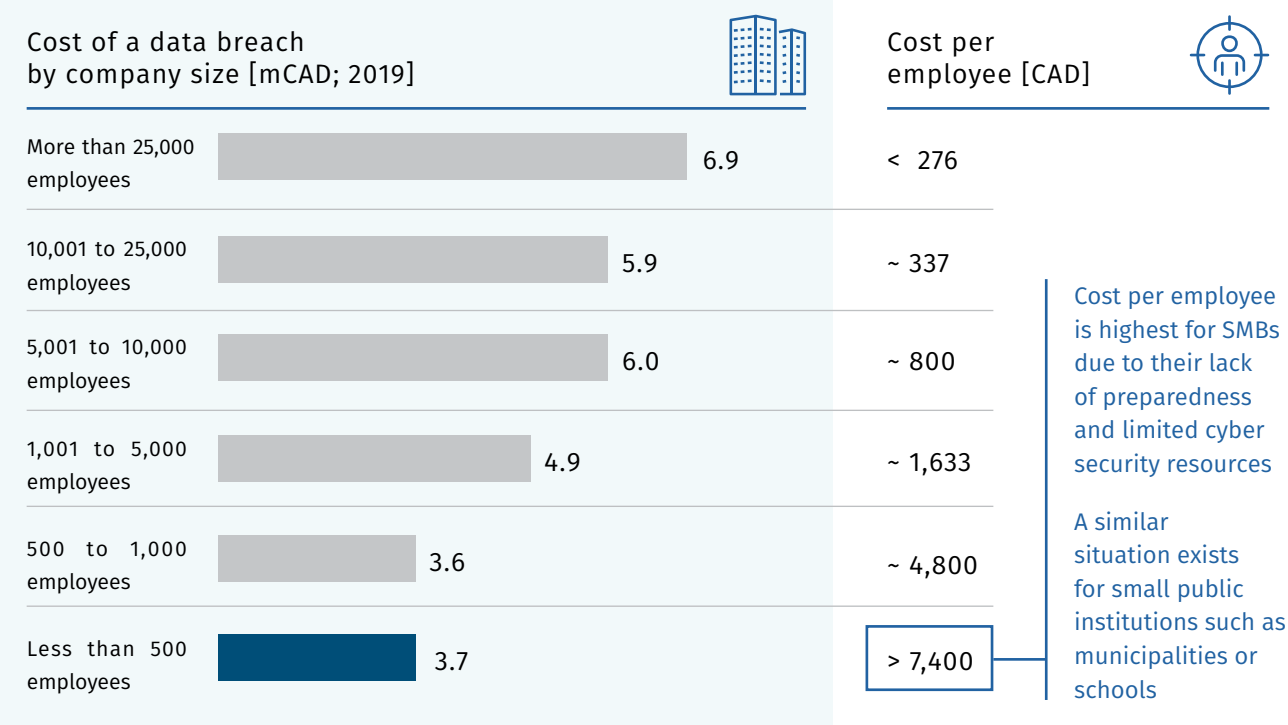
The United Kingdom has identified the lack of cyber threat awareness as a major deficiency of its national cyber security. Thus, to improve cyber security in the private sector, the National Cyber Security Centre (NCSC), the UK's equivalent of the CCCS, supports employee training. The NCSC provides a training certification program that allows companies to easily identify quality training services. It developed rigorous standards against which courses are assessed. Certified training programs are compiled on the NCSC website as an easy reference for cyber security managers seeking to improve awareness and knowledge of their workforce. Additionally, the NCSC also provides a free training program designed for SMBs to educate employees on the risks of cyber attacks and on the basic measures to defend against most common tactics.

2.4 CHALLENGE 2 – SUPPORTING SMALL INSTITUTIONS IN THEIR DIGITAL TRANSFORMATION

2.4.1 Context

Although cyber attacks affect businesses and public institutions of all sizes, their impact is particularly significant for SMBs and smaller public administrations such as schools and municipalities. In fact, the cost of data breaches, presented in figure 2.3, is largest for smaller businesses when considering it on a per-employee basis. This stems from the fact that SMBs have limited resources to dedicate to cyber security and often lack the necessary preparation and skills to fight cyber attacks. This problem is of particular concern for the Canadian economy where a majority of the private sector consists of SMBs, with 55% of Canadian employees working in companies of fewer than 500 employees (Statistics Canada, 2019).

Figure 2.4 – Average cost of a data breach by company size [mCAD; 2019]



Source: IBM Security / Ponemon Institute, Roland Berger

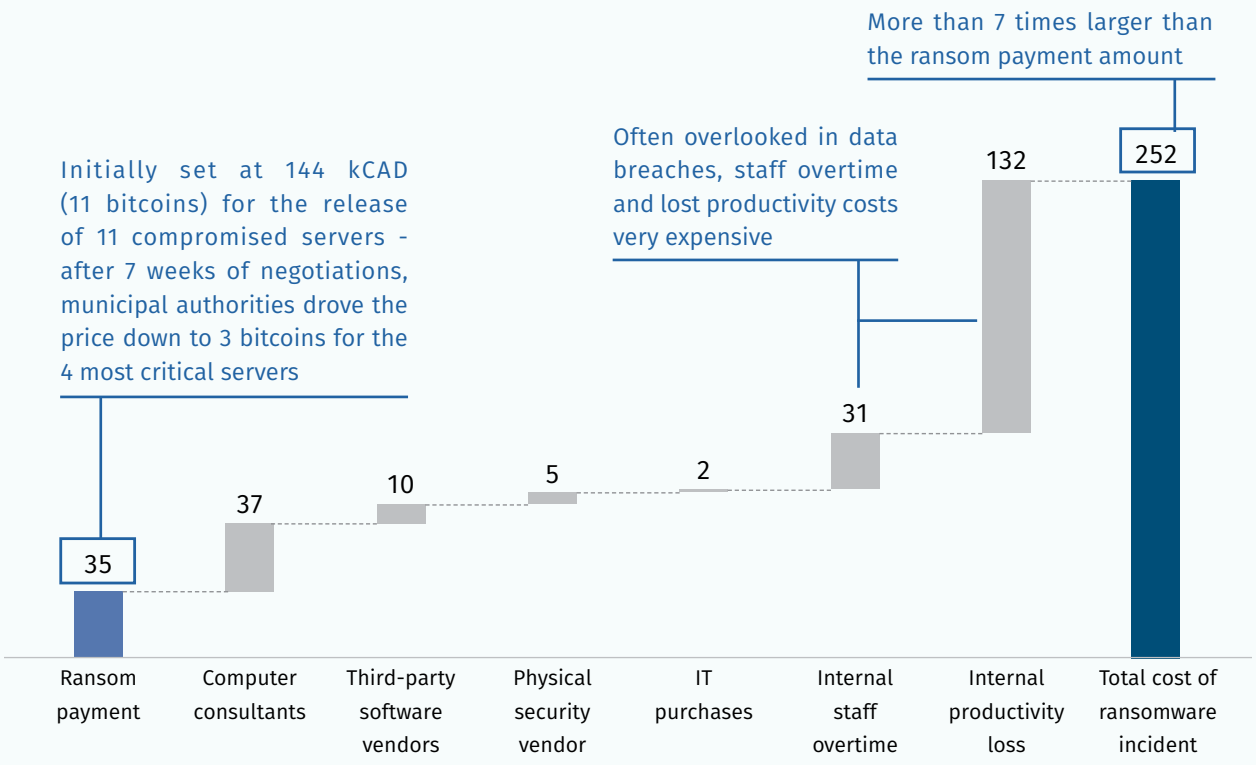
A similar situation exists for small public institutions as they generally have limited capacities in cyber security. In Canada, multiple cases of municipalities falling victim to ransomware or phishing have been exposed in the media. In 2019, Woodstock (ON), Stratford (ON), Ottawa (ON) and Saskatoon (SK) were victims of such incidents. Many more attacks on municipalities are likely to go unreported or undetected given there is no law mandating the reporting of ransomware or phishing incidents, with only data breaches requiring reporting.

SMBs or small public institutions often feel they are not a potential target for cyber criminals, another factor explaining their lack of precautionary measures. The media often only focuses on large data leaks affecting the general public. This reinforces the perception that smaller organizations are not affected, which is unfortunately untrue.

AGGREGATE COSTS OF CYBER ATTACKS

The total cost of cyber attacks for small institutions often grows far larger than the sole direct cost of a ransom or phishing payment. Figure 2.4 presents a breakdown of the total cost of a ransomware incident for Wasaga Beach, a small town in rural Ontario, and shows how the total cost became seven times larger than the ransom payment.

Figure 2.5 – Total cost breakdown for the 2018 ransomware incident in Wasaga Beach, Ontario [kCAD]



Source: Canadian Centre for Cyber Security Research, Roland Berger

2.4.2 Key considerations for future policy

The Government of Canada's current answer to the issue of cyber attacks on small institutions is the creation of an assessment and certification program dedicated for SMBs. The CyberSecure Canada certification program was created by Innovation, Science and Economic Development Canada (ISED) in collaboration with existing certification agencies. Although this program helps managers of SMBs orient the development of their IT infrastructure towards cyber security, it offers little direct support. Canada should take inspiration from the Cyber Security Small Business Program of Australia.

CASE OF AUSTRALIA
SUPPORTING THE COST OF CYBER HEALTH CHECKS FOR SMBS

Due to the vulnerability of SMBs to cyber attacks, the government of Australia has instituted a financing program to support cyber security health checks. This encourages business owners to learn about their vulnerabilities and to get expert advice on how to remedy them. The program reimburses a portion of the cost of cyber health checks done by security providers certified by the Council of Registered Ethical Security Testers.

Governments should also encourage and support the migration of small institutions, public or private, towards managed and secure cloud services. In recent years, cloud services have allowed SMBs to expand their digital capabilities and easily gain effective cyber security defences. In fact, cloud services are generally operated by large companies with far superior cyber security expertise than most small institutions. By migrating to managed cloud services, SMBs and smaller public institutions can benefit from this expertise without building a strong internal cyber security team.

Canadian small businesses are already voicing their willingness to be accompanied through implementation of new cyber security measures, as seen by the 2019 advocacy campaign launched by the Canadian Advanced Technology Alliance (CATA), whose members are mostly comprised of SMBs.

2.5 CHALLENGE 3 – SECURING CRITICAL INFRASTRUCTURE AND GOVERNMENTAL NETWORKS

2.5.1 Context

Critical infrastructure providers are increasingly adopting digital technologies to improve real-time operational monitoring, better capacity management and enhanced decision-making. This quest for increased efficiency and additional capabilities is opening the door to more cyber attacks. Connecting industrial control systems (ICS) to the Internet allows operators to better monitor and control their physical infrastructure from any location at any time. However, it gives cyber criminals the opportunity to significantly harm the infrastructure in case of a security breach. Built for longevity, these systems often run on legacy software that may be particularly vulnerable to cyber attacks.

In recent years, multiple international examples proved the efficacy of attacks on connected CI and the risk they represent to national security. For example, coordinated power disruption in Ukraine left 225,000 citizens without electricity and crippled the network operator capabilities to fix the situation. Canada has managed to avoid such situations but has not been exempt from smaller but still damaging incidents. Multiple hospitals and healthcare networks across the country have been affected by infamous ransomware such as WannaCry and Ryuk. The rise in use of digital records in the healthcare industry has increased its efficiency but rendered its day-to-day operations vulnerable to cyber attacks.

2.5.2 Key considerations for future policy

Protection of critical information infrastructure (CII) is one of the key elements in the current cyber security strategy and action plan. The federal government aims to provide cyber security assessments of CII networks as well as help operators address vulnerabilities and keep them informed of potential threats. Also, as industrial control systems (ICS) play a major role in the vulnerability of critical infrastructure, Public Safety Canada organizes ICS symposiums and offers technical training on the subject. Furthermore, in an effort to improve cyber security of CII networks, the current federal government plan is to conduct cyber-based exercises to test CII operators' capacity to respond and recover from attacks.

The federal government should also adopt a more comprehensive set of critical infrastructure cyber security regulations that includes proper guidelines to update and enforce them, holding CII providers accountable for the digital safety of their infrastructure. Such regulations should be technology-neutral and built on a risk-based approach rather than on prescriptive measures. This would allow them to evolve with the inevitably changing technology. These regulations should also not hinder any collaboration efforts.

In addition, Canada should enhance its international collaborative protection efforts, as its infrastructure can be used as an entry door to access other country infrastructures, notably the US. Demonstrating that Canada is vigilant regarding cyber security matters is critical to maintaining and building trust with economic partners.

IMPORTANCE OF TELECOMMUNICATION NETWORKS

With the growth of the digital economy, our society becomes increasingly dependant on the reliability of telecommunication networks. Through the COVID-19 crisis, telcos have been vital to maintaining some level of business continuation. This dependence will continue to grow with time along with the need to ensure that telecommunication networks are adequately protected.

Currently, limited regulation exists concerning the resilience of telecommunication networks to cyber attacks. Telcos have a vested interest in creating a highly reliable network, which promotes higher security for their critical infrastructure. Policymakers nevertheless remain relevant in their capacity to prescribe cyber security measures and to ensure that Canada's networks do not fall behind on key cyber security technology.

CASE OF SOUTH KOREA
IMPOSING THE APPLICATION OF A NATIONAL CYBER SECURITY STANDARDS TO CRITICAL INFRASTRUCTURE NETWORKS

South Korea has developed its own cyber security standards, K-ISMS, and made its application mandatory for governmental institutions and multiple private or public sector companies such as telecommunication networks, internet service providers, hospitals and educational institutions. K-ISMS is a development of the international information security management system standard ISO 27001, similarly to Canada's own ITSG-33. However, Canada's standard was developed solely for federal governmental departments and agencies.

2.6 CHALLENGE 4 – KEEPING UP WITH A CHANGING TECHNOLOGICAL ENVIRONMENT

2.6.1 Context

New technologies, such as AI, quantum computing, blockchain, 5G and IoT, present opportunities and threats to cyber security. Despite not being primarily focused on security, except for blockchain, they all have important cyber security implications and may bring new tools to both cyber criminals and security experts.

- **AI –** The power of AI is widely recognized across multiple fields but remains marginally used in cyber security up to now. For cyber criminals, AI could improve current attack techniques. Sifting through large amounts of data or scanning networks to identify vulnerabilities to prepare subsequent attacks are potential use cases. Social engineering or hacking techniques can also be improved by AI tools that can mimic human behavior, making these tactics harder to detect. On the other hand, AI may improve the effectiveness of antivirus and cyberthreat intelligence systems. It may also help understaffed cyber security teams to improve their incident response capabilities.
- **Quantum computing –** Quantum computing's ability to break most current encryption methods remains theoretical but is, according to most experts, inevitable whenever it becomes a reality. To ensure that protection measures remain efficient, it is essential to implement new encryption techniques that won't be vulnerable to upcoming quantum computers.
- **Blockchain –** Blockchain technology has been developed as a novel way to keep ledger databases secure, allowing for decentralized and temper-resistant ledgers that ensure the exact tracking of transactions. Besides cryptocurrencies, blockchain currently has limited but promising applications in various fields such as logistics, financial services or healthcare. Harnessing the full potential of this technology would help secure many online services and networks.

  However, its application does not guarantee protection. Networks backed by blockchain have vulnerabilities, especially at the interface between end users and the blockchain system itself. For example, the Bitcoin cryptocurrency ledger has never been significantly compromised since its inception but exchanges, where end users interact with the blockchain, have been attacked successfully multiple times.
- **5G –** 5G networks are destined to become the backbone of future digital infrastructure, making cyber security highly important to society. 5G builds on high-performance 4G networks which will exist in networks for years to come. 5G enhances existing 4G networks, enabling multiple new applications generating massive amounts of data.

  The evolution of 4G networks to 5G coincides with a network architecture shift towards software-based virtualized networks with the potential for higher performance, flexibility, and lower latency for real-time applications. New network topology and virtualization can lead to new network vulnerability challenges, however, diligent standards work by organizations such as 3GPP, GSMA, and the National Institute of Technology (NIST), ensures that modern security checkpoints use industry best practices to monitor networks efficiently and effectively.
- **Big data analytics –** The use of big data, enabled by IoT, AI and by 5G, empowers many companies to optimize their processes, improve their customer journeys and gain insight into market dynamics. Unfortunately, large amounts of data generated and stored by various companies also represent potential gold mines for cyber criminals. Advanced analytics methods now allow them to compare data from multiple breaches and build more complete profiles of their potential victims. On the other hand, advanced analytics methods can also be used on network activity data by cyber security professionals to efficiently identify cyber attacks or vulnerabilities.
- **IoT –** The proliferation of IoT devices in both consumer and industrial sectors will be further enabled by the many advancements of 5G networks (increased network capacity, lower latency and better throughput). From connected home appliances to connected sensors in factories, the increasing number of IoT devices multiplies the amount of potential entry points for cyber criminals into sensitive networks. Many IoT devices (especially consumer-oriented applications) lack proper cyber protection, have often known vulnerabilities and are rarely updated. Moreover, consumers are often unaware of cyber security risks related to IoT devices.

2.6.2 Key considerations for future policy

Addressing the cyber risks resulting from these new technologies is done through focused research and development of new security tools and best practices, and through the development of a knowledgeable workforce capable of implementing them.

Financial support of research in each of these subjects already exists across many Canadian universities through governmental research programs. Such research initiatives are currently backed by the National Research Council (NRC) through programs such as the Canadian Institute for Cybersecurity at the University of New Brunswick, and the NRC-Waterloo Collaboration on AI, IoT and Cybersecurity at the University of Waterloo. Beyond financing each research program individually, promoting collaboration, domestically and internationally, is also essential.

To develop the necessary skilled workforce, support must be offered to colleges, universities and companies to attract highly coveted ICT students and workers into the often less appealing field of cyber security. The talent shortage in this field is an international problem caused by high demand in the global technology sector. In addition, jobs in the cyber security field in Canada are often less attractive for ICT professionals. To attract talent, the federal government already operates a work insertion and internship financing program – the Student Work Placement Program – that caters, among others, to the cyber security field. Additionally, the government supports cyber security R&D jobs in the private sector by directly financing some privately led research initiatives through the Cyber Security Cooperation Program. Nevertheless, the talent shortage is likely to increase with time due to demographic pressure. It is therefore important to ensure that these programs are effective and updated adequately.

EDUCATION DIVERSITY IN CYBER SECURITY

The workforce shortage in cyber security is a major concern for the industry and is likely to get worse. To alleviate the issue, companies should increase the diversity of their cyber security workforce. Improving diversity in terms of gender, age, ethnicity, work history etc. is an important challenge that, if solved, would widen the talent pool. Additionally, companies should also consider individuals with more diverse educational backgrounds that don't necessarily hold the usual computer science degree.

Although cyber security roles often require technical skills, there are many positions for which other educational backgrounds may be helpful. For example, lack of cyber awareness in companies, which is a major challenge for cyber security (cf. section 2.3) may be better addressed by someone with training in communications rather than a computer science expert. Workforces with wider sets of skills may find new solutions to address major challenges in cyber security.

Additionally, recruiting people with diverse educational and work experiences would allow companies to fill important gaps. Providing training through apprenticeships or dedicated education programs would provide easier and faster routes for people without computer science degrees to fill some basic technical roles.

CASE OF THE UNITED KINGDOM
NATIONAL PROGRAM ENCOURAGING DEVELOPMENT OF NEW TALENT IN CYBER SECURITY

To address the cyber security workforce shortage, the United Kingdom launched, among other initiatives, the CyberFirst national campaign aimed at informing teenagers of the possibility of a career in cyber security and encouraging them towards relevant higher education degrees. This campaign is orchestrated by the NCSC, the UK's equivalent to the CCCS, and supports school cyber security courses and offers generous scholarships and apprenticeships for higher education students aiming for a career in cyber security.

2.7 CHALLENGE 5 – STRENGTHENING POLICING EFFORTS AGAINST CYBER CRIMINALITY

2.7.1 Context

The four previous challenges concentrate primarily on the prevention of cyber criminality. However, to reduce the rate and impact of cyber crimes, the identification and prosecution of the perpetrators of these crimes are also essential. Currently, cyber criminals generally act with relative impunity – they rarely get caught and even more rarely get convicted. This is due to three main factors: the capacity of most sophisticated criminals to make their attack highly difficult to track down, a lack of capabilities of law enforcement agencies to tackle the ever-growing number of attacks, and the lack of an international regulatory framework which complexifies the coordination of cyber crime investigations.

- **Cyber criminal capabilities –** The technical capabilities of cyber criminals are likely to improve, and no entity can realistically slow this trend. The popularization of the Tor network (i.e. the Dark Web) allows increasing collaboration and the sharing of cyber criminality tools such as new malware.
- **Law enforcement capabilities –** It is often estimated that less than 1% of cyber crime incidents see law enforcement actions being taken to identify or prosecute the perpetrators. The exact prosecution rate of cyber crimes is unknown due to the fact most of them remain unreported. While 20% of Canadian businesses stated having been affected by cyber attacks in 2017, only 10% reported these incidents to the police (Statistics Canada, 2017).

  The low prosecution rate of cyber crime is indicative of the inadequacy of cyber law enforcement capabilities in terms of human resources, technical proficiency and legal framework. Building a sufficient force to address all incidents is realistically unfeasible, but additional resources are needed to tackle the prosecution of a larger number of attacks. Tracing criminals and producing evidence that stand the test of the tribunal is even more difficult when lacking proper resources and legal frameworks.

- **International regulatory framework –** Establishing an international framework for collaboration in cyber crime law enforcement would be ideal but it is impossible to achieve in practice. Currently, the largest agreement is the Budapest Convention, originally signed by the Council of Europe in 2001. Through this treaty, 67 countries, as of 2020, commit to align their national cyber laws and to set up the proper infrastructure to cooperate with other nations' law enforcement agencies. Countries opposing the Budapest Convention argue it goes against their digital sovereignty.

  Multiple bilateral and regional agreements also frame collaboration between countries with similar views on cyber law enforcement strategy. For instance, the United States-Mexico-Canada Agreement (USMCA) includes formal engagements to develop advanced cyber incident response capabilities and to share information on cyber crime intelligence gathering and investigations.

  Multiple international forums promote collaboration between countries and large corporations in the fight against cyber crime. The World Economic Forum's Center for Cybersecurity and the Global Forum on Cyber Expertise both promote public-private cooperation on multiple cyber-related issues. Other groups such as the G7 and INTERPOL have set up incident response cooperation centres providing tools to rapidly share information vital to cyber crime investigations.

2.7.2 Key considerations for future policy

The Government of Canada recognizes in its most recent cyber security strategy the need for additional resources in cyber crime policing efforts and included such provision in its 2019 action plan. Police agencies, including the RCMP and other provincial and municipal agencies, have advocated for improved data collection infrastructure to build a better image of the current cyber crime situation. This knowledge is necessary to ensure that planned resource increases are in line with the scope of the problem.

Current plans to increase cyber security capabilities of police forces extend through multiple years due to the lengthy process of recruiting experts and / or training officers. Considering the strong growth of cyber criminality, capability targets should be set to answer the future level of cyber crime, not the current one. More resources combined with an easier method to report cyber crimes would help to have a better picture of the state of cyber crimes.

As technology evolves faster than laws, the legal framework is likely to lag on cyber criminal tactics. Reviewing regularly the legal framework to consider the cyber criminals' evolving tactics is still beneficial, even if there is always a lag. Currently, prosecution based exclusively on digital evidence is very difficult and thus also makes policing many cyber crimes problematic. However, providing additional education to judges and juries on cyber criminal tactics would ensure a better understanding of evidence presented in court.

Development of national cyber law enforcement capabilities is only part of the solution to effectively prosecute cyber criminals. Investigation and prosecution of international cases require effective law enforcement in other countries and a proper collaboration framework. To that end, Canada should continue to pursue its efforts in the advocacy of more collaboration regarding cyber security enforcement. By enacting initiatives that support more effective responses to cyber crimes, Canada can become a thought leader in cyber security and promote better legislative practices to the global community.

DATA PRIVACY ECOSYSTEM

3.1 GLOBAL CONTEXT IN DATA PRIVACY

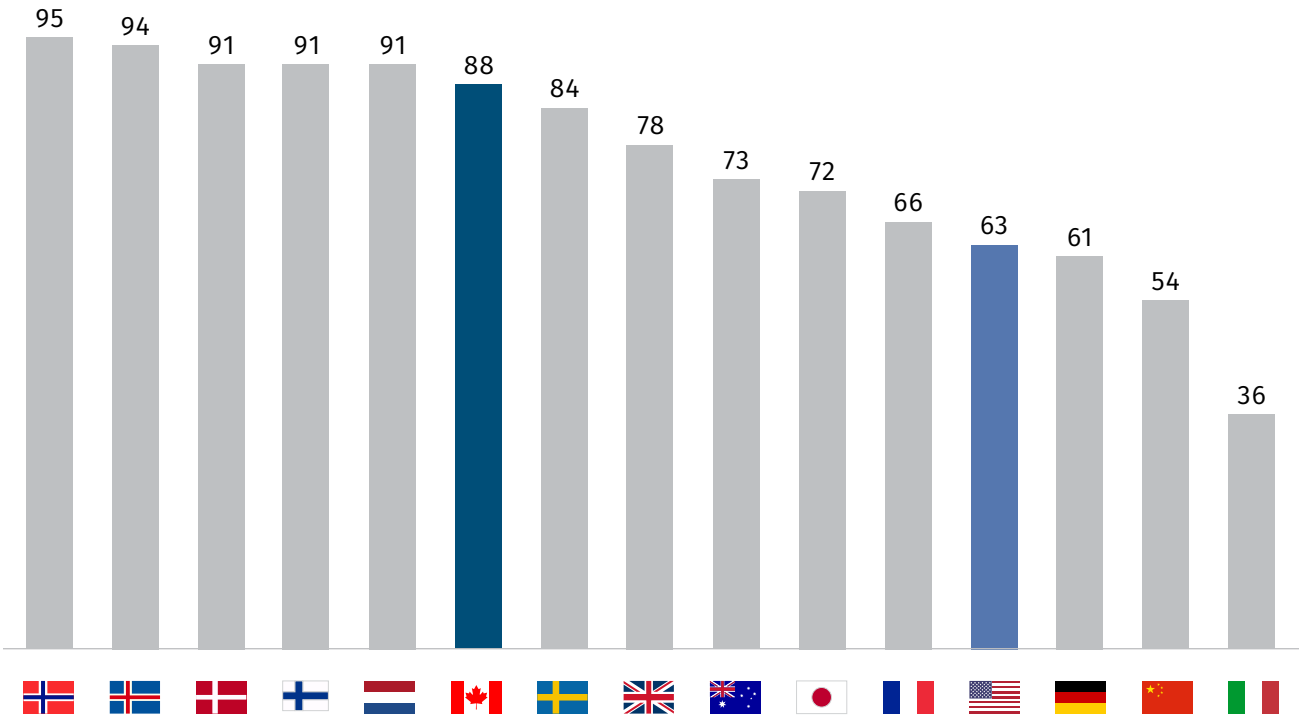
Data privacy awareness from the general public has risen in recent years around the world on the heels of major documented data breaches and data collection abuse cases. Privacy is an especially difficult subject to regulate in an ever-changing business and political landscape, fuelled on one side by the quest for increased technological development and adoption, and on the other by harrowing examples of data mismanagement.

3.1.1 Increased digitalization of the general public

The global population has shifted a growing portion of its activities online, seeking additional flexibility and convenience relative to traditional methods. In 2019 alone, the number of Internet users globally increased by 7% to reach 4.5 billion users, a growth rate more than 6 times higher than the growth of the general population. In Canada specifically, the Internet penetration rate is set at 94%, with more than 35 million active users (DataReportal, 2020).

Canadian citizens are at ease and relatively well-versed in the use of various online platforms, as exemplified by online banking where Canada's adoption trails only few countries. More than two thirds (25 million people) of the population are also active on social media, with nearly 1 million new users in the second half of 2019 (DataReportal, 2020).

Figure 3.1 – Online banking penetration rate by country [%; 2019; non-exhaustive]



Source: Canadian Bankers Association, Eurostat, Cint, eMarketer, DataReportal, CNNIC, desk research, Roland Berger

3.1.2 Recent breaches and data collection abuse cases

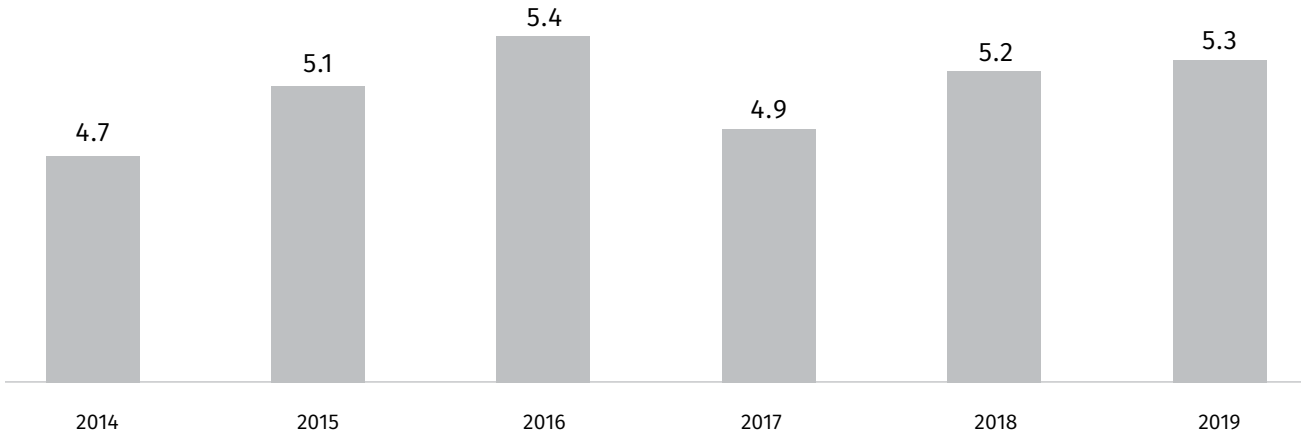
This growing level of digitalization is however not without risk in terms of data privacy. Two trends have gained attention from the general public: data breaches from large organizations and data collection abuse cases.

Data breaches

The average data breach cost attained 5.3 mCAD in 2019 (IBM Security / Ponemon Institute, 2019), a number that has been continuously growing over previous years. This figure has been driven upwards by large documented breaches of international corporations, such as the breach of all 3 billion Yahoo user accounts and the leak of critical personal information of Equifax customers, including social security numbers and dates of birth of 143 million people (representing more than 40% of the US population).

In Canada alone, recent breaches disclosed personal and sensitive information from a variety of established entities, such as Ashley Madison (32 million accounts breached by a hacktivist group), Capital One (106 million accounts - a portion being Canadian accounts - accessed from an outside individual connected to 30 other breaches) and Desjardins (4.2 million records exposed due to privileged access abuse from an ill-intentioned employee in the IT department).

Figure 3.2 – Global average total cost of a data breach [mCAD]



Source: IBM Security / Ponemon Institute, Roland Berger

Data collection abuse cases

Some large companies have also attracted unwanted attention by collecting seemingly unnecessary information and instilling fears of a “Big Brother” climate.

Reports have surfaced in recent years documenting extensive data collection from giant corporations including, among other examples, Google (Curran, 2018) (detailed recollection of location data; comprehensive search histories, including deleted searches; list of everything said to the Google Assistant and audio recording playback) and Facebook (Singer, 2018) (users and nonusers activity tracking on other sites and apps; biometric facial data without explicit opt-in consent).

These reports shed some light on commercial tactics used by global players and fueled the debate regarding the boundary between appropriate and inappropriate data collection.

3.1.3 Awareness and trust of the general public

These breaches and abuse cases negatively affect the general population's trust of online platforms, a perception shared by Internet users around the world. 76% of Canadian citizens say that they are at least somewhat concerned about their online privacy, and only 40% believe that the Canadian government is doing enough to protect their online data (Centre for International Governance Innovation, 2019).

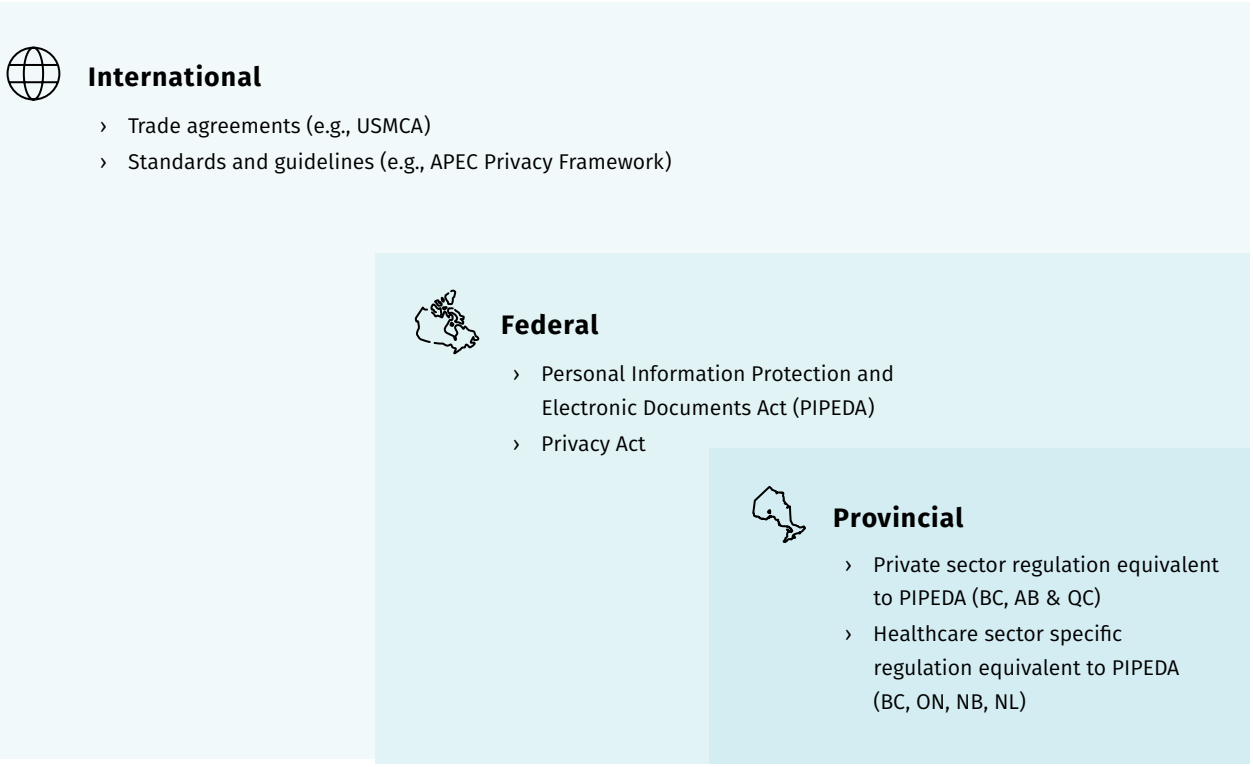
These figures might appear worrisome to players of the digital economy, who may feel that user adoption of new technologies, capabilities and services will slow based on fears of data privacy abuse. The figures may also worry legislators, who cannot always trust corporations to act and behave in a manner that protects the population and its interests. With that being said, the most critical component for the growth of the digital economy is the level of confidence held by the general public. Policymakers must ensure that consumers and clients feel protected to support the adoption of digital technologies.

While no absolute solution exists in the wide-reaching domain of data privacy, clear direction and regulation are preferable. The following sections will provide an overview of Canada's current legal landscape, as well as an incursion into two major challenges for the policymaker: the balance of privacy and economic growth, and the complexity of international regulations.

3.2 OVERVIEW OF CANADA'S POLICY FRAMEWORK

Canada's policy framework on data privacy is articulated in three segments: international relations and trade agreements, federal policies, and provincial policies.

Figure 3.3 – Three segments of policymakers



Source: Roland Berger

3.2.1 International agreements

Given the international nature of digital data and its flows, it remains logical for regulators to view it from a global standpoint. Historically, data provisions in international trade agreements were mostly linked to intellectual property protection efforts. However, a new wave of agreements, highlighted by the new United States-Mexico-Canada Agreement (USMCA), is increasingly including data privacy provisions, embedding the subject into larger aspects of trade.

The USMCA updates the previously standing North American Free Trade Agreement (NAFTA) in a significant way, comprising a digital trade chapter which promotes the free flow of electronic commerce. This chapter is based on the shared understanding from signing parties of the necessity to adopt or maintain a legal framework protecting the personal information of all users of digital trade (USMCA, 2020).

While the details of the required legal frameworks are left to the discretion of the countries, the partners are strongly encouraged to follow guidelines and principles from relevant international bodies, notably the Asia-Pacific Economic Cooperation (APEC) and its privacy framework (see Appendix 1). The guidelines included in the framework aim to facilitate the exchange of information without compromising personal information.

The inclusion of data privacy rules in the USMCA, along with other international agreements, constitutes an encouraging step towards increased international collaboration regarding the online security of citizens' and businesses' interests and may serve as the baseline of future trade agreements.

3.2.2 Federal policies

Aside from the Privacy Act which regulates the individuals' right to access their information held by federal entities (Office of the Privacy Commissioner of Canada, 2019), legal obligations in Canada regarding data privacy can be found in the Personal Information Protection and Electronic Documents Act (PIPEDA). This key piece of legislation, based on a set of 10 principles (see Figure 3.4), covers the ways in which data should be safely stored as well as the ways organizations must collect, use and disclose personal information in the course of commercial activities. The main objective is to balance on one side the need for organizations to use personal information for legitimate, intended business purposes, and on the other the essential right to privacy of individuals (Office of the Privacy Commissioner of Canada, 2019).

The PIPEDA applies to federally regulated businesses and to private sector organizations conducting businesses in most provinces (excluding Quebec, Alberta and British Columbia), or handling personal information crossing provincial or national borders. It generally does not apply to not-for-profit and charity groups or political parties and associations.

The Digital Privacy Act, effective since 2018, amended the PIPEDA to introduce data breach response obligations, related to record-keeping, reporting and notification (see Figure 3.5). Failure to comply with any of these requirements can lead to penalties similar to criminal offences and exposes the organization and its directors personally to fines of up to 100 kCAD per violation (Office of the Privacy Commissioner of Canada, 2015).

This amendment to the PIPEDA constitutes an important element for data privacy enforcement, requiring increased accountability from organizations and providing reinforced peace of mind to individuals, in line with the global trend of similar regulation. However, the maximum penalty amount is far lower than that of other countries, making it more symbolic rather than clearly discouraging wrong practices. For reference, the maximum penalty for violation to the European Union General Data Protection Regulation (GDPR) can go up to 4% of a company's worldwide revenue.

Figure 3.4 – 10 principles of PIPEDA

1	**Be accountable**
2	**Identify the purpose of personal information collection**
3	**Obtain valid, informed consent**
4	**Limit collection**
5	**Limit use, disclosure and retention**
6	**Be accurate**
7	**Use appropriate safeguards**
8	**Be open**
9	**Give individuals access**
10	**Provide recourse**

Source: Personal Information Protection and Electronic Documents Act, Roland Berger

Figure 3.5 – Data breach response obligations introduced in the Digital Privacy Act

Source: Digital Privacy Act, Roland Berger

3.2.3 Provincial policies

Many provinces implemented additional privacy laws to complement PIPEDA. British Columbia, Alberta and Quebec have passed laws that are viewed as similar enough to the PIPEDA to allow them to independently regulate data privacy in the private sector.

Some provinces (British Columbia, Ontario, New Brunswick, and Newfoundland and Labrador) have also adopted laws specifically related to the healthcare sector, which have been viewed as substantially similar to the PIPEDA, and thus exempting them from federal privacy oversight in this department (FairWarning, 2019).

Following the recent PIPEDA update that introduced stronger enforcement criteria, some provinces are also considering a review of their own privacy laws. This is particularly true of Quebec (following the Desjardins data breach) and Ontario (following multiple data breaches and attacks in its healthcare sector).

The Quebec government introduced Bill 64 (An Act to modernize legislative provisions regarding the protection of personal information) stating that current data protection laws are outdated and no longer adequately regulate an evolving digital landscape. While replicating the Digital Privacy Act regarding requirements for breach reporting, the Act would significantly increase penalties related to non-compliance (currently set at a maximum of 50 kCAD), with private sector entities subject to fines reaching up the highest amount between 25 mCAD or 4% of a company's worldwide revenue, making it the most punitive privacy law in Canada (Tehrani, Oates, Kappler, & Matziorinis, 2020).

In Ontario, the various breaches having affected the healthcare industry prompted the adoption of a new law amending the province's Personal Health Information Protection Act (PHIPA). This new law is also raising the maximum penalty amount (from 500 kCAD to 1 mCAD for organizations). Additionally, the law introduces new powers to the province's Privacy Commissioner, notably the ability to order health information custodians to cease providing personal health information to a consumer electronic service provider (including entities involved in the communication of personal health information through electronic means, like mobile apps, online portals and smart devices). By solidifying the privacy of individuals in the healthcare sector, these increased sanctions and updated powers may in return slow down the digital healthcare revolution currently in progress (Morgan, Glover, Scherman, & Chen, 2020).

3.2.4 Main challenges related to Canada's data privacy framework

International agreements, national policies and distinct provincial regulation all aim to provide individuals with concrete data protection measures and proactively defend their interests. Policymakers face challenges and must formulate a strategy to tackle them in the most efficient way. Key challenges can be categorized into two broad topics: the need to balance digital privacy with the digital economy growth and the complexity of the international legislative landscape in a more digitalized world.

3.3 CHALLENGE 1 – BALANCING OF DATA PRIVACY AND DIGITAL ECONOMY GROWTH

3.3.1 Context

The digital economy is a particularly fast-paced industry with an evolving environment prone to innovation. Such a climate encourages businesses to favor a rapid route to market, sometimes at the expense of data privacy and security.

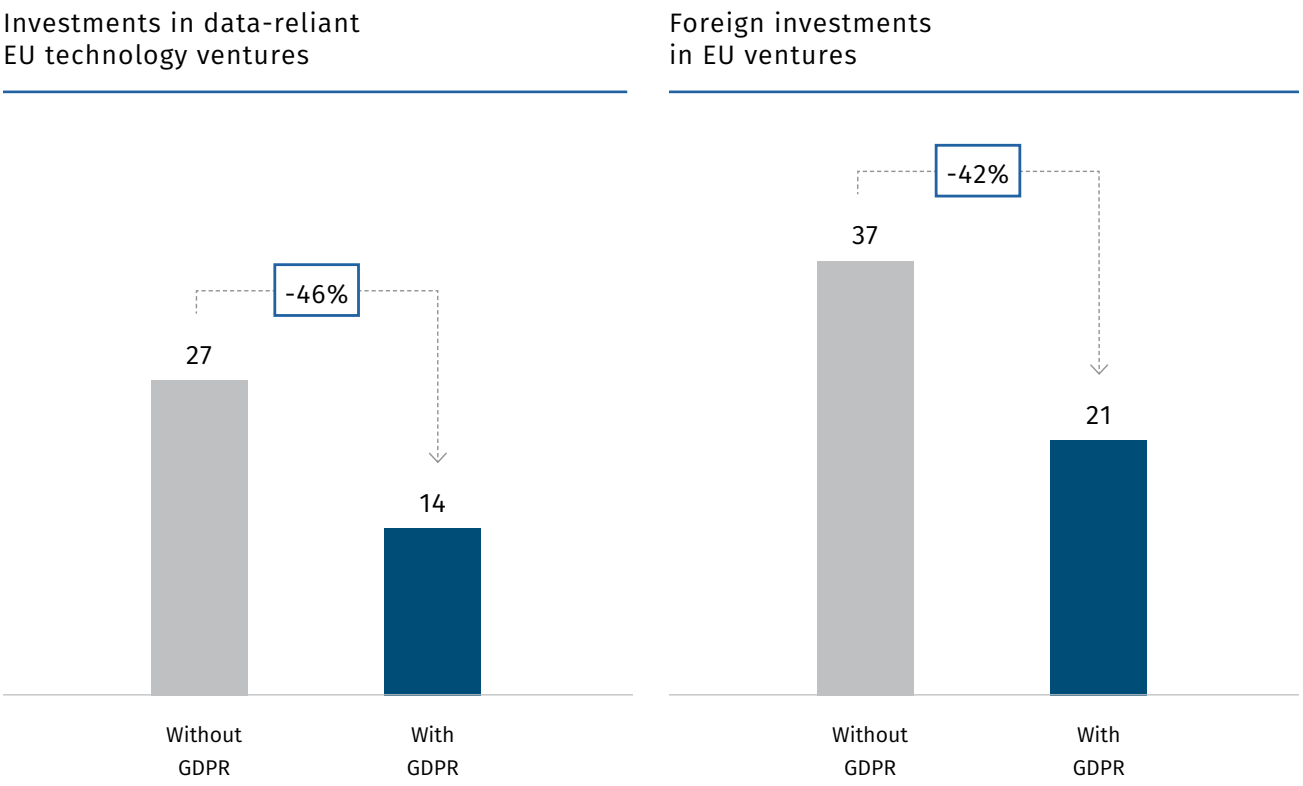
The balance of data privacy and digital innovation is pivotal in today's society and should be considered in the highest regard in growing the digital economy. While users want to experience innovative solutions, they should not be asked to trade off security for the sake of innovation. The regulatory environment should seek to make this balance inherent to the successful deployment of new technologies.

The current COVID-19 crisis offers a great example of the delicate balance required between technology and privacy. Countries around the world have rolled out or are in the process of rolling out COVID-19 contact-tracing applications based on a variety of technologies and standards. Canada is no exception, having launched a nationwide application in August. This mobile application is a great case of rapid digital innovation and could play a crucial role in the global fight against COVID-19, enabling tracking of the spread of the virus and proactively informing individuals of possible exposure. However, it raises important questions related to data privacy, with many citizens expressing concerns about intensified government surveillance resulting from constant position monitoring (Singer, 2020).

These privacy concerns led to a joint statement from federal, provincial and territorial Privacy Commissioners, outlining guiding principles to be respected. They argue that the application should be built around notions of consent, transparency and purpose limitation, helping Canadians make the informed decision to voluntarily use the application and honouring their right to privacy (Office of the Privacy Commissioner of Canada, 2020).

The line between the adoption of a new digital tool and privacy is one that is difficult to draw. The United States, on one hand, usually favors innovation, which led to many key technological advances. On the other hand, the European Union tends to put privacy interests first. While highly protective of individuals' interests, this increased focus on privacy seemed to cause a decline in investment in various ventures following the implementation of the GDPR, particularly in data-reliant EU ventures (Jia & Wagman, 2020).

Figure 3.6 – Dollar amount per deal in EU ventures following GDPR implementation [mCAD]



Source: Jia & Wagman – One-year impact of the GDPR on European Ventures, Roland Berger

3.3.2 The case of smart cities

The use of IoT devices to create smart cities allows for a multitude of new possibilities. Municipalities become better equipped to make decisions based on relevant data and plan more efficiently for future urban needs. Devices can monitor, for example, road traffic, noise levels, and air pollution, allowing the city to establish a data-driven response certain of achieving its purpose.

The more data is collected, however, the greater is the risk for citizens' privacy from a data collection abuse standpoint. These connected devices also provide additional entry points for potential cyber attacks, which could result in the disclosure of sensitive personal information, exposing citizens to further harm. Recent cases in both the private and the public sphere highlight the emerging need for established regulation parameters.

In the private sector, the Sidewalk Labs' project in Toronto was particularly ambitious, seeking to create a futuristic community, where everything could be managed by IoT devices, from heated sidewalks to retractable umbrellas.

The company stated that data collected from citizens would be de-identified and aggregated (in accordance with guiding principles outlined by Privacy Commissioners), then made available publicly to businesses and government institutions seeking to use it for future developments. However, de-identification poses a risk of re-identification, accrued by the collection and storage of localization data. In addition, Sidewalk Labs did not clearly indicate the way it would collect consent from individuals, a fundamental right covered by the PIPEDA.

This lack of potential "opt-out" ability prompted a lawsuit from the Canadian Civil Liberties Association (CCLA). While consent is easy to provide when an individual puts a smart assistant (e.g., Alexa, Google Home) in its home, it is much trickier to provide when walking from one block in Toronto to the next. Citing poor economic conditions resulting from the COVID-19 crisis, Sidewalk Labs decided to abandon its Toronto project (Doctoroff, 2020). It is clear that public concerns played a meaningful role in this decision, CCLA having targeted all three levels of government in its lawsuit.

In the public sector, Canada's Smart City Challenge (a national competition encouraging cities to formulate technological solutions to their challenges) is an example where policymaker had to balance innovation and data privacy. Following its announcement in 2017, all federal, provincial and territorial Privacy Commissioners addressed a joint letter to the Minister of Infrastructure and Communities, urging him to "proactively take steps to ensure that privacy and security of personal information are specifically considered in the selection, design, and implementation of the winning proposals" (Office of the Privacy Commissioner of Canada, 2018). While, the challenge may promote innovative solutions to the "most pressing challenges", they fear that the short timeline involved in the challenge may relegate privacy and data security to secondary concerns.

3.3.3 Key considerations for future policy

To better align positions around various interests, the National Digital and Data Consultations were launched by the Ministry of Innovation, Science and Economic Development in 2018, seeking to obtain the perspectives and ideas of all Canadians. This led to the launch of the Digital Charter in 2019, a set of 10 principles (see Figure 3.7) hoping to increase the trust of Canadians in the digital sphere and emphasize notions around the fiduciary duty of data owners.

Figure 3.7 - Ten principles of the Digital Charter

1	**Universal Access**
2	**Safety and Security**
3	**Control and Consent**
4	**Transparency, Portability and Interoperability**
5	**Open and Modern Digital Government**
6	**A Level Playing Field**
7	**Data and Digital for Good**
8	**Strong Democracy**
9	**Free from Hate and Violent Extremism**
10	**Strong Enforcement and Real Accountability**

Source: Digital Charter, Roland Berger

The Charter provides tremendous guidance to corporations and increased perceived security from individuals due to the privacy requirements involved. However, the Charter is not a legal document.

As part of the actions necessary to implement the principles outlined by the Digital Charter, Minister Bains (responsible for the Charter) announced the government's proposal to modernize the PIPEDA. There is a recognized need to update the PIPEDA to mirror these principles and "strengthen privacy for the digital age" (Government of Canada, 2019).

The proposal for the PIPEDA modernization is divided in 4 sections: Enhancing individuals' control, enabling responsible innovation, enhancing enforcement and oversight, and ongoing assessment. In each segment, multiple ideas are expressed as ways to directly implement change.

The Digital Charter clearly communicated the direction and strategy that is to be favored in the format of guidelines. However, these guidelines are not legislation and thus, create uncertainty and even confusion as to the expected approach to managing digital data. It would be preferable to modify the law as promptly as possible to create cohesiveness between regulation and guidelines. In doing so, Canada would minimize the risk of technology investments that result from an uncertain context. Furthermore, by updating the regulation that is currently viewed by some as lacking teeth (Baer & Newman, 2019), the country would be in a better position to enforce higher privacy standards in digital technologies. The result would heighten trust from individuals, further promoting the adoption of new digital technologies.

The federal government must consider the various regulations adopted around the world (e.g., the US legislation, the European Union GDPR and the discussed updates in Quebec and Ontario) to formulate its new legislation. Canada must adopt regulation relevant in the evolving global context, framing it with the best interests of Canadians in mind, notably regarding the intricacies of the protection of their data and the growth of the digital economy. Given the rapidly evolving landscape, Canada should also make a commitment to frequently re-examine the legislation to make sure it remains relevant with the development of new technologies.

3.4 CHALLENGE 2 – NAVIGATING THE COMPLEXITY OF THE INTERNATIONAL LEGISLATIVE LANDSCAPE

Data privacy is a concept viewed in strikingly different ways by countries sharing relatively similar political cultures.

For the European Union, data protection is considered a fundamental right and is related to the rights of dignity and personality of individuals. The right to privacy is included as part of the European fundamental rights system having emerged as a necessary post-World War II supranational identity. The underlying language of European data protection law is centred around human rights and seeks to protect individuals from wrongful processing of their personal data, defining as a basic rule that all data processing requires legal basis.

In the United States, the favored approach to data protection is related to the country's free-market ideology, referring to individuals as privacy consumers, participants in market relations using their personal information as a commodity. The US Constitution does not consider the right to privacy in the same way as in the European Union, only protecting citizens from specific kinds of data collection and processing by the government, not by other private individuals (Schwartz & Peifer, 2017).

This dichotomic perception provides a brief introduction to the complexity of data privacy management on a global scale. The complexity can be broken down into six separate issues that Canadian policymakers must consider when building their policy.

THE AMERICAN VIEW OF PRIVACY

In 2011, the Supreme Court invalidated a Vermont law preventing pharmacies from selling identifying information of prescribers without the explicit consent of the prescribing party. The judgment stated that the law violated the free speech clause of the First Amendment because it restricted the speech in aid of pharmaceutical marketing. This example illustrates the market-centric view of privacy in the US. (Schwartz & Peifer, 2017)

3.4.1 Context: Issues and challenges of international data protection

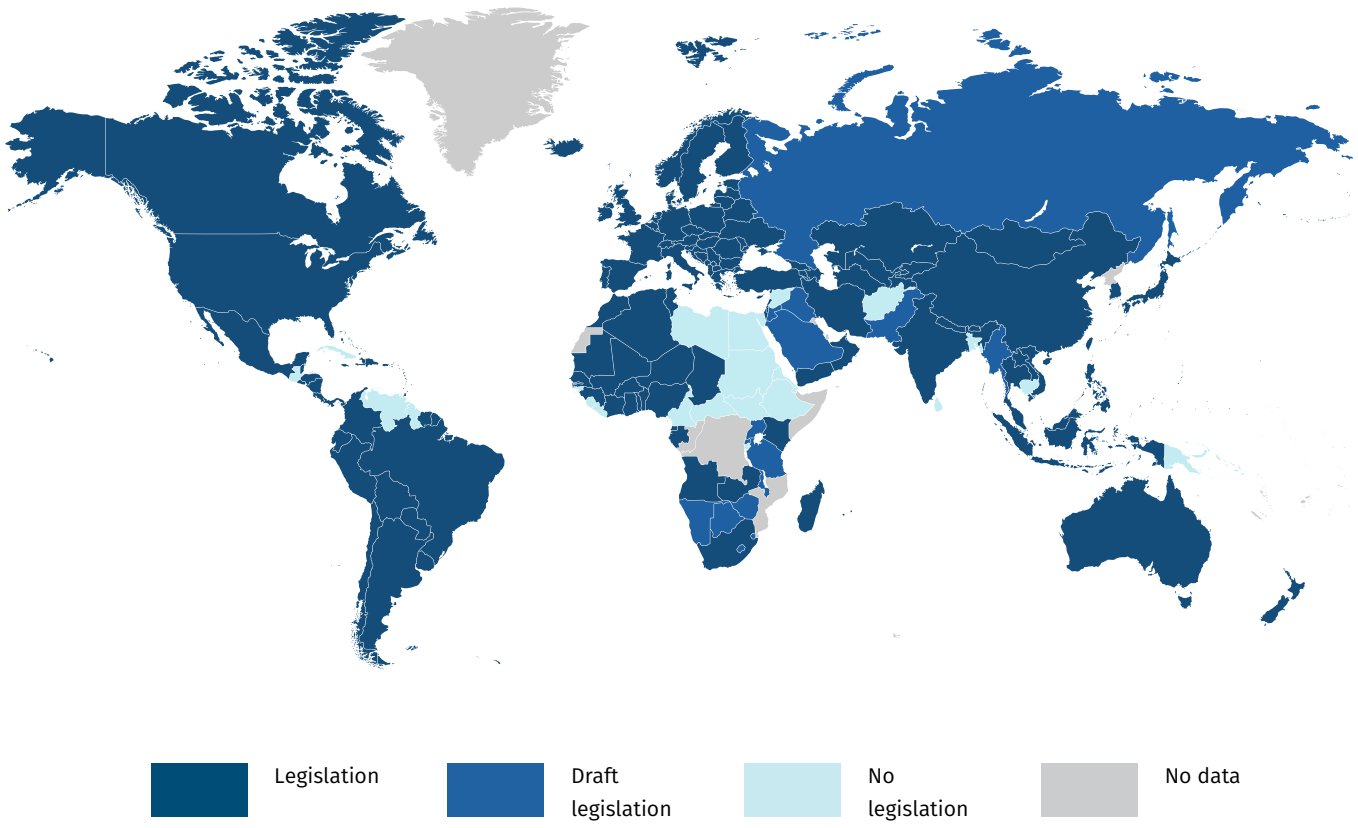
There are 6 key interconnected issues regarding international data protection. Each of them presents different challenges for policymakers.

3.4.1.1 Coverage of data protection laws

The first difficulty associated with international data protection is the fragmentation and diversity of privacy laws around the world. Most countries have data protection laws, but some exclude specific services and practices from coverage (such as the exclusion of cloud services from regulation). Some others contain gaps and exemptions, although this is becoming less common. For example, Japan abolished in 2017 the exemption it used to provide small businesses using personal information databases of fewer than 5,000 records (Hayashi & Yukawa, 2020). There is also a group of countries, generally not major trade partners with Canada, that are currently drafting (e.g. Russia, Saudi Arabia) or simply still do not have (e.g. Venezuela, Egypt) any data protection legislation (UNCTAD, 2020).

Navigating the web of data protection laws is a complex task as many trade agreements require adequacy between data protection standards to ensure the free flow of information. If provisions are not symmetric, countries can enter in specific collateral agreements, such as the European Union – United States Privacy Shield. By engaging in such distinct regulating frameworks, the need for the creation of a shared set of international guidelines is limited, which might eventually decrease international collaboration between economies.

Figure 3.8 – Data protection and privacy legislation worldwide [2020]



Source: UNCTAD, Roland Berger

3.4.1.2 Emergence of new technologies

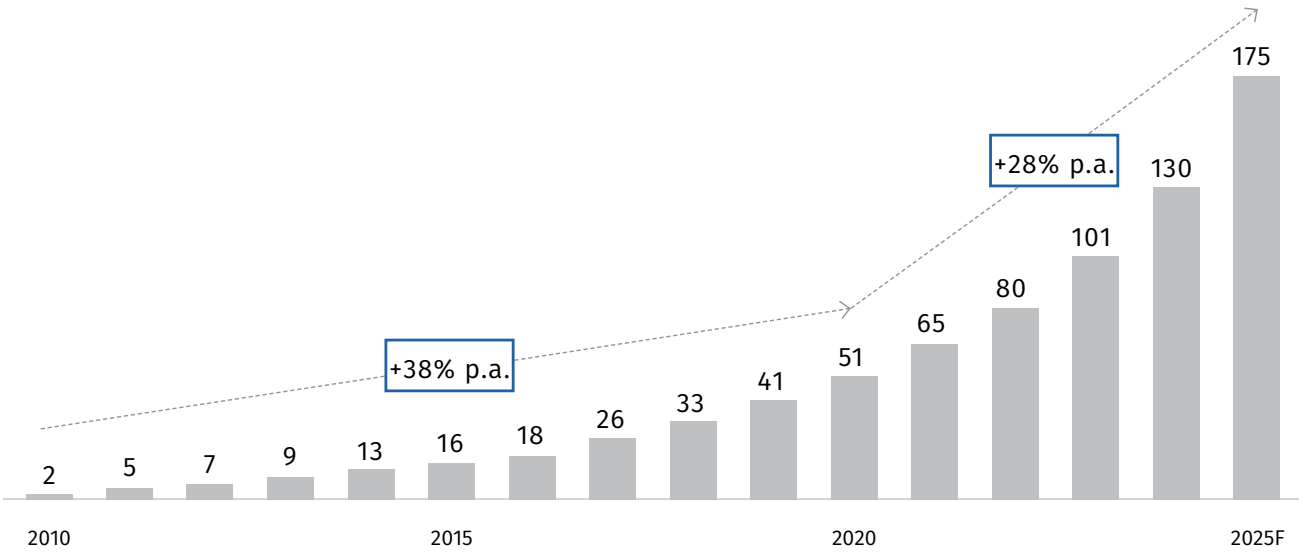
New technologies provide revolutionary possibilities for the digital economy, but also pose an important challenge for policy and lawmakers struggling to implement regulation in a fast-paced environment. Risks of security breaches and privacy mismanagement increase due to the emergence of new technologies. Many specific technologies raise questions in data privacy, particularly cloud computing, the Internet of Things (IoT) and big data analytics.

Cloud computing – Complex issues related to cross-border data transfers arise from cloud computing. By connecting users on a global scale, cloud service providers may store data in a foreign location and communicate it to clients using local infrastructure. To limit potential exposure of domestic data, some countries have implemented data localization rules imposing that overseas service providers store data within the country. There is no unanimous agreement upon ways to regulate cloud computing, and some countries (including Canada) rather favour the free flow of information in their international trade agreements (USMCA, 2020).

Internet of Things (IoT) – The number of connected devices and the amount of data they generate is growing quickly, resulting in more information exchange across international borders. IoT cyber attacks are increasingly prevalent, highlighting the need for international cooperation and regulation. For instance, 80% of healthcare security decision makers in China, Germany, Japan, the UK, and the US reported attacks on their connected devices between 2018 and 2019 (Irdeto, 2019).

Big data analytics – Large databases are increasingly targeted by hackers given the amount of information available. The hefty amount of data collected from users around the world are highly useful for organizations seeking to better understand market dynamics and prepare for upcoming projects. However, big data's underlying principle of collecting all data, not only directly pertinent data, is in opposition with global data collection limitation principles (as outlined in the APEC privacy framework). These principles, guidelines rather than binding regulation, offer wiggle room for corporations, which may negatively affect the privacy of individuals.

Figure 3.9 – Worldwide amount of data created by year [zettabytes]



Source: Centre for Strategic and International Studies, Roland Berger

3.4.1.3 Cross-border data transfers

Legislations on cross-border data transfers are useful to understand countries' positions on data privacy and information flow. Some countries, like the United States, have few restrictions on the transfer of personal data to foreign jurisdictions (Congressional Research Service, 2019). Others favour "exceptional circumstances" or "ongoing exceptions".

Exceptional circumstances exceptions are included in many privacy laws and provide countries with the right to allow cross-border data transfers in specific cases, highlighting some common ground among national privacy laws (Centre for Information Policy Leadership, 2015). These transfers may be allowed, among other cases, when the data is necessary for the performance of a contract between the data subject and the controller, or when it is used in legal proceedings or to exercise legal rights.

Ongoing exceptions are less consistent, but typically follow a combination of up to four approaches, all presenting various strengths and limitations.

- The **adequacy** approach, equivalent to the maintenance of a whitelist, is based on the assessment that a foreign jurisdiction provides a sufficient level of protection. It promotes interoperability among partner countries but may cause difficulties for countries found inadequate. Based on this assessment, an international trade agreement between nations deemed adequate may include provisions to encourage the free flow of information across borders, as is the case in the USMCA.
- The **binding rules** approach evaluates whether a specific company has put in place processes and mechanisms (namely an independent review process) providing an appropriate level of protection. It allows free movement of information among corporate participants and encourages the implementation of best practices but is a demanding exercise that is not easily transferable to other groups.
- The **model contracts** approach examines contracts to determine if specific wording appears in order to provide sufficient protection. The language element promotes interoperability with other groups, but partners may circumvent the provision on a technicality.
- Finally, the **consent** approach determines if individuals can consent to the transfer of their data. It is effectively the clearest approach, presenting the lowest compliance burden for organizations, but can expose businesses to complaints and disputes over differing interpretations.

Most countries combine multiple approaches in order to establish cross-border transfer mechanisms as no single approach yields exclusively positive results. There is no standard combination, which requires countries to negotiate one-on-one agreements and limits the interoperability of chosen combinations.

3.4.1.4 Balance between surveillance and data protection

This issue calls upon ethical judgment, preventing the agreement on international guidelines. Data privacy is regarded by countries to be, at least at some level, an undeniable right of citizens. Widespread surveillance, however, is often authorized in the context of national security concerns.

Many national laws around the world include exceptions related to law enforcement on national security counts. The American Patriot Act notably allows the government to monitor phone and email communications and track Internet activity of Americans, should they be on domestic or international soil. While aimed at terrorism, it was found in 2015 that during the 14 years it had been effective, no major terrorism cases had been cracked due to surveillance authorized by the Patriot Act (Ybarra, 2015), raising questions about the delicate balance between appropriate and undue surveillance techniques and authorizations.

Governments around the world adopt different positions which is a significant source of friction.

3.4.1.5 Strengthening of data protection sanctions and enforcement by trade partners

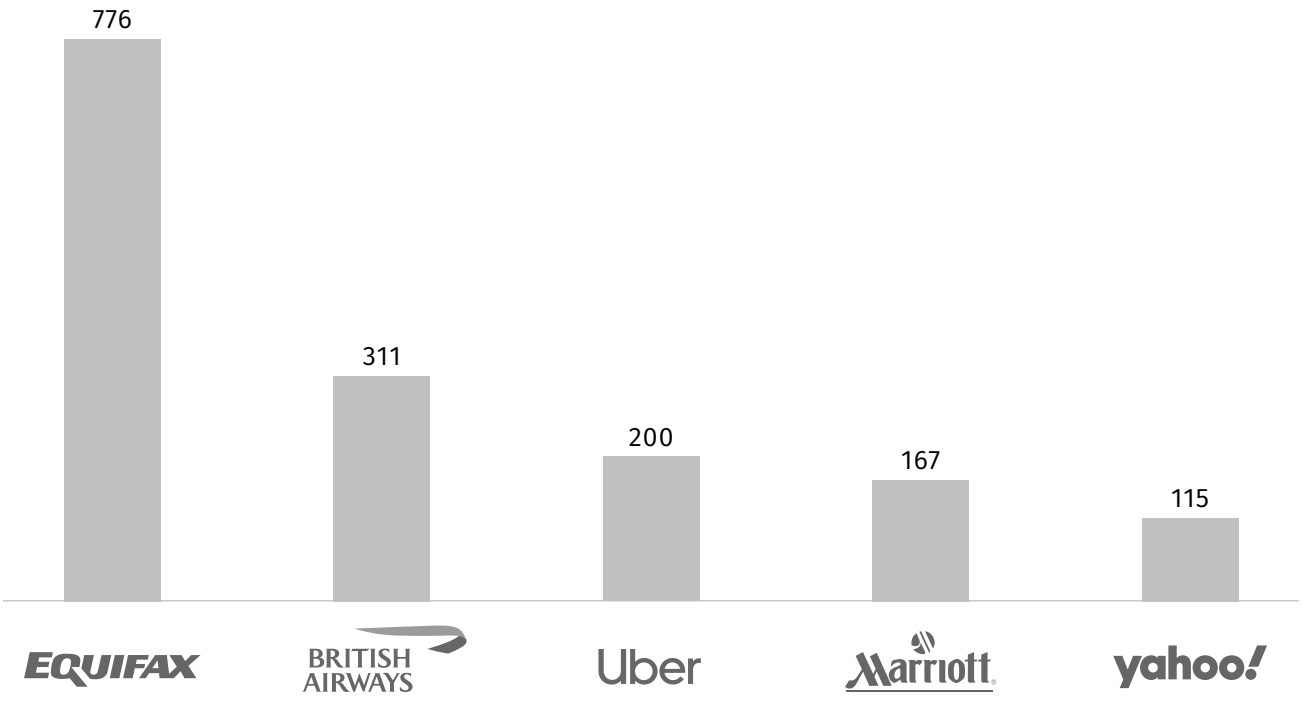
Organizations guilty of a data breach have recently been subject to increasingly higher fines and penalties. Many large, well-renowned organizations had breaches reaching unprecedented consequences, much larger than foreseen in previously existing regulations. The US is considered a leading country in terms of enforcement, imposing massive fines and sanctions in recent years. Other countries have also planned to or have already amended their privacy laws to strengthen their powers, namely the European Union (GDPR, 2016) and Australia (Office of the Australian Information Commissioner, 2018).

These increased sanctions speak to all parties concerned by a data breach:

- **The target company –** Heavy fines and sanctions send a clear message regarding the necessary reform of internal practices;
- **The affected individuals –** The fines provide a needed form of redress to the harm suffered from the breach;
- **The larger industry –** Sanctions act like a shockwave among similar companies, which might be more inclined to adopt leading best practices rather than to suffer similar fines.

These fines help communicate to all parties that data privacy is important, but lack uniformity. Canada lags the US and Europe with penalties up to only 100 kCAD – a mere symbolic fine for large multinationals.

Figure 3.10 – 5 largest data breach penalty amounts [mCAD; as of July 2020]



Source: CSO, Roland Berger

3.4.1.6 Determining jurisdiction linked to a data protection law contravention

Determining jurisdiction, a major component of law, is made increasingly difficult to establish in matters of data privacy by the international nature of data flows. Data traceability and the absence of a global agreement on data protection are factors that add complexity to the determination of jurisdiction for data privacy regulation enforcement.

Most domestic legislation aims to regulate any activity targeted at a country's residents, regardless of the guilty business's location. The GDPR is the most comprehensive example of such regulation, applying to any organization around the world either offering goods and services to or monitoring the behaviour of European citizens.

Some countries have passed regulations for specific sectors. For example, the US Child Online Privacy Protection Act (COPPA) extends to foreign service providers that aim their activities towards US children or collect information from them (Federal Trade Commission, 2000).

However, the adoption of international jurisdiction laws and policies requires stronger alignment between countries, an objective that is highly difficult to achieve. The GDPR is a rare example of successful cooperation as it mobilizes a large consortium of countries around this crucial issue.

3.4.2 Key considerations for future policy

The analysis of these six issues exposes the complexity of international data privacy regulation. The cultural definition of privacy, the disparity of opinions and the evolving landscape create difficulties for any country who would try to push ahead its ideology and its regulation in the hope to set the international standard.

Policymakers in Canada must consider each of these issues, keeping in mind both a national and international perspective, when designing and implementing data privacy policies. There is no fundamentally right or wrong answer regarding data privacy. There are, however, choices to be made related to future regulations and their intended angle and purpose.

Should new technologies be embraced immediately to encourage economic growth and technological research and development, or should increased scrutiny and compliance be the focus, to the risk of falling behind other countries?

Should Canada establish its own adequacy requirements to cross-border data transfers, or should it follow more stringent requirements implemented by regulations such as the GDPR?

Should provisions for surveillance under national security concerns be more detailed and restricted, or should they be loosened to allow for a larger potential amount of foiled terrorist plots?

Each of these positions presents valid advantages, but also drawbacks. Adopting one or the other should be done in a cohesive manner with Canada's foreign policy and consider the evolving environment. Policymakers should continue their current efforts to include provisions in trade agreements regarding new technologies and cross-border data transfers. Other principles should also guide policymakers' action, for example revising penalty amounts related to data breaches by evaluating positions adopted by economies like the US and the EU and adopting provision allowing the prosecution of foreign entities directing their activities at Canadian citizens.

Policies must frequently be reviewed to ensure they keep up to date with changing technologies, national priorities and international relations. For Canada, a thought leader mentality is a good strategy for this sensitive topic and may help foster international collaboration in line with Canada's perception of the issue.

FINAL REMARKS

The evolving landscape of digital technologies poses an important challenge for policymakers around the world. Cyber attacks, threatening everything from the integrity of personal information to the performance of critical infrastructure, have increased in recent years and show no sign of slowing down. The dematerialized and increasingly global nature of data calls for additional attention from policymakers on both a local and international level.

Cyber security and data privacy are wide-reaching subjects comprising ethical, legal, societal and business implications. The issues faced by regulators, as well as their potential responses, can be summarized by the seven challenges outlined in this document.

1. Improving the general public's digital literacy – By educating individuals and organizations of the threats posed by cyber attacks, policymakers will help consolidate the first line of defence against future threats;
2. Supporting smaller institutions in their digital transformation – By providing additional tools and resources to small institutions lacking the necessary skills to adequately protect the data they manage, policymakers will contribute to the safe continued growth of the digital economy;
3. Securing critical infrastructure and governmental networks – By increasing standards and accountability for critical infrastructure providers and offering them the necessary guidelines, policymakers will reduce risk of disruption;
4. Keeping up with a changing technological environment – Preparing tomorrow's workforce and encouraging research and developments in key topics is essential to future efforts in the evolving fight against cyber attacks;
5. Strengthening policing efforts against cyber criminality – By ensuring the right level of resources and improving capabilities of the police force and the legal system, the country will have better means to convict cyber criminals;
6. Balancing of data privacy and digital economy growth – By introducing principles such as those outlined by the Digital Charter in an updated piece of legislation, Canadian policymakers will ensure digital innovation is done in respect of data privacy;
7. Navigating the complexity of the international legislative landscape – By formulating its strategy on international data privacy, emergence of technologies, cross-border data transfers, surveillance, strengthening enforcement, and jurisdiction, Canada will act as a thought leader and encourage international collaboration.

By responding to these challenges while respecting its values, Canada will be able to further protect its citizens, businesses, critical infrastructure, and government / institutions, as well as encourage international collaboration on cyber security and data privacy.

APPENDIX

Established in 2005 and revised in 2015, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework reaffirms the value of privacy in the context of electronic commerce promotion throughout the Asia-Pacific region. The framework developed by the Forum, of which Canada is one of the twelve founding nations, identifies nine principles at the root of ethical and trustworthy information practices:

- **Preventing harm:** personal information protection should be designed to prevent the misuse of such information, and remedial measures should be proportionate to the likelihood and severity of harm threatened by the collection, use and transfer of information;
- **Notice:** personal information controllers should provide clear statements about their practices, including the fact that personal information is collected, the purpose of collection, the types of organizations to whom information might be disclosed and the choices offered to limit the use and disclosure of personal information;
- **Collection limitation:** collection of personal information should be limited to information that is relevant to the purposes of collection;
- **Uses of personal information:** personal information collected should only be used to fulfill the purposes of collection except with the consent of the individual whose information is collected, when necessary to provide a service requested by the individual or by the authority of law and other legal instruments;
- **Choice:** where appropriate, individuals should be provided with clear, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information;
- **Integrity of personal information:** personal information should be accurate, complete and kept up to date to the extent necessary for the purposes of use;
- **Security safeguards:** personal information should be protected with appropriate safeguards against risks. Those safeguards should be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information;
- **Access and correction:** individuals should be able to
  - obtain confirmation of whether the personal information controller holds personal information about them;
  - have their collected information communicated to;
  - challenge the accuracy of their personal information and have the information rectified or deleted.
- **Accountability:** a personal information controller should be accountable for complying with measures that give effect to principles stated above.

REFERENCES

- Asia-Pacific Economic Cooperation. (2015). *Asia-Pacific Economic Cooperation Privacy Framework.*
- Baer, A., & Newman, S. (2019, June 26). *Canada's New Digital Charter and What This Means For PIPEDA.* Retrieved from Mondaq: https://www.mondaq.com/canada/privacy-protection/818948/canada39s-new-digital-charter-and-what-this-means-for-pipeda
- Britneff, B. (2020, June 18). *Coronavirus contact-tracing app to launch nationally in early July, Trudeau says.* Retrieved from Global News: https://globalnews.ca/news/7079851/coronavirus-tracing-app-launch-nationally/
- Canadian Bankers Association. (2019, March 13). *Focus: How Canadians Bank.* Retrieved from Canadians Bankers Association: https://cba.ca/technology-and-banking
- Center for Strategic and International Studies. (2018). *Economic Impact of Cybercrime - No Slowing Down.* McAfee.
- Centre for Information Policy Leadership. (2015). *Cross-Border Data Transfer Mechanisms.*
- Centre for International Governance Innovation. (2019). *Internet Security & Trust.*
- Congressional Research Service. (2019). *Data Flows, Online Privacy, and Trade Policy.*
- Curran, D. (2018). Are you ready? Here is all the data Facebook and Google have on you. *The Guardian*.
- DataReportal. (2020). *Digital 2020: Canada.*
- Doctoroff, D. L. (2020, May 7). *Why we're no longer pursuing the Quayside project – and what's next for Sidewalk Labs.* Retrieved from Medium: https://medium.com/sidewalk-talk/why-were-no-longer-pursuing-the-quayside-project-and-what-s-next-for-sidewalk-labs-9a61de3fee3a
- Electronic Privacy Information Center. (Multiple years). *Investigations of Google Street View.* Retrieved from EPIC.org: https://epic.org/privacy/streetview/
- Eurostat. (2020). *Individuals using the Internet for Internet banking.*
- FairWarning. (2019, March 20). *Canadian Data Privacy Laws, Security Frameworks, and Cloud Compliance.* Retrieved from FairWarning: https://www.fairwarning.com/insights/blog/canadian-data-privacy-laws-security-frameworks-and-cloud-compliance
- Federal Trade Commission. (2000). *COPPA.*
- Fraser, D., & Dykema, S. (2018, August 6). *The Digital Privacy Act: 5 FAQs about the new mandatory breach response obligations effective November 1, 2018.* Retrieved from Mondaq: https://www.mondaq.com/canada/privacy-protection/725602/the-digital-privacy-act-5-faqs-about-the-new-mandatory-breach-response-obligations-effective-november-1-2018
- GDPR. (2016). *General conditions for imposing administrative fines.* Retrieved from General Data Protection Regulation.
- Gemalto. (2018). *Breach Level Index.*
- Government of Canada. (2019). *Proposals to modernize the Personal Information Protection and Electronic Documents Act.*
- Hayashi, H., & Yukawa, M. (2020). *Japan: Data Protection Laws and Regulations 2020.*
- IBM Security / Ponemon Institute. (2019). *Cost of a Data Breach Report.*
- Innovation, Science and Economic Development Canada. (2019). *Canada's Digital Charter in Action: A Plan by Canadians, for Canadians.*
- Irdeto. (2019). *Irdeto Global Connected Industries Cybersecurity Survey: IoT cyberattacks are the norm, the security mindset isn't.*
- Jia, J., & Wagman, L. (2020). *The One-Year Impact of the General Data Protection Regulation (GDPR) on European Ventures.*
- Morgan, C., Glover, D., Scherman, M., & Chen, E. Y. (2020, June 24). *Amendments to Ontario's health information legislation bring new obligations and penalties.* Retrieved from Mondaq: https://www.mondaq.com/canada/privacy-protection/957346/amendments-to-ontario39s-health-information-legislation-bring-new-obligations-and-penalties

- Office of the Australian Information Commissioner. (2018, April 9). *OAIC Guide to Privacy Regulatory Action.* Retrieved from McCullough Robertson: https://www.mccullough.com.au/2019/04/09/its-no-secret-10-million-penalties-to-be-introduced-for-privacy-law-breaches/
- Office of the Privacy Commissioner. (2018, April 26). *Privacy guardians: Smart city initiatives must include privacy protections.* Retrieved from Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_180426/
- Office of the Privacy Commissioner of Canada. (2015). *Digital Privacy Act.*
- Office of the Privacy Commissioner of Canada. (2018). *Joint letter to the Minister of Infrastructure and Communities on Smart Cities Challenge.*
- Office of the Privacy Commissioner of Canada. (2019). *Personal Information Protection and Electronic Documents Act.*
- Office of the Privacy Commissioner of Canada. (2019). *Privacy Act.*
- Office of the Privacy Commissioner of Canada. (2020, May 7). *Office of the Privacy Commissioner of Canada.* Retrieved from Supporting public health, building public trust: Privacy principles for contact tracing and similar apps: https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/
- Pearson, J. (2019, April 17). *Canada is Getting Sued Over Sidewalk Labs' 'Smart City' In Toronto.* Retrieved from Vice News: https://www.vice.com/en_us/article/gy4bgj/canada-is-getting-sued-over-sidewalk-labs-smart-city-in-toronto
- Rotenberg, M. (2016). *Promoting innovation, protecting privacy.* Retrieved from OECD Observer: https://oecdobserver.org/news/fullstory.php/aid/5593/Promoting_innovation,_protecting_privacy.html
- Schwartz, P. M., & Peifer, K.-N. (2017, November 7). Transatlantic Data Privacy. *Georgetown Law Journal*, pp. 115-179.
- Singer, N. (2018). What you don't know about how Facebook uses your data. *The New York Times*.
- Singer, N. (2020, July 8). *Virus-tracing apps are rife with problems. Governments are rushing to fix them.* Retrieved from The New York Times: https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html
- Statistic Canada. (2019). Police-reported cybercrime, by cyber-related violation.
- Statistics Canada. (2017). Profile of Canadian Businesses who Report Cybercrime to Police.
- Statistics Canada. (2019). Table: 14-10-0068-01.
- Tehrani, M., Oates, C., Kappler, J., & Matziorinis, P. (2020, June 24). *Quebec to introduce the most punitive privacy laws in Canada - with fines of up to $25 million.* Retrieved from Mondaq: https://www.mondaq.com/canada/privacy-protection/956848/quebec-to-introduce-the-most-punitive-privacy-laws-in-canada--with-fines-of-up-to-25-million
- UNCTAD. (2016). *Data protection regulations and international data flows: Implications for trade and development.* New York and Geneva: United Nations Publication.
- UNCTAD. (2020, February 4). *Data Protection and Privacy Legislation Worldwide*. Retrieved from United Nations Conference on Trade and Development: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
- USMCA. (2020). *United States-Mexico-Canada Agreement Digital Trade Chapter.*
- Verizon. (2020). *Data Breach Investigations Report.*
- Ybarra, M. (2015). FBI admits no major cases cracked with Patriot Act snooping powers. *The Washington Times*.


HUAWEI
Roland
Berger