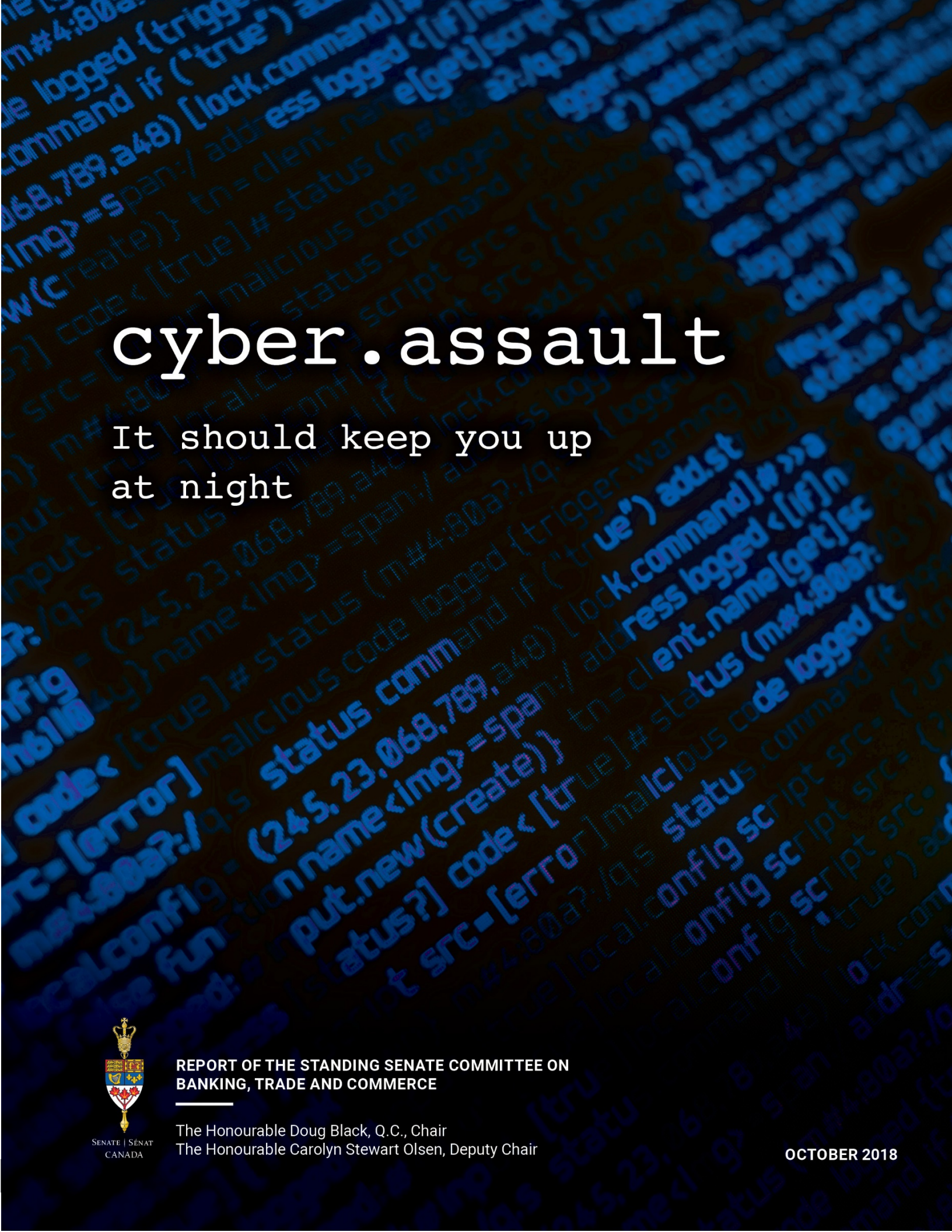


cyber.assault

It should keep you up at night

SENATE | SÉNAT CANADA

REPORT OF THE STANDING SENATE COMMITTEE ON BANKING, TRADE AND COMMERCE

The Honourable Doug Black, Q.C., Chair
The Honourable Carolyn Stewart Olsen, Deputy Chair

OCTOBER 2018

For more information please contact us:
by email: *BANC@sen.parl.gc.ca*
by mail: The Standing Senate Committee on Banking, Trade and Commerce
Senate, Ottawa, Ontario, Canada, K1A 0A4
This report can be downloaded at: *www.senate-senat.ca/*
The Senate is on Twitter: @SenateCA,
follow the committee using the hashtag #BANC

Ce rapport est également offert en français

TABLE OF CONTENTS

COMMITTEE MEMBERSHIP

The Honourable Senator Doug Black, Q.C., *Chair*
The Honourable Senator Carolyn Stewart Olsen, *Deputy Chair*

The Honourable Senators

Jean-Guy Dagenais
Joseph A. Day
Colin Deacon
Pierrette Ringuette
Scott Tannas
David Tkachuk
Pamela Wallin
Howard Wetston

Ex-officio members of the committee:

The Honourable Senators Peter Harder, P.C., Diane Bellemare, Grant Mitchell, Larry W. Smith, Yonah Martin, Joseph A. Day, Terry M. Mercer, Yuen Pau Woo and Raymonde Saint-Germain.

Other senators who have participated in the study:

The Honourable Senators Pierre-Hugues Boisvenu, Larry W. Campbell, Claude Carignan, P.C., Tobias Enverga, Jr., Stephen Greene, Michael L. MacDonald, Ghislain Maltais, Elizabeth Marshall, Sabi Marwah, Paul J. Massicotte, Lucie Moncion and Betty Unger.

Parliamentary Information and Research Services, Library of Parliament:

Adriane Yong, Analyst
Brett Stuckey, Analyst

Senate Committees Directorate:

Lynn Gordon, Clerk of the Committee
Kalina Waltos, Administrative Assistant

Senate Communications Directorate:

Stav Nitka, Communications Officer
Marcy Galipeau, Communications Officer

ORDER OF REFERENCE

Extract from the *Journals of the Senate*, Tuesday, October 17, 2017:

The Honourable Senator Day moved, seconded by the Honourable Senator Eggleton, P.C.:

That the Standing Senate Committee on Banking, Trade and Commerce be authorized to study and report on issues and concerns pertaining to cyber security and cyber fraud, including:

- cyber threats to Canada's financial and commercial sectors;
- identity theft, privacy breach and other fraudulent activities targeting Canadian consumers and small businesses;
- the current state of cyber security technologies; and
- cyber security measures and regulations in Canada and abroad.

That the committee submit its final report no later than Friday, June 29, 2018, and that the committee retain all powers necessary to publicize its findings until 180 days after the tabling of the final report.

The question being put on the motion, it was adopted.

Clerk of the Senate

Nicole Proulx

Extract from the *Journals of the Senate*, Tuesday, June 5, 2018:

The Honourable Senator Black *(Alberta)* moved, seconded by the Honourable Senator McPhedran:

That, notwithstanding the order of the Senate adopted on October 17, 2017, the date for the final report of the Standing Senate Committee on Banking, Trade and Commerce in relation to its study on issues and concerns pertaining to cyber security and cyber fraud be extended from June 29, 2018 to November 30, 2018.

The question being put on the motion, it was adopted.

Clerk of the Senate

Richard Denis

LIST OF RECOMMENDATIONS

The committee recommends that:

1. All levels of government prioritize cyber security education in their cyber security strategies. To achieve this, the federal government should enable and fund:

    Cyber security skills training programs, in collaboration with the provinces, territories and municipalities, to assist businesses with their cyber security needs;

    Three national centres of excellence in cyber security research in order to promote basic research in the science of cyber security at the university level and to encourage Canadians to pursue education and careers in cyber security-related fields, with the goal of doubling the number of graduates with cyber security expertise in the next four years; and

    A national cyber literacy program, led by the Canadian Centre for Cyber Security, to educate consumers and businesses on how to become cyber resilient. The program should promote awareness of the importance of cyber security needs at the junior and senior high school levels and encourage further education in science, technology, engineering and mathematics programs.

2. The federal government develop standards to protect consumers, businesses and governments from threats related to the Internet of Things devices.

3. The federal government develop a rapid and responsive national cyber security information sharing framework and make any necessary legislative changes to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to allow information sharing about cyber threats within the private sector and between the private sector, government and relevant international organizations.

4. The federal government identify any deficiencies in information sharing and determine how law enforcement agencies can be provided with the necessary tools to actively and quickly share information and work with other jurisdictions in the prosecution of cyber criminals.

5. The federal government develop a consistent set of leading cyber security standards that are harmonized with the highest international standards and would apply to all entities participating in critical infrastructure sectors.

6. The federal government provide incentives for all businesses, particularly those in critical infrastructure sectors, to improve their cyber security practices, such as allowing accelerated capital cost allowance deductions to companies under the *Income Tax Act* for investments in cyber security.

7. The federal government modernize Canada's privacy legislation to take into account emerging cyber security concerns and international standards. It should provide the Office of the Privacy Commissioner with new resources to carry out its mandate and provide the Commissioner the power to make orders and impose fines against companies that have failed to take adequate measures to protect customers' personal information.

8. The federal government create a new federal minister of cyber security. This minister would be responsible for cyber security policy, including the national cyber security strategy, and have oversight over the new Canadian Centre for Cyber Security and the National Cybercrime Coordination Unit.

   Until the minister of cyber security is created, the person designated as the federal lead for cyber security should report directly to the Prime Minister on these matters.

   Lastly, the Prime Minister should table an annual report to Parliament on issues related to Canada's cyber security strategy.

9. The federal government create a federal expert task force on cyber security to provide recommendations regarding the national cyber security strategy that would establish Canada as a global leader in cyber security.

10. The federal government require its departments and agencies to report privacy breaches to the Office of the Privacy Commissioner.

    and

    The federal government continue to implement best practices for the federal public service to ensure that properly secured devices are used to protect sensitive information.

INTRODUCTION

Cyber attacks are in the headlines on a weekly, if not daily, basis. Companies operating around the world are hesitant to reveal — sometimes months or years later — that they were the victim of a cyber attack, and that the personal information that was given to them by Canadians in trust may now be in the hands of criminals.

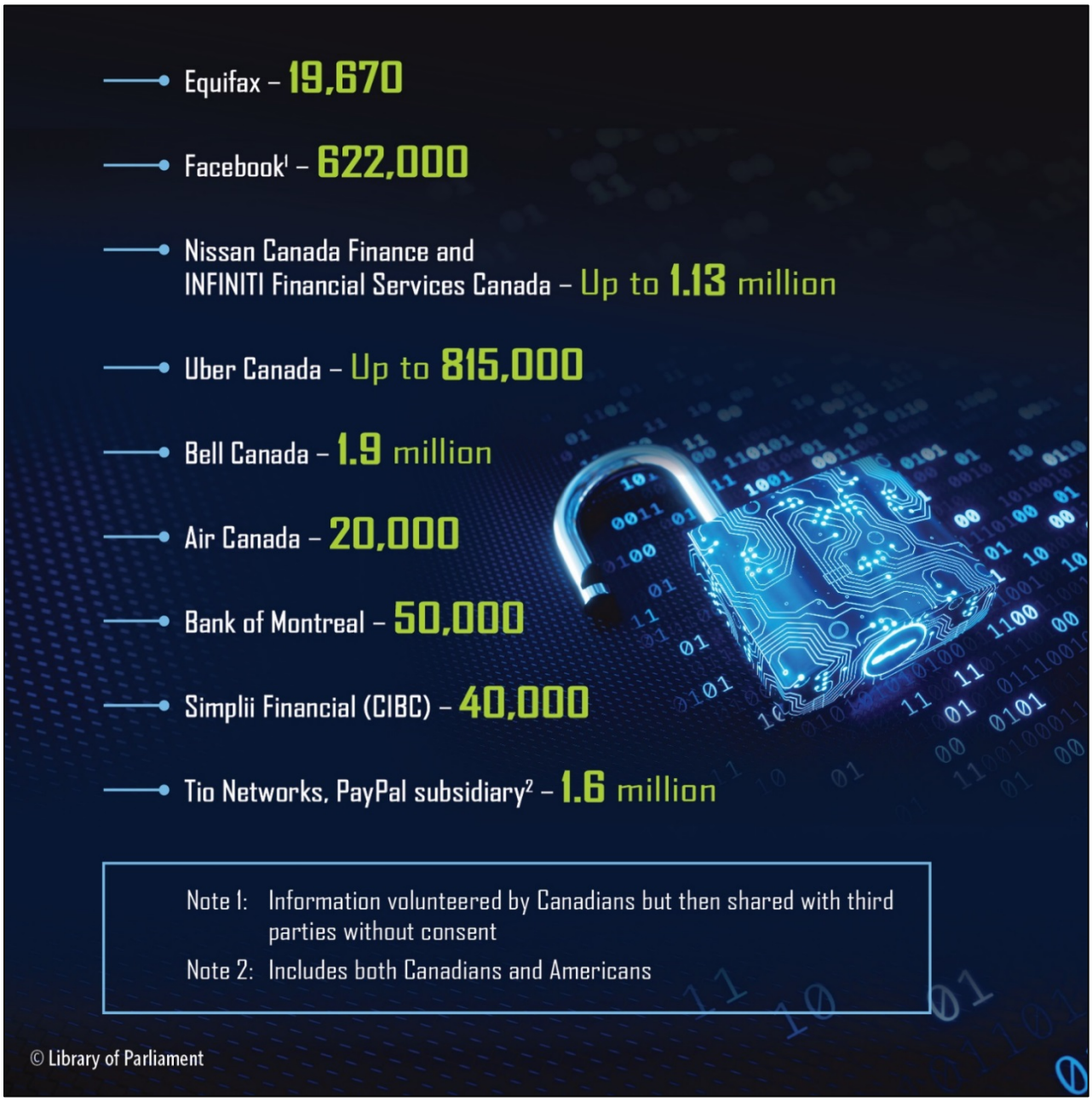
> ***…Over a 25- to 30-year period, we moved almost everything we value in the west from analogue form — books and papers — to digital form, and then connected it through an internet protocol — TCP-IP — that was never designed for security. We did so without properly calculating the risk that would come from making that move as terrorists, crooks, spies and nation states moved to exploit this now digitally stored information that's connected through the internet.***
>
> *John P. Carlin, Chair, Morrison & Forester LLP, 22 March 2018.*

In undertaking a study on cyber security, the Standing Senate Committee on Banking, Trade and Commerce (the committee) was originally focused on the cyber attacks that resulted in the compromise of Canadians' financial data, but we became increasingly concerned about constantly evolving cyber risks that affect all sectors of society, particularly Canada's critical infrastructure sectors.

In 2017, 19,700 Canadians had their personal financial data stolen in a cyber security breach of Equifax — a company that collects sensitive credit history data and even offers identification theft services. Equifax admitted that hackers stole the personal information of 145.5 million mostly-American consumers. A year later, hackers were able to steal the personal financial information of 90,000 Bank of Montreal and Simplii Financial (CIBC) customers and threatened to make the information public.

While some progress has been made federally in the past year, there is much more that the federal government and Canadians must do to protect ourselves. We must take the appropriate steps now, or soon we will all be victims.

Figure 1: Number of Canadians affected by Recent Privacy Breaches



Source: Data compiled by authors from various sources

Figure 2: Number of Victims of Cyber Crime in 2017, selected countries

Source: Norton by Symantec, 2017 Norton Cyber Security Insights Report Global Results, p. 11

Over the course of nine meetings, the heard testimony from representatives from government departments and agencies, the Office of the Privacy Commissioner of Canada, the legal community, academia, the financial sector and other business groups to learn about Canada's approach and attitude towards cyber security and the measures that need to be taken to improve cyber security in Canada.

Do you think you are cyber secure? Take this quiz and see if you recognize cyber risks.

Several important issues were identified by witnesses.

Investments in cyber security education was highlighted by several witnesses as a necessity to address the shortage of cyber security professionals and to help Canadians become aware of the risks of Internet-connectivity. Consequently, how to effectively educate Canadians about cyber security forms the basis for the main recommendation of this report.

We were particularly disheartened to learn that, other than suing the company that was hacked, Canadian consumers generally have few options for recourse when their personal information is stolen. It was noted that:

> When a business is hacked, the RCMP will conduct an investigation to determine the identity of the cyber attacker, but the loss of customers' personal information is considered to be a breach of contract by the business, and not necessarily a crime that would be investigated by law enforcement. Often the personal information that is lost is not even shared with law enforcement agencies. Therefore, when notified of a data breach, it is up to individual Canadians to take steps to determine if their information is being used by cyber criminals, as there is no mechanism to help them.
>
> Examining cyber security requires an understanding of Canada's privacy laws. The Office of the Privacy Commissioner oversees compliance with Canada's two federal privacy statutes, the *Privacy Act,* which regulates personal information held by federal government departments and agencies and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which governs the personal information collected by many Canadian businesses from their customers. Individuals can contact the Privacy Commissioner to make privacy complaints; however, the Privacy Commissioner does not have power to make companies comply with PIPEDA or impose fines.

It was also alarming to hear that the Royal Canadian Mounted Police (RCMP) may not have the capacity to commence any new investigations into major cyber threats. The RCMP also commented that:

> The multiple avenues by which cyber crimes are reported in Canada causes confusion and underreporting among Canadians. Underreporting leads to an inability of law enforcement to conduct a comprehensive analysis of cyber crimes and impedes a coordinated response, domestically and across national jurisdictions.

Witnesses also emphasized the importance of protecting Canada and the world's critical infrastructure systems and the challenges businesses face in protecting their networks. They warned that:

> In Canada, there are ten critical infrastructure sectors. All sectors are connected to the Internet and are highly dependent on each other. Representatives from the financial sector noted their concern regarding differences in cyber security standards across the sectors. They also questioned whether it was wise to allow smaller companies with less resources and potentially lower cyber security standards, such as fintech companies, to gain access to Canada's financial systems and data.
>
> In general, businesses do not invest enough in cyber security because cyber breaches have minimal long-term effects on stock prices or consumers' behaviour.
>
> There is a global shortage of cyber security professionals, and Canadian companies are looking outside of Canada for expertise in cyber security.

Regarding Canada's national cyber security strategy and national security, witnesses said that:

> The federal government provided funding through the 2018 federal budget to revamp Canada's national cyber security framework and create the Canadian Cyber Security Centre, located within the Canadian Security Establishment, and the National Cybercrime Coordination Unit, situated within the RCMP. These two new entities will work with the Department of Public Safety and Emergency Preparedness, which remains responsible for national coordination and policy. A new National Cyber Security Strategy was also introduced by the federal government in June 2018.

Figure 3: Canada's Ten Critical Infrastructure Sectors

- Health
- Food
- Finance
- Water
- Information and Communication Technology
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

Countries such as the United States, the United Kingdom, Australia, Israel, the Netherlands and Singapore were mentioned to have prioritized cyber security in terms of its importance in relation to the economy and research and development.

Rather than just defending against cyber attacks, governments are using offensive cyber operations that interfere with foreign countries, critical infrastructure institutions and businesses. As cyber attacks are considered a global problem, global surveillance is required.

Canadians need to know that cybersecurity is a serious problem — people are failing to protect themselves from current and emerging cyber threats. All Canadians must take action to protect the country before cyber criminals are able to infiltrate critical systems and orchestrate a technological catastrophe in Canada.

EDUCATING CANADIANS ABOUT CYBER SECURITY AND RESILIENCE

It was made clear that more cyber security education is needed in Canada. According to the Office of the Superintendent of Financial Institutions, "cyber resilience" refers to an institution's ability to anticipate, withstand, contain and rapidly recover from a cyber attack before it compromises operations or harms its customers. Becoming cyber resilient is a joint responsibility for governments, private sector and consumers as they all play a role in protecting key networks from long-term cyber threats.

> ***There [should be an] awareness for security where you understand that there is a need for security, that you have to protect your private data, that you decide what you want to share with Facebook and if you decide what you share, what that means and implies to your data. These kinds of decisions need to be understood, probably even earlier than high school***
>
> *Cybersecurity and Privacy Institute, University of Waterloo, 21 March 2018*

One of the three themes of Canada's 2018 national cyber security strategy is "cyber innovation," which includes "support for advanced research and developing cyber skills and knowledge." The committee proposes that this theme become the priority of the strategy and offers a three-pronged approach to enhance cyber security education and the importance of cyber resilience in Canada while balancing the need to support and promote innovative technologies and opportunities: developing skills, supporting research and development, and educating the general public and businesses.

First, skills training in cyber security is needed as there is a global shortage of cyber security professionals. The committee's approach to skills development would have the federal government consult with the private sector and the provinces and territories to develop national skills training programs in cyber security to help businesses address their short-term cyber security needs. These types of programs could include retraining options for current employees, management level programs that focus on risk assessment or ways to retain skilled cyber security professionals, and co-op placements for high school and university students in cyber security or computer firms to learn about cyber security fields. Canadian businesses need help now and this requires investments in skills training.

Second, the federal government needs to fund basic research in the science of cyber security. Basic scientific and technological research is required in order to answer essential cyber security questions – such as what it means to be "secure." Once these principles have been established, cyber security experts can determine the best practical solutions to improve Canada's cyber standards and operations.

Building Canada's talent pool requires improved educational options for careers in cyber security, retraining options for the existing workforce, mature career development management practices and creative cross-pollination with high-demand disciplines that are closely linked to cyber security.

Canadian Bankers Association, 26 October 2017

Some countries have already made progress with respect to developing both research and expertise in the cyber security field. For example, the United States' National Security Agency has designated certain academic programs at various U.S. colleges and universities as National Centers of Academic Excellence in Cyber Operations or Cyber Defense. The purpose of these designations is to promote higher education and research in cyber defense and security and to produce cyber professionals capable of supporting the private sector or government.

Germany has established the Helmholtz Association of German Research Centers, which conduct research on various scientific and technological fields. Opened in December 2017, the Center for IT-Security, Privacy and Accountability – Helmholtz Center (i.G.) GmbH, known as CISPA, will have over 500 researchers examining the important cyber security and privacy research challenges of a digital society.

Canada has the Networks of Centres of Excellence program, through which the Smart Cybersecurity Network (SERENE-RISC) receives funding. However, in order to stay relevant and competitive with other countries, the federal government needs to create and provide adequate funding for national centres of excellence specifically for basic cyber security research. Three centres of excellence should be established: the Canadian Institute for Cybersecurity at the University of New Brunswick, the Cybersecurity and Privacy Institute at the University of Waterloo, a third located in Western Canada. Having a designation as a centre of excellence will encourage other Canadian universities to establish similar programs. These university programs will attract students from around the world, assisting them in developing the skills and expertise in cyber security that is desperately needed in both the private and public sectors in Canada. The goal is to increase the number of graduates with cyber security expertise by 100%.

The Internet and other online systems have allowed criminals and other actors to remove the personal interaction elements, and some of those personal communication skills that we see that people use to identify when a threat is present and when a threat is not present.

Royal Canadian Mounted Police, 18 October 2017

Third, the committee suggests the federal government focus on ways to effectively educate the general public and businesses on cyber security and cyber resilience. Ordinary citizens and small businesses are targets of online scams, such as phishing attacks and malware, and most do not know how to deal with these threats, who to contact when they happen or how to protect themselves from further attacks.

A national cyber literacy strategy, similar to Canada's financial literacy strategy that is overseen by the Financial Consumer Agency of Canada, would help ensure that all Canadians have the knowledge and tools required to defend themselves from current and future threats. The cyber literacy strategy should be led by the new Canadian Centre for Cyber Security and developed in conjunction with the provinces and territories, as well as

Figure 4: Tips for Consumers to Protect their Personal Information

1. Think twice before sharing personal data online or in person.
2. Ask questions about a company's privacy policies with respect to customers' information.
3. Speak up and let a company know if you are concerned about how your personal information is being handled.
4. Just say no when asked for personal information by a company and subscribe to do not call or do not mail lists.
5. Safeguard your social insurance number as it is confidential personal information that should only be shared for income reporting purposes.
6. Protect your devices with passwords, anti-virus, anti-spam and firewall programs and consider encrypting sensitive data and shutting off Wi-Fi and Bluetooth when they are not being used.
7. Protect your passwords by making them difficult to guess and use different passwords for different accounts, websites and devices.
8. Get to know the privacy settings of your devices, browsers, websites, apps and cameras and adjust them regularly.
9. Properly discard data stored on devices that are no longer being used or are being sold or recycled.
10. Know your privacy rights under Canada's federal and provincial privacy laws.

Source: Office of the Privacy Commissioner of Canada, 10 Tips for Protecting Personal Information

stakeholders such as financial institutions and cyber security firms that would play a role in working directly with Canadians that are victims of a cyber attack. It should focus on how to effectively educate Canadians at all levels of computer literacy and what tools the federal government could provide to individuals and businesses to secure their computers, networks and systems.

Because of their use of social media and other digital technologies at a very young age, it is important that Canada's youth becomes aware of online risks long before they reach university. As part of the cyber literacy strategy, this awareness should be introduced at the junior and senior high school levels, in conjunction with encouragement to pursue further education in science, technology, engineering and mathematics. The federal government needs to work with the provinces and territories so that their school curriculums reflect these goals.

By having these discussions in high school, young Canadians can learn to protect themselves and their families from cyber threats, adopt good cyber security practices and consider career opportunities in computer science and cyber security.

Therefore, the committee recommends that:

All levels of government prioritize cyber security education in their cyber security strategies. To achieve this, the federal government should enable and fund:

Cyber security skills training programs, in collaboration with the provinces, territories and municipalities, to assist businesses with their cyber security needs;

Three national centres of excellence in cyber security research in order to promote basic research in the science of cyber security at the university level and to encourage Canadians to pursue education and careers in cyber security-related fields, with the goal of doubling the number of graduates with cyber security expertise in the next four years; and

A national cyber literacy program, led by the Canadian Centre for Cyber Security, to educate consumers and businesses on how to become cyber resilient. The program should promote awareness of the importance of cyber security needs at the junior and senior high school levels and encourage further education in science, technology, engineering and mathematics programs.

Figure 5: Keeping Personal Information Private

Source: prepared by authors

ENHANCING CANADA'S CYBER SECURITY STRATEGY

In addition to prioritizing cyber security education, witnesses made other suggestions to improve Canadians' cyber security practices, including making consumers aware of the risks associated with the Internet of Things, assisting Canadian businesses with their cyber security needs and in complying with privacy laws, and making changes to the national cyber security framework.

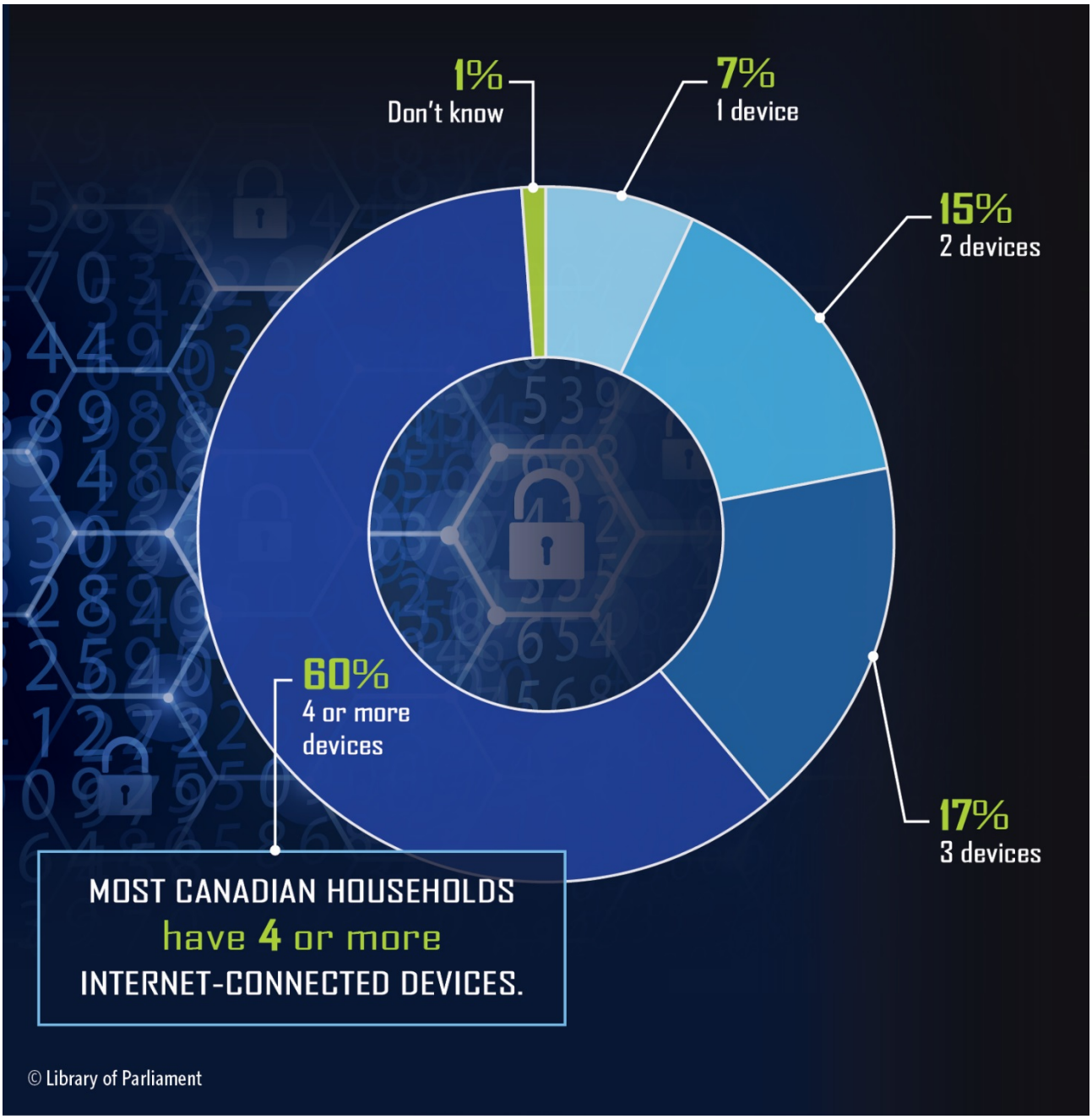
A. Making consumers aware of the risks associated with the Internet of Things

Witnesses spoke with concern about the growing network of Internet-connected devices on the market – otherwise known as the Internet of Things – and the risks these devices pose to consumers. The Internet of Things is much more than household devices such as baby monitors, fridges, and thermostats. It includes sensors on the roads, autonomous vehicles, machines with artificial intelligence capabilities and has become a driving factor for change for many businesses. While these devices have made life more enjoyable and convenient for Canadian consumers, this convenience comes with substantial cyber security risks as these devices are not being designed with security as a priority.

As seen in Figure 6, over half of Canadian households have 4 or more Internet-connected devices, and each of these devices could potentially serve as a target for cyber criminals.

> ***One of the things I think we should probably have a larger conversation about is the Internet of things, or the Internet of everything, as some companies have characterized it, where you have billions of devices being deployed – some of them in the homes, some of them artificial intelligence, or at least machine learning – that are not necessarily designed with security in mind. I think that's one of the bigger challenges we're going to see in the next 10 years.***
>
> *Canadian Chamber of Commerce,* 1 March 2018

Figure 6: Number of Internet-connected devices in Canadian households, 2017



Source: Canadian Internet Registration Authority, 2018 Canada's Internet Factbook, p. 13

Recent examples show that Internet-connected devices that are vulnerable to cyber attacks could have enormous impacts on consumers' safety. In 2015, it was proven that certain Jeep models could be hacked through the entertainment system and could result in the hacker being able to control the braking and steering systems of the car. Jeep had to recall 1.4 million cars. In 2017, the U.S. Food and Drug Administration recalled almost half

a million pacemakers over concerns that they could be hacked if proper updates were not installed.

The federal government needs to consider how these devices should be secured before they are introduced to the market. Should all devices be encrypted? Should there be multiple levels of security? How will the devices be provided with updates? Should the government certify devices that have adequate cyber security?

> ***One of the objectives of state-sponsored cyber-activity is to obtain information which will give foreign companies a competitive edge over Canadian firms. This can have a negative impact on investment or acquisition negotiations involving Canadian companies and the Government of Canada, and, in turn, lead to lost jobs, revenue, and market share. Ultimately, cyber-espionage negatively impacts Canada's economy as a whole.***
>
> *Canadian Security Intelligence Service,* 18 October 2017

If these devices are intended to be deployed into critical infrastructure systems, other considerations could include the type of testing that should be done to ensure they are cyber secure and whether these devices could be used for cyber espionage.

These are just some of the issues that the federal government must study to determine what types of standards should be developed to protect Canadians' devices and critical infrastructure from cyber threats.

Consequently, the committee recommends that:

> **The federal government develop standards to protect consumers, businesses and governments from threats related to the Internet of Things devices.**

B. Assisting Canadian businesses and ensuring compliance with privacy laws

The private sector plays a significant part of Canada's cyber security strategy. Businesses are the providers of critical infrastructure services and thus key targets for domestic and state-sponsored cyber criminals. They also collect vast amounts of consumer information, and therefore need to protect both their databases and any networks to which they are connected from cyber threats. The committee is especially concerned about the smaller firms that operate within Canada's ten critical infrastructure sectors. Unlike the federal government and large businesses such as banks, these companies generally do not have the resources to effectively protect their systems.

While addressing the shortage of cyber professionals through education will meet the long-term cyber security needs of businesses, more can be done to meet the short and medium-term cyber security concerns of the private sector and to safeguard the economy at large.

1. Allowing information sharing among the private sector and governments

Cyber attacks spread quickly, and governments will often need to share information and intelligence with other countries to stop an attack. Similarly, the interconnectedness of the world's critical infrastructure networks might require the swift sharing of consumer data to effectively respond to a threat. There is a need for the government and the private sector to coordinate their efforts to rapidly respond to cyber attacks, which could involve sharing sensitive and confidential information. However, information sharing can be difficult since government information may be classified and companies can only share limited or very general information about selected types of cyber crimes with other businesses or with their customers.

> ***There are several reasons why sharing cyber-threat information is important. Sharing leverages the knowledge of others and makes the cost of an attack more expensive. It enriches the cyber threat information held by companies, making it more actionable. Timely, actionable information provides the means to harden cyber defences.***
>
> *Canadian Cyber Threat Exchange,* 1 March 2018

The federal government should examine initiatives put forth by organizations such as the Canadian Cyber Threat Exchange that allow businesses to share information about cyber threats and cyber security practices in a secure environment with other businesses, government and research institutions, with the goal of developing a national information-sharing framework to combat cyber threats. This framework would set out the parameters for sharing information between private sector businesses, government and other relevant international organizations. Privacy legislation should also be re-examined to determine how information sharing can be facilitated while still respecting the privacy rights of Canadians.

There is a clear need for public/private coordination in responding to attacks against critical infrastructure and a single clear point of contact in the public sector for chief information security officers in the private sector. These improvements will help us better share information in a protected fashion and will help us manage and prevent future attacks.

Payments Canada, 28 February 2018

Therefore, the committee recommends that:

> **The federal government develop a rapid and responsive national cyber security information sharing framework and make any necessary legislative changes to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to allow information sharing about cyber threats within the private sector and between the private sector, government and relevant international organizations.**

Information sharing can not only help as a preventative measure against cyber threats, but it is also necessary when trying to prosecute these crimes. As cyber criminals can perpetrate their crimes from any location in the world and have multiple concurrent targets, prosecuting these crimes can be a significant challenge. It was noted that it is not often practical to request information through international agreements, such as the Mutual Legal Assistance Treaty, as it can take more than a year to process these types of requests. More needs to be done to support law enforcement agencies in investing and prosecuting these types of crimes, including studying whether any changes to Canadian legislation needs to be made to allow a relatively quick sharing of information with law enforcement in other jurisdictions.

As such, the committee recommends that:

> **The federal government identify any deficiencies in information sharing and determine how law enforcement agencies can be provided with the necessary tools to actively and quickly share information and work with other jurisdictions in the prosecution of cyber criminals.**

2. Introducing consistent cyber security standards across sectors and jurisdictions

> ***Companies frequently confront an expanding and overlapping set of sound regulations in different jurisdictions. Those need to be harmonized using a baseline framework.***
>
> MasterCard, *1 March 2018*

Having consistent and harmonized cyber security standards across sectors and ideally countries was mentioned several times as one important way to slow the spread of a cyber attack.

A uniform set of cyber security standards would be particularly important when considering standards for the critical infrastructure sectors. Having cyber security standards that are consistent would help the government in its oversight of cyber security for these sectors and would provide consumers with confidence that these systems are protected.

Some witnesses suggested that minimum cyber security standards be extended to include all companies operating within a critical infrastructure sector. For example, with respect to the financial sector, it was noted that while banks have the knowledge and experience in combatting cyber security attacks, new entrants into the sector, such as fintech companies, may have less stringent cyber security practices, thus making them a vulnerability for the sector. However, the recent cyber attacks on the Bank of Montreal and Simplii Financial, a subsidiary of Canadian Imperial Bank of Canada, show that even those companies that are highly regulated and have arguably the best cyber security defences against attacks, have their weaknesses. As a result, the committee is of the view that minimum cyber security standards should be developed and applied to all entities within the critical infrastructure sectors.

Guidance for these standards can be found in countries that were highlighted as leaders in cyber security. In particular, the European Union's General Data Protection Regulation (GDPR) and the United States' National Institute for Standards and Technology were mentioned by witnesses: the GDPR for its privacy rules in relation to data capture, storage, usage, and sharing by companies and the National Institute for Standards for its technological expertise.

> ***The high degree of interconnectedness between institutions means a single attack against a financial institution could spread to the broader financial system. As a result, cyber threats have become a key vulnerability that both financial system participants and regulators will have to confront for a long time to come.***
>
> *Bank of Canada, 28 February 2018*

> ***The growing global reach of financial service providers, be they major financial institutions or an Internet-based money service provider, means one weak link in the chain can import risk into the broader financial system if not well governed and coordinated.***
>
> *Department of Finance Canada, 28 February 2018*

Therefore, the committee recommends that:

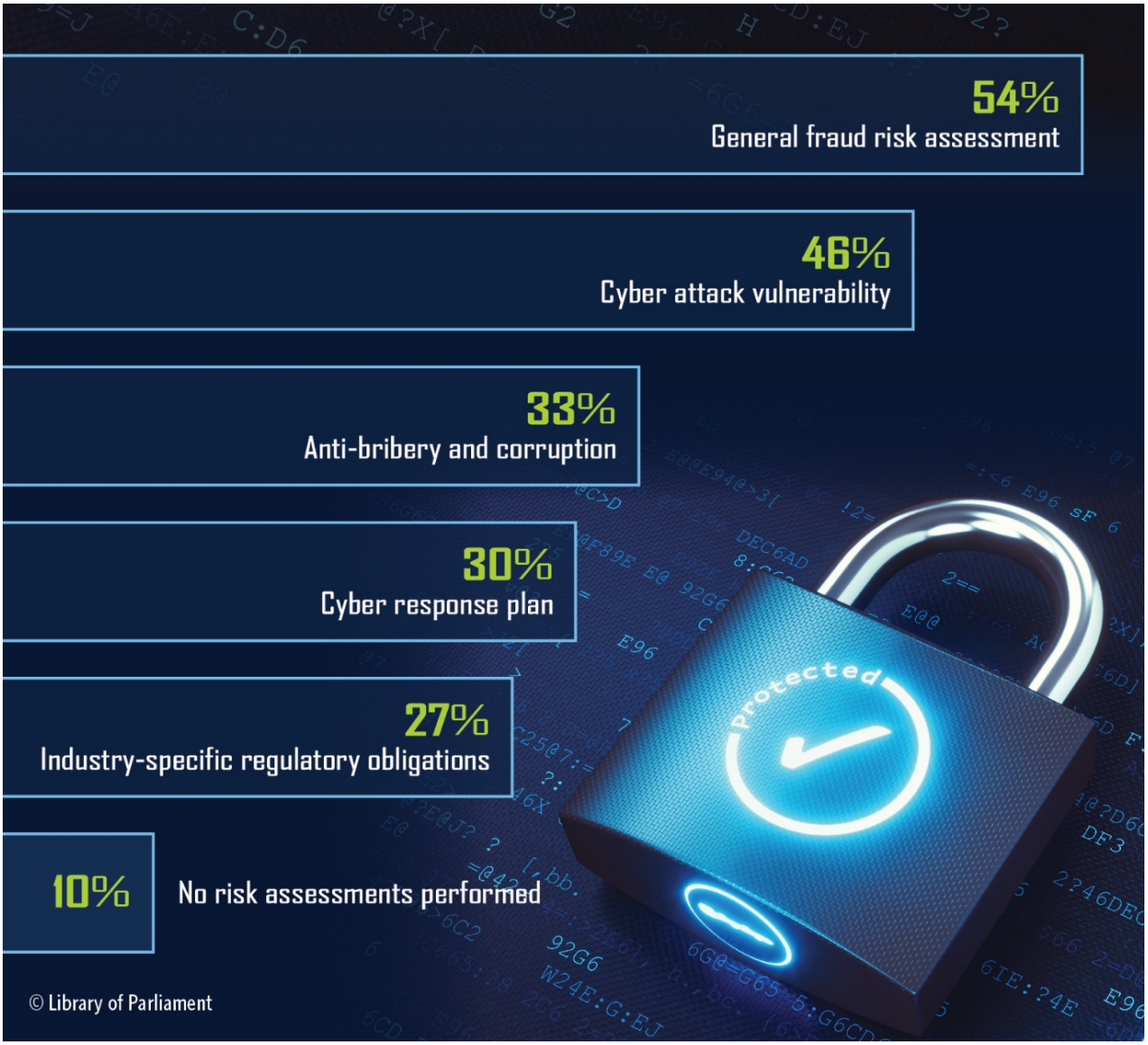
> **The federal government develop a consistent set of leading cyber security standards that are harmonized with the highest international standards and would apply to all entities participating in critical infrastructure sectors.**

3. Providing businesses with tax incentives to invest in cyber security

Despite there being a need in the private sector for more cyber security professionals, it appears that businesses are reluctant to invest in improving their cyber security practices if a cyber attack does not have long-term effects on stock prices or its consumers' behaviour. A 2017 survey by the Canadian Chamber of Commerce found that 64% of businesses surveyed had no intention of investing in cyber security measures at that time, with 55% of small businesses and 74% of micro-business not planning on making any cyber security training investments over a three-year period.

As noted in Figure 7, PricewaterhouseCoopers also found that only 46% of businesses participating in its global survey had conducted a cyber attack vulnerability risk in the past two years and only 30% had a cyber response plan in place.

Figure 7: Percentage of Companies that have conducted Specific Risk Assessments, 2016-2018, worldwide



Source: PricewaterhouseCoopers, Pulling fraud out of the Shadow – Global Economic Crime and Fraud Survey 2018, p. 7

In the committee's view, smaller companies that operate in the critical infrastructure sectors without adequate cyber security practices are cause for great concern. To assist these businesses, the federal government should decide whether it can provide support to the private sector for cyber security-related expenses, such as through accelerated capital cost allowance deductions for these expenses under the *Income Tax Act*.

Thus, the committee recommends that:

> **The federal government provide incentives for all businesses, particularly those in critical infrastructure sectors, to improve their cyber security practices, such as allowing accelerated capital cost allowance deductions to companies under the *Income Tax Act* for investments in cyber security.**

4. Ensuring businesses comply with Canadian privacy laws

Data has immense value and protecting this asset from cyber attacks should therefore be a key priority for any business as well as governments. The European Union's GDPR is considered to have the highest standards for data privacy legislation. It ensures that businesses comply with its rules by fining companies that do not comply up to 4 percent of annual revenue of 20 million €, whichever is higher.

> ***Cyber attacks can impact organizations of all sizes, potentially leading to significant privacy breaches. In the case of larger organizations, their substantial customer holdings may pose considerable interest for criminals. But in today's online economy, small and even micro organizations can also hold vast amounts of personal information or may be particularly vulnerable because they can be targeted as a prelude to attacks on larger or partner organizations.***
>
> *Office of the Privacy Commissioner of Canada, 2 November 2017*

Some changes were introduced to PIPEDA in 2015 to address the digital economy, such as mandatory data breach reporting by companies effective November 2018; however, the Privacy Commissioner indicated that his office was not given additional resources to deal with these reports. More recent parliamentary studies have determined that, in the age of quickly-advancing technology, Canada's privacy statutes may need to be re-examined and modernized. Recent reports of the House of Commons Standing Committee on Access to Information, Privacy and Ethics and the Senate Standing Senate Committee on Transport and Communications have made recommendations to the federal government to make amendments to Canada's privacy legislation in order to enhance cyber security for new technological devices and to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance.

The Office of the Superintendent of Financial Institutions expects the largest financial institutions to notify us when they observe a major cyber incident. These incidents should be reported even if they did not result in an observable cyber event, such as an online outage. We focus on major cyber incidents because they have the potential to disrupt the financial sector.

Office of the Superintendent of Financial Institutions, 28 February 2018

The committee agrees with these recommendations. Given today's digital economy, all businesses should understand the importance of protecting their systems and networks and that there are laws that require them to protect consumers' information. And when some businesses choose not to make their systems cyber secure, the federal government has to ensure that the Office of the Privacy Commissioner has the power and resources to make these businesses comply with the law.

Before we let consumers sue large companies on their own, which is not likely to be a fair fight, it could be helpful to send companies, large and small, clearer expectations and more specific guidelines on the levels of the security expected from them. At that point, if they do not implement the necessary measures, we could then eventually foresee penalties or allow lawsuits if we see that they have not done the basic minimum.

Smart Cybersecurity Network (SERENE-RISC), 19 October 2017

For those reasons, the committee recommends that:

The federal government modernize Canada's privacy legislation to take into account emerging cyber security concerns and international standards. It should provide the Office of the Privacy Commissioner with new resources to carry out its mandate and provide the Commissioner the power to make orders and impose fines against companies that have failed to take adequate measures to protect customers' personal information.

C. Improving Canada's cyber security framework

The federal government's 2018 National Cyber Security Strategy highlighted that the federal government will play a leadership role in advancing cyber security in Canada. Specifically, the strategy states that the federal government will establish a "clear focal point for cyber security," which will be the new Canadian Centre for Cyber Security established within the Communications Security Establishment.

Designating an agency as the cyber security lead within the federal government was a suggestion made to the committee by several witnesses, as, under the 2010 cyber security strategy, cyber security oversight was fragmented over several federal departments and agencies. While the 2018 strategy appears to consolidate some of the cyber security oversight responsibilities, it remains unclear which minister would act as lead, the Minister of Public Safety and Emergency Preparedness, who remains responsible for national cyber security policy, or the Minister of National Defence, which has oversight over the Communications Security Establishment.

> ***Stakeholders want the federal government to take a leading role domestically and internationally to foster collaboration among cyber security experts, drive investment in the cyber security industry, facilitate information sharing, and safeguard rights and freedoms in cyberspace.***
>
> *Department of Public Safety and Emergency Preparedness Canada, 21 March 2018*

The committee believes that more can be done to clarify the federal government's leadership role.

A new federal minister of cyber security should be created. This minister would take on some of the responsibilities currently held by the Minister of Public Safety and Emergency Preparedness and be responsible for all aspects of cyber security, from threats to national security and critical infrastructure to protecting Canadians online. The minister would be involved in coordinating cyber security efforts across provincial and territorial governments and with the private sector and consumers.

By consolidating operational cyber expertise from across the federal government under one roof, the new cyber centre will establish a single, unified Government of Canada source of unique expert advice, guidance, services and support on cyber security operational matters, providing Canadian citizens and businesses with a clear and trusted place to turn to for cyber security advice.

Canadian Security Establishment, 21 March 2018

It was pointed out that in countries that are considered leaders in cyber security, the head of state was the entity in charge of cyber security, with the office of the prime minister or president coordinating cyber security efforts. The reason that this approach seems to be effective is that cyber security touches all departments and agencies within the federal government and having leadership on the issue at the head of government ensures that it receives the attention that it deserves. The committee suggests that until a new minister is created, whichever entity is in charge of cyber security issues should report directly to the Prime Minister Office.

From this perspective, the committee recommends that:

> **The federal government create a new federal minister of cyber security. This minister would be responsible for cyber security policy, including the national cyber security strategy, and have oversight over the new Canadian Centre for Cyber Security and the National Cybercrime Coordination Unit.**
>
> **Until the minister of cyber security is created, the person designated as the federal lead for cyber security should report directly to the Prime Minister on these matters.**
>
> **Lastly, the Prime Minister should table an annual report to Parliament on issues related to Canada's cyber security strategy.**

Given the rapid development of technology and the types cyber attacks being committed, the new federal minister of cyber security should be advised by experts in cyber security. A task force should be commissioned, similar to the one created by the White House in 2016, that would provide recommendations to the minister about the national cyber security strategy, including how to strengthen Canada's digital economy through cyber security and how critical infrastructure networks and consumers can be protected.

Therefore, the committee recommends that:

> **The federal government create a federal expert task force on cyber security to provide recommendations regarding the national cyber security strategy that would establish Canada as a global leader in cyber security.**

One area of focus identified in the national cyber security strategy is the federal government's role in securing government systems from cyber attacks.

The federal government is not immune from cyber threats. Serious issues with cyber security have been discovered at various government departments and agencies, including the Canada Revenue Agency, Statistics Canada, the National Research Council, and Public Services and Procurement Canada. The Privacy Commissioner noted that the *Privacy Act* does not require federal departments and agencies to report privacy breaches to the Office of the Privacy Commissioner. In contrast, effective 1 November 2018, PIPEDA will require private sector companies to report a breach to the Privacy Commissioner and to notify customers if it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm" to its customers.

Given the amount of personal information collected by the federal government from Canadians, the Privacy Commissioner suggested that federal institutions be subject to the same legal reporting requirements as private sector companies when its data has been breached.

It was also proposed that the federal government put more effort in educating public servants and parliamentarians about the risks of using devices that connect to the Internet, particularly when travelling internationally. Best practices could be developed that would require government officials use different devices for different purposes. For example, when travelling internationally, an official should use a device that is more secure against cyber threats, even if the device is less convenient for the official.

The committee agrees that these measures will ensure that federal officials understand the importance of protecting government systems from cyber threats. Informing the Office of the Privacy Commissioner and the public of any data breaches within the government should be mandatory, as it will reveal how well our systems are protected against threats and will alert Canadians that their personal information may be in the hands of cyber criminals and take steps to protect themselves.

Consequently, the committee recommends that:

> **The federal government require its departments and agencies to report privacy breaches to the Office of the Privacy Commissioner.**

and

> **The federal government continue to implement best practices for the federal public service to ensure that properly secured devices are used to protect sensitive information.**

THE COMMITTEE'S CONCLUSIONS

With new technologies and applications forming the basis for Canada's new and future economy, the federal government must act now to educate Canadians about our shared role in protecting our country from constantly evolving cyber threats. Whether it be through learning new skills to work in the cyber security field, participating in cyber security research and development or simply becoming educated about how to keep personal information secure in cyberspace, each Canadian must learn how to do his/her part in combatting cyber crime.

Businesses hold vast amounts of personal information because customers trust them to keep it safe. They need to be informed of current and emerging cyber threats and learn how to best safeguard their systems. The Privacy Commissioner should have the power to ensure that failing to protect the personal information of Canadians has serious repercussions.

Lastly, government departments, agencies and systems are regularly being attacked by cyber criminals, and Canadians need to know when breaches occur. More needs to be done to make sure that Canadians know where to look for help in the face of a cyber attack. Creating a new minister of cyber security, supported by cyber security experts, would ensure this.

Cyber security has become a serious problem which can only be resolved if Canadians, businesses and governments work together to find solutions.

Cyber security and privacy, once issues only for technology experts, have become widespread concerns in business and society. Cyber security is no longer just an IT problem. It is a business problem; it is everyone's problem. The weakest link in cyber security is now people, not devices. As such, the human factor is considered the biggest threat to cyber safety.

Canadian Institute for Cybersecurity, University of New Brunswick, 29 March 2018

APPENDIX A: WITNESSES WHO APPEARED BEFORE THE COMMITTEE

October 18, 2017

Canadian Security Intelligence Service
Charles Lowson, Director General, Counter Intelligence and Counter Proliferation

Public Safety Canada
Adam Hatfield, Acting Director General, National Cyber Security Directorate

Royal Canadian Mounted Police
Chief Superintendent Scott Doran, Director General, Federal Policing Criminal Operations
Superintendent Mark Flynn, Director, Cybercrime, Federal Policing

October 19, 2017

Communications Security Establishment
André Boucher, Director General, Cyber Security Partnerships
Scott Jones, Deputy Chief, IT Security

Smart Cybersecurity Network (SERENE-RISC)
Benoît Dupont, Scientific Director

October 26, 2017

Canadian Bankers Association
Darren Hannah, Vice President, Finance, Risk and Prudential Policy
Andrew Ross, Director, Payments and Cyber Security
Sandy Stephens, Assistant General Counsel

November 2, 2017

Office of the Privacy Commissioner of Canada
Daniel Therrien, Privacy Commissioner
Brent Homan, Director General, Personal Information Protection and Electronic Documents Act Investigations Branch
Steven Johnston, Senior IT Research Analyst
Patricia Kosseim, Senior General Counsel and Director General, Legal Services, Policy, Research and Technology Analysis Branch

February 28, 2018

Bank of Canada
Ron Morrow, Managing Director, Financial Stability Department

Department of Finance Canada
Annette Ryan, Associate Assistant Deputy Minister, Financial Sector Policy Branch

Office of the Superintendent of Financial Institutions Canada
Judy Cameron, Senior Director, Legislation, Approvals and Strategic Policy
Theresa Hinz, Director, Approvals and Precedents

Payments Canada
Justin Ferrabee, Chief Operating Officer
Martin Kyle, Chief Information Security Officer

March 1, 2018
Canadian Cyber Threat Exchange
Robert W. Gordon, Executive Director

Mastercard
Ron Green, Chief Security Officer

The Canadian Chamber of Commerce
Scott Smith, Director, Intellectual Property and Innovation Policy

March 21, 2018
Communications Security Establishment
André Boucher, Associate Deputy Chief, IT Security

Cybersecurity and Privacy Institute (University of Waterloo)
Florian Kerschbaum, Interim Director

Public Safety Canada
Colleen Merchant, Director General, National Cyber Security Directorate

Royal Canadian Mounted Police
Chief Superintendent Jeff Adam, Acting Assistant Commissioner, Technical Operations

March 22, 2018
Morrison & Foerster LLP
John P. Carlin, Chair, Global Risk and Crisis Management

March 28, 2018
Canadian Institute for Cybersecurity (University of New Brunswick)
Ali Ghorbani, Director

APPENDIX B: WRITTEN SUBMISSIONS

Office of the Privacy Commissioner of Canada
Daniel Therrien, Privacy Commissioner