THE CANADIAN CHAMBER OF COMMERCE
LA CHAMBRE DE COMMERCE DU CANADA

The Voice of Canadian Business™
La porte-parole des entreprises Canadiennes^MD

Cyber Security in Canada:

Practical Solutions to a Growing Problem

April 2017

THE POWER TO SHAPE POLICY & OF OUR NETWORK

Get plugged in.

As Canada's largest and most influential business association, we are the primary and vital connection between business and the federal government. With our network of over 450 chambers of commerce and boards of trade, representing 200,000 businesses of all sizes, in all sectors of the economy and in all regions, we help shape public policy and decision-making to the benefit of all Canadians.

This report was made possible by the generous support of our sponsors

Title

AIMIA

CYBERNB
CYBERSECURITY EPICENTRE FOR CANADA

Deloitte.

Edelman

FASKEN MARTINEAU

Google

Grant Thornton
An instinct for growth™

intuit

LOCKHEED MARTIN

mcmillan
lawyers | mcmillan.ca

Symantec

Associate

Trisura Guarantee Insurance Company

TABLE OF CONTENTS

INTRODUCTION

In March of 2017, WikiLeaks released 8,761 classified CIA documents[1] that revealed many of the tools the Agency uses to exploit the vulnerabilities of everyday devices we all use—smartphones, smart TVs, telematics systems on vehicles. Putting aside the assumptions of what governments are up to, the more worrisome implications of this release is the fact that information about these vulnerabilities was not shared with the companies that make these products—their back doors remained open.

Wired magazine notes the CIA considers three things when assessing threats:

- Confidentiality means protecting and keeping your secrets. Espionage and data theft are threats to confidentiality.
- Availability means keeping your services running and giving administrators access to key networks and controls. Denial of service and data deletion attacks threaten availability.
- Integrity means assessing whether the software and critical data within your networks and systems are compromised with malicious or unauthorized code or bugs. Viruses and malware compromise the integrity of the systems they infect.[2]

This paper focuses on how business needs to be aware of this triad, how cyber security is a vital risk management exercise, how government can facilitate awareness and engagement, and the steps companies can take to protect themselves.

The digital marketplace is growing exponentially faster than the traditional economy. The global internet economy is estimated to be valued at $4.2 trillion in 2015.[3] Canada's GDP is $1.83 trillion, and the internet economy now accounts for 3.6%,[4] but this does not consider the value of data. The growth of the internet economy and the digitization of record keeping have fostered an increase in the number of cyber criminals attempting to steal data. Data has a black market value—about $1 for a credit card number or up to $10 for health information that can be used to steal an identity.[5]

1 https://wikileaks.org/ciav7p1/

2 www.wired.com/2015/12/the-cia-secret-to-cyber security-that-no-one-seems-to-get

3 Boston Consulting Group, The internet economy in the G20, 2015: www.bcg.com/documents/file100409.pdf

4 IBID

5 Reuters: www.reuters.com/article/2014/09/24/us-cyber security-hospitals-idUSKCN0HJ21I20140924

This black market value is now putting pressure on the Canadian economy and is hindering Canada's ability to compete globally. Denial of service attacks (botnets) are becoming alarmingly more frequent as the cost of acquiring customized software to conduct these attacks is just a few hundred dollars yet can have consequences costing millions. Cybercrime extracts 15-20% of the $3 trillion global internet economy, and Canada loses 0.17% of GDP to cybercrime, which is equal to $3.12 billion/year.[6]

The most obvious impact of cybercrime is the direct costs to business, such as financial loss due to fraud, loss recovery, loss of business (churn), reputational damage, infrastructure, training, monitoring and the potential for a conviction for a Personal Information Protection and Electronic Documents Act (PIPEDA) compliance failure, which can be up to $100,000 per record. But other societal costs, which can be more complicated to place a value on, include increased consumer prices, job losses, IP and innovation crises, loss of confidence, damage to critical infrastructure and breach of national security.

The Government of Canada has a clear role to play in promoting digital literacy, providing leadership (in partnership with the business community), establishing best practices for cyber resilience and building public trust and trust in the business community through a commitment to enforcement actions against cyber criminals.

Our objective with this report is to examine the Canadian cyber security landscape through various lenses (literature, quantitative analysis, workshops and roundtables), evaluate the feasibility and receptiveness of a national cyber security certification program and generate recommendations for federal government cooperation.

To achieve this objective, we took the approach of engaging businesses directly—hosting workshops in partnership with local chambers of commerce and roundtables with sponsors and CIOs, speaking at various events across the country, conducting a survey of our members and participating in a national thought leadership forum.

6 Intel Security, Net Losses – Estimating the Global Cost of Cybercrime: www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf

DEFINING "CYBER"

"Cyber" is just a prefix but it has become synonymous with computer security. Cyber security is the protection of computer systems from the theft of or the damage to the hardware, software or the information on them as well as from the disruption or misdirection of the services they provide.

It includes controlling physical access to the hardware as well as protecting against harm that may come via network access, data and code injection or because of malpractice by operators, whether intentional, accidental or due to people being tricked into deviating from secure procedures.

There is a hierarchy of cyber targets and the hierarchy is based on value. Value is not always a dollar figure. If we were to assess potential targets in terms of value, they would generally fall into these categories and in the following order:

- **National security:** As noted by the Canadian Security and Intelligence Service (CSIS), foreign intelligence agencies are making increasing use of the internet to conduct their espionage operations: it is a relatively low-cost and low-risk way to obtain classified, proprietary or other sensitive information. CSIS is aware of a

significant number of attacks against agencies at the federal, provincial and municipal levels. The Government of Canada, like those of other countries, witnesses serious attempts to penetrate its networks on a daily basis.[7]

- **Critical infrastructure**: According to Public Safety Canada, critical infrastructure refers to the processes, systems, facilities, technologies, networks, assets and services that are essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence. In 2016, the Government of Canada tabled a report entitled *Fundamentals of Cyber Security for Canada's Critical Infrastructure Community*[8] that endorsed the National Institute of Standards and Technology's (NIST) framework for cyber security[9] and put forward a strategy to implement an all-hazards risk management approach and share and protect information.[10] The sectors identified as critical infrastructure are energy and utilities, information and communications technology, finance, health, food, water, transportation, safety, government and manufacturing.

- **Intellectual property (IP):** IP refers to creations of the mind, such as inventions, literary and artistic works, designs and symbols, names and images used in commerce. IP is protected in law by patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create.[11] IP is the wealth creator of the next generation and is increasingly a cyber espionage target.

- **Personal data:** Personal data is a catch-all phrase that captures everything from databases with names, phone numbers and email addresses to email and social media content, social media profiles, behavioural profiles, location data and cloud-based media content.

7 www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php

8 www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf

9 www.nist.gov/cyberframework

10 www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf

11 http://www.wipo.int/about-ip/en/

The value of data is usually defined by its sensitivity (who gets hurt if it gets into the wrong hands), its function (is it critical to operations and long-term viability) and its volume (how many records). The higher value targets, like national security, tend to attract the attention of more sophisticated attackers, whereas personal data, such as phone numbers and email addresses, have a comparatively lower intrinsic value and tend to be the target of the cyber criminal masses.

We can assume then that there is also a hierarchy of where cyber attacks originate. Although some jurisdictions refer to only two groups—state actors and non-state actors—these groups tend to fall into one of the following more narrowly refined categories:

- State or state-sponsored actors
- Politically motivated activist organizations
- Organized crime
- Hackers or hacktivists (individuals)
- Disorganized crime (usually individuals and often an insider)

The majority of attacks come from the cyber criminal masses and are focused on the path of least resistance. Many cyber attacks share the following characteristics:[12]

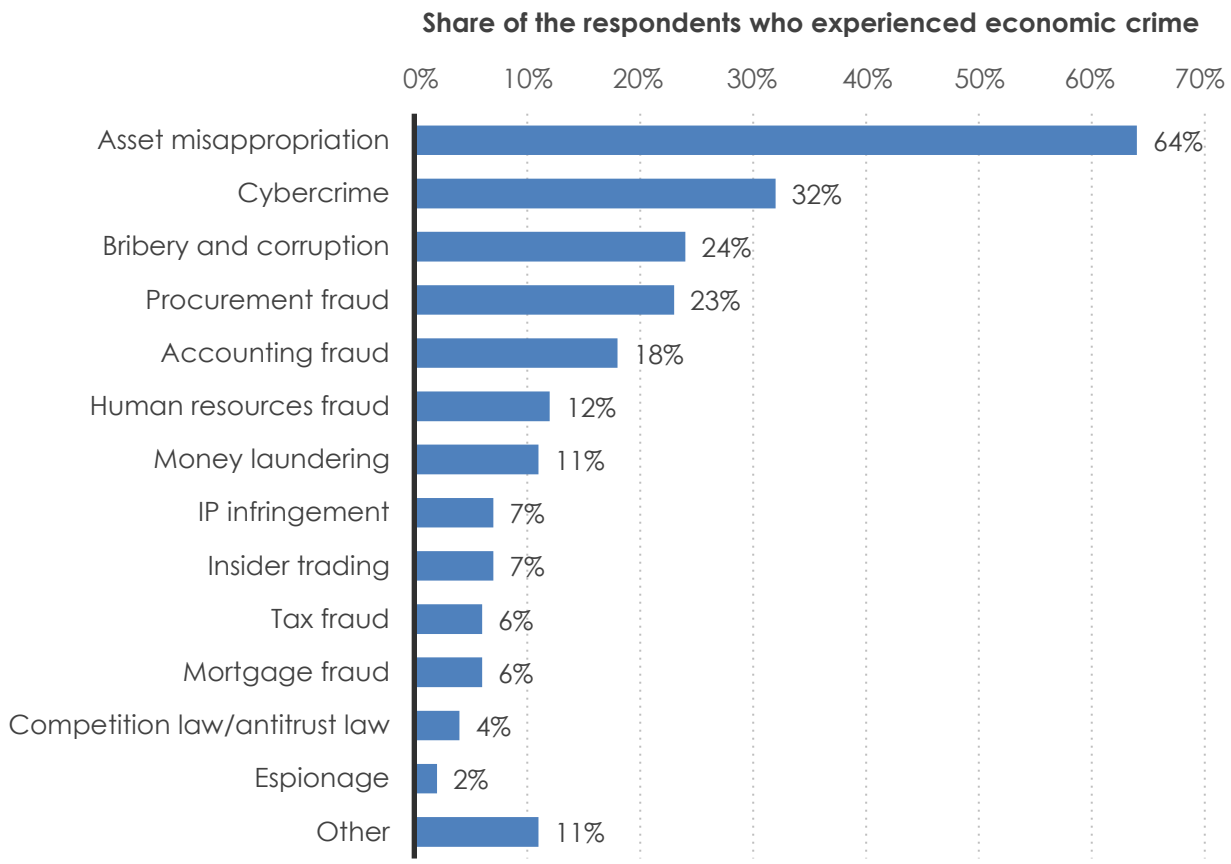
- Inexpensive: Many attack tools can be purchased for a modest price or downloaded for free
- Effective: Even minor attacks can cause extensive damage
- Low-risk: Attackers can evade detection and prosecution by hiding their tracks through a complex web of computers and exploiting gaps in domestic and international legal regimes

12 www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf

THE CYBER LANDSCAPE

Cybercrime has more visibility in boardrooms. The number and reach of cyber threats and cyber attacks that have followed greater global connectivity means cyber security has become one of the major concerns of companies across all industries. Cybercrime is now the third leading risk to businesses in the U.S. and is increasingly becoming a preoccupation in corporate boardrooms. In larger companies, chief information officers and chief technology officers have had to adapt to this increasing threat and respond by finding frameworks that answer basic risk management questions: what is at stake, who is after it and what do we do to protect our interests?

Figure 1 - Types of Economic Crime Reported Worldwide 2016[13]



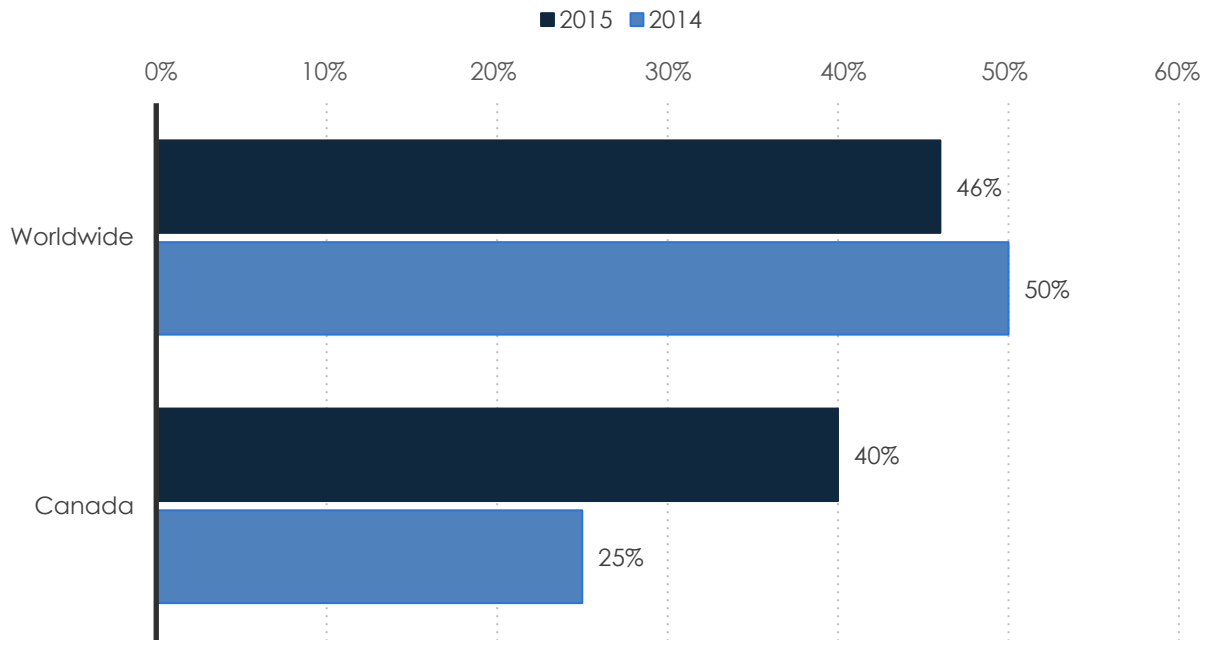
13 www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

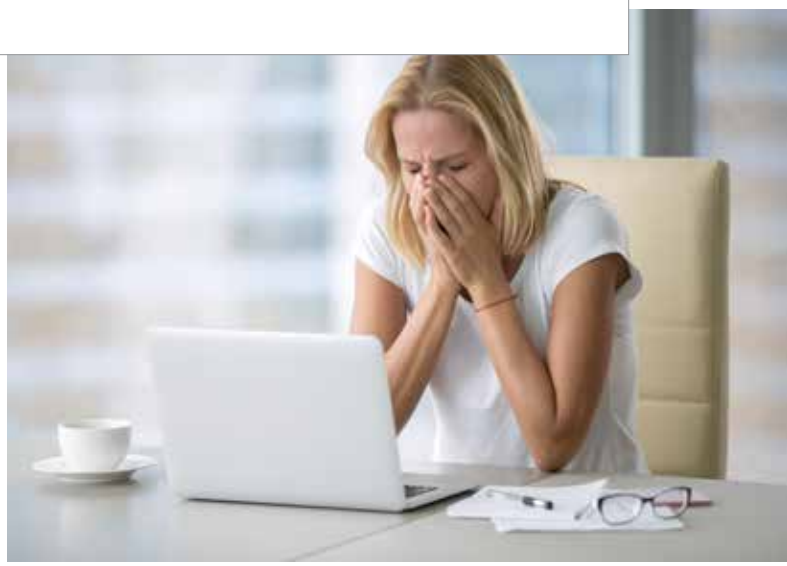
Figure 2 - Leading Risks to Global Business in 2016 (By Company Size)[14]

	Small and mid-size enterprise (up to 500 million euro revenue)	Large enterprise (over 500 million euro revenue)
Business interruption (including supply chain disruption)	30%	43%
Market developments (volatility, intensified competition, market stagnation)	38%	31%
Cyber incidents (cyber crime, data breaches, IT failures)	21%	34%
Natural catastrophes (storm, flood, earthquake)	23%	25%
Changes in legislation and regulation (economic sanctions, protectionism)	21%	26%
Macroeconomic developments (austerity programs, commodity price increase, inflation/deflation)	20%	23%
Loss of reputation or brand value	16%	20%
Fire/explosion	18%	15%
Political risks (was, terrorism, upheaval)	10%	12%
Theft, fraud, corruption	16%	7%
New technologies (impact of increasing interconnectivity and innovation)	9%	11%
Human error	12%	7%
Talent shortage, aging workforce	8%	8%
Quality deficiencies, serial defects	7%	7%

14 www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometerTopBusinessRisks2016.pdf

Figure 3 - Board Participation Rate in Cyber Security[15]



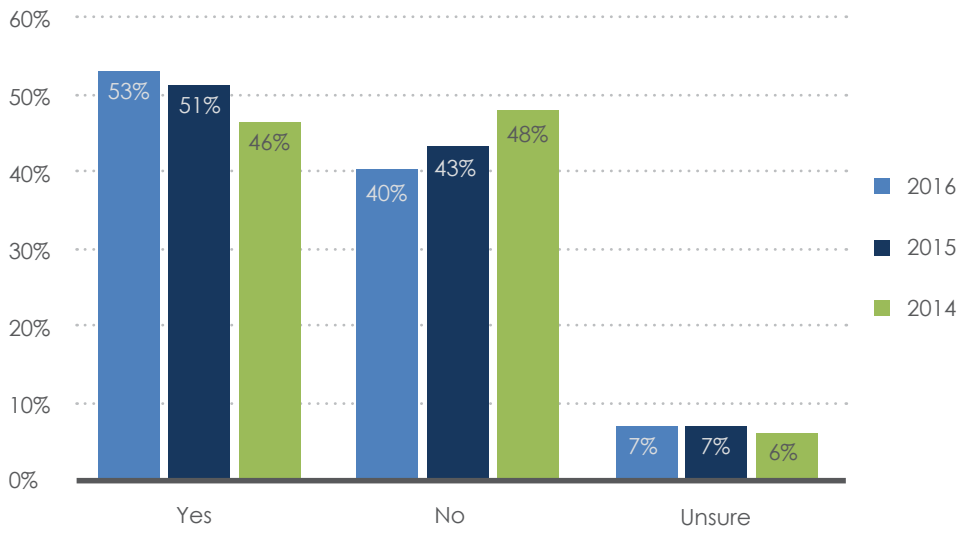


The number of data breaches is on the rise. Recent statistics paint a very clear picture that the value and relative accessibility of data in every form is too tempting to pass up. In a recently released Scalar Security study, the number of businesses reporting a loss or exposure of sensitive data over a 12-month period has increased every year for the past three years and 8% overall.[16]

15 www.canadianunderwriter.ca/insurance/cyber-security-must-be-viewed-as-a-business-issue-not-a-technology-only-issue-pwc-1003978981/

16 https://media.scalar.ca/uploads/2017/02/Scalar_SecurityStudy2017.pdf

Figure 4 - Businesses Reporting a Loss or Exposure of Sensitive Data in the Past 12 Months[17]



The cost of these breaches is escalating. As with the number of data breaches, the number of businesses reporting financial losses as a result of cybercrime over the last two years is increasing. At the same time, the dollar value of those incidents is also on the rise. In a recent PwC survey, business executives note the cost of cybercrime on the bottom line is increasing. These costs include downtime, compensation for breached records and loss of intellectual property.

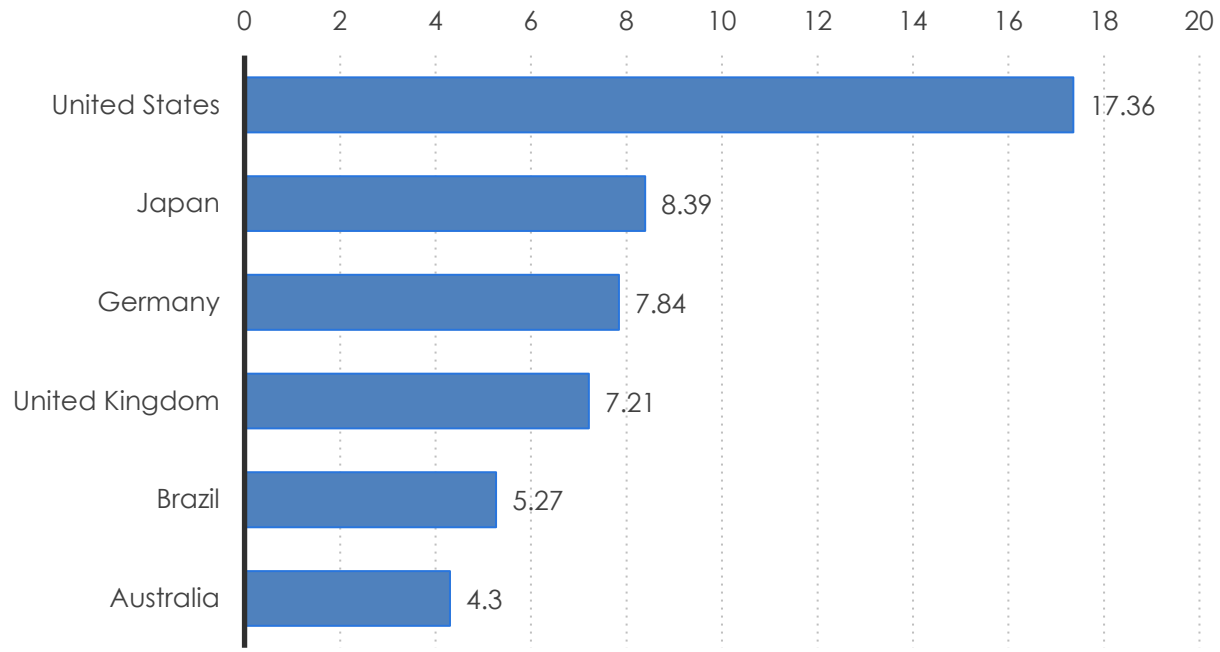
Cybercrime costs everyone, everywhere. Studies suggest that cyber attacks alone cost the global economy $445 billion annually.[18] Creating a more secure and trustworthy digital environment is critical to ensure the opportunities of digitalization are fully realized. Governments around the world are developing cyber security strategies, guidelines, regulations and national standards.

17 https://media.scalar.ca/uploads/2017/02/Scalar_SecurityStudy2017.pdf

18 WEF, *Global Risk Report* (2016), 77; McAfee Inc., *Net Losses: Estimating the Global Cost of Cybercrime* (2014), 6.

Regulatory approaches are often flawed. Frequently, this results in public policies with an undue focus on compliance instead of risk-based security performance, which creates additional costs. Although states are adopting the Budapest Convention on cybercrime[19] or defining regional cyber security regulations,[20] there is little international alignment. The fragmentation of cyber security regulations hampers cross-border activities and diminishes actual security, adversely affecting the growth potential of digitalization.

Figure 5 - Average Cybercrime Cost in U.S. Dollars[21]



19 The EU Budapest Convention on Cybercrime, accessed January 16, 2017, http://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185.

20 Regional agreements such as the European Union General Data Protection Regulation (GDPR).

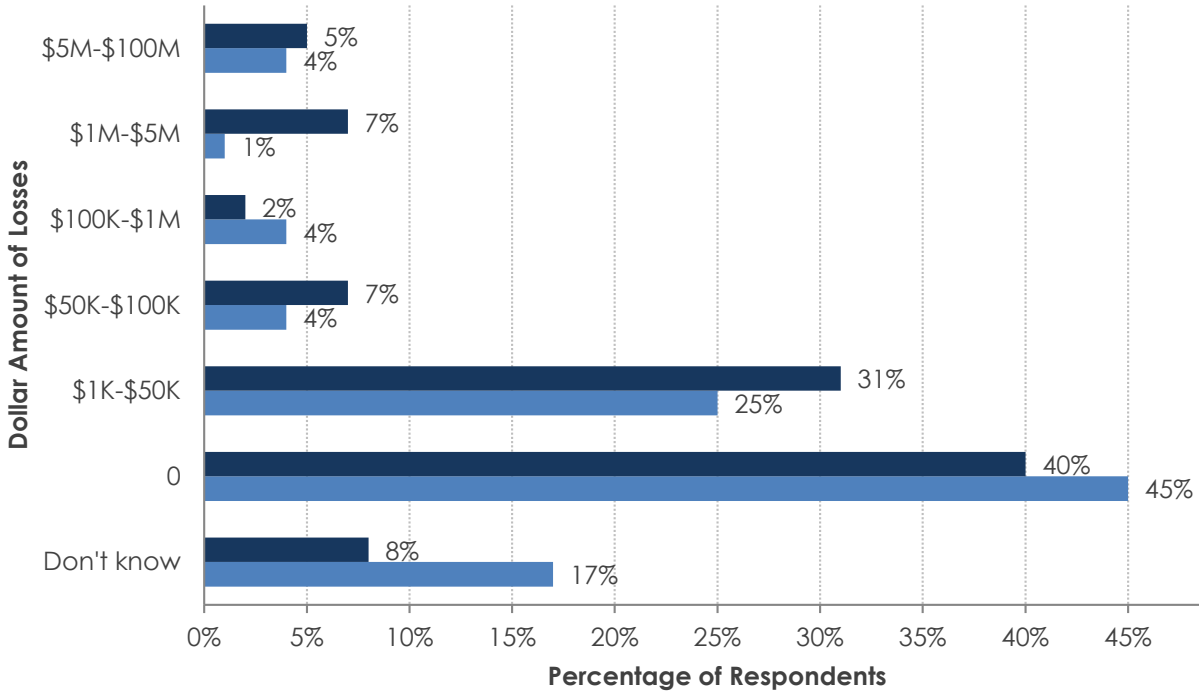
21 2016 Cost of Cybercrime Study: Global, Ponemon Institute; Hewlett-Packard (HP Enterprise Security), November 2016, p 4

In Canada, the number of businesses experiencing losses from cybercrime is increasing. The Ponemon Institute surveyed 24 companies across all sectors for IBM.[22] It noted:

- Average cost of data breach: $6.03 million
- Average cost per record of a breach: $258
- Average number of records breached in 2016: 20,456

The number of businesses that reported having no losses resulting from cybercrime has decreased from 45% to 40%. This is a good sign that awareness and visibility of threats are improving. More businesses have become aware of losses. The number of respondents who indicated not knowing if they had losses or what those losses were decreased from 17% to 8%. Along with the proliferation of attacks, the scale of losses has also increased. The number of businesses reporting a CDN$1-million+ loss has risen to 7% from just 1% two years ago.

Figure 6 - Estimated Business Losses Due to Cybercrime in Canada 2014-2016[23]



22 Ponemon Institute for IBM: 2016 Cost of Data Breach Study: http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03065caen/SEW03065CAEN.PDF

23 www.pwc.com/ca/en/deals/publications/2016-02-Global-Crime-Survey-Canada.pdf

CYBER INSURANCE

Cyber insurance is a growing business. Another way to assess the cyber landscape is through the lens of the dramatic growth of the cyber insurance industry. According to the International Risk Management Institute, cyber liability insurance can be defined as follows:

- A type of insurance designed to cover consumers of technology services or products. More specifically, the policies are intended to cover a variety of both liability and property losses that may result when a business engages in various electronic activities, such as selling on the internet or collecting data within its internal electronic network.

- Most notably, but not exclusively, cyber and privacy policies cover a business's liability for a data breach in which the firm's customers' personal information, such as social security or credit card numbers, is exposed or stolen by a hacker or other criminal who has gained access to the firm's electronic network. The policies cover a variety of expenses associated with data breaches, including notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties and loss resulting from identity theft.

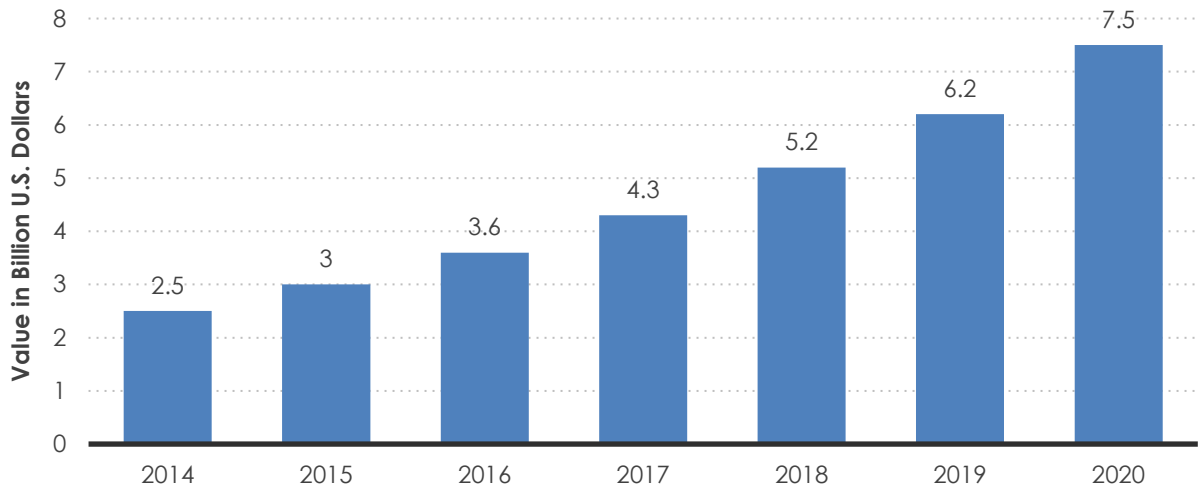
- In addition, the policies cover liability arising from website media content as well as property exposures from: (a) business interruption, (b) data loss/ destruction, (c) computer fraud, (d) funds transfer loss and (e) cyber extortion.

- Cyber and privacy insurance is often confused with technology errors and omissions (tech E&O) insurance. In contrast to cyber and privacy insurance, tech E&O coverage is intended to protect providers of technology products and services, such as computer software and hardware manufacturers, website designers and firms that store corporate data on an off-site basis. Nevertheless, tech E&O insurance policies do contain a number of the same insuring agreements as cyber and privacy policies.[24]

24 www.irmi.com/online/insurance-glossary/terms/c/cyber-and-privacy-insurance.aspx

The value of insurance premiums for cyber liability policies is expected to triple between 2014 and 2020, rising to USD$7.5 billion (see: Figure 7 - Estimated Value of Cyber Insurance Premiums). Growth in the industry so far has largely be concentrated in multi-nationals, with half of the $1 billion+ companies polled reporting they use cyber insurance (see: Figure 8 - Share of Companies with Cyber Insurance). The growth in the value of premiums comes from the nearly doubling of the number of companies purchasing cyber liability policies between 2011 and 2016 (see: Figure 9 - Companies Purchasing Cyber Liability Insurance).

Figure 7 - Estimated Value of Cyber Insurance Premiums[25] Worldwide from 2014 to 2020 (In $USD Billion)



25 www.forbes.com/sites/stevemorgan/2015/12/24/cyber-insurance-market-storm-forecast-2-5-billion-in-2015-projected-to-reach-7-5-billion-by-2020/#378ebf2a3ffe

Figure 8 - Share of Companies with Cyber Insurance Worldwide as of November 2014 (By Company Revenue)[26]

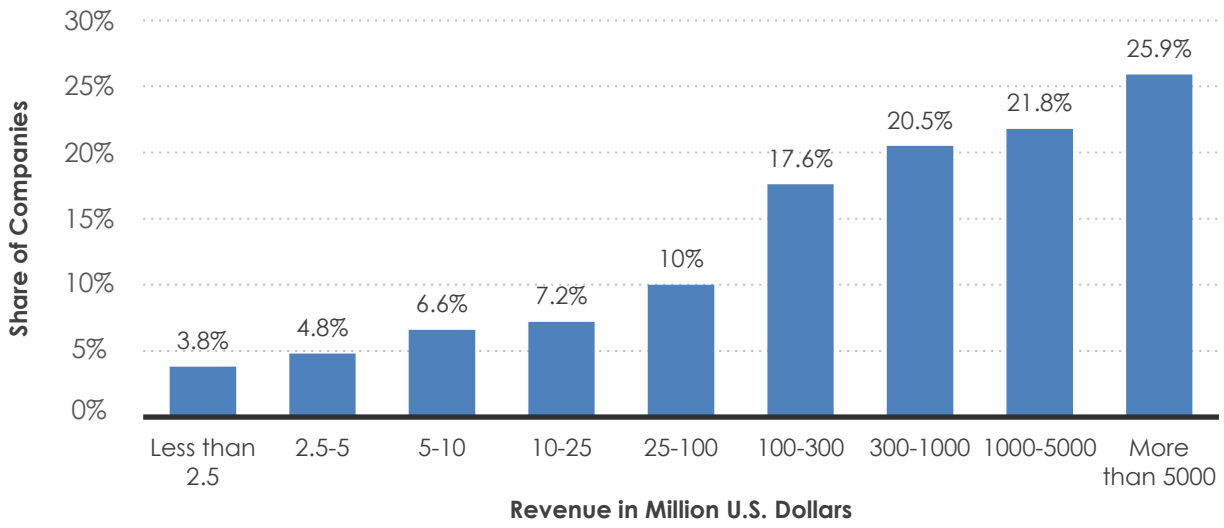
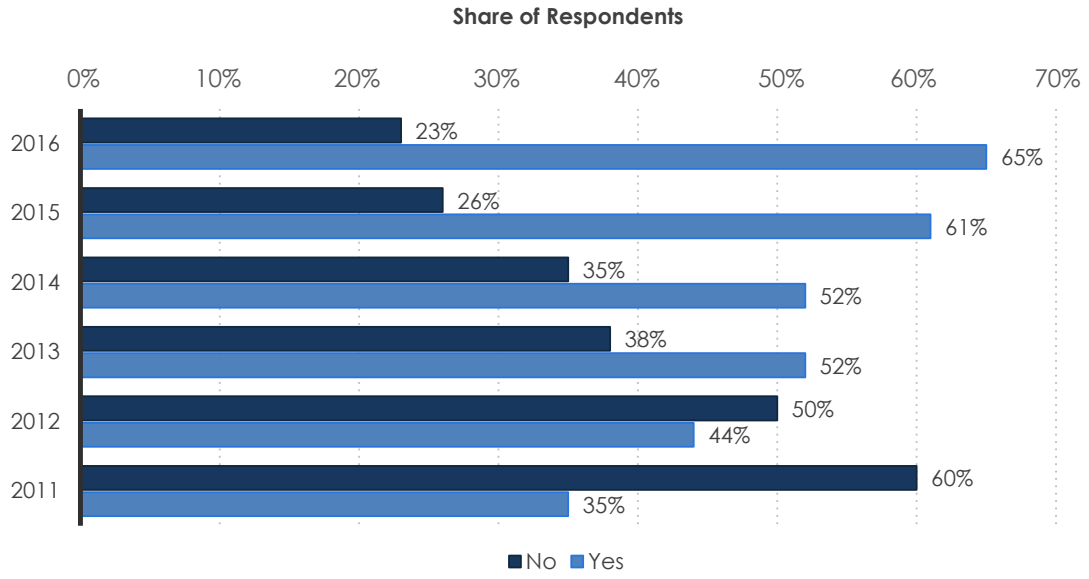


Figure 9 - Companies Purchasing Cyber Liability Insurance Worldwide 2011-2016[27]



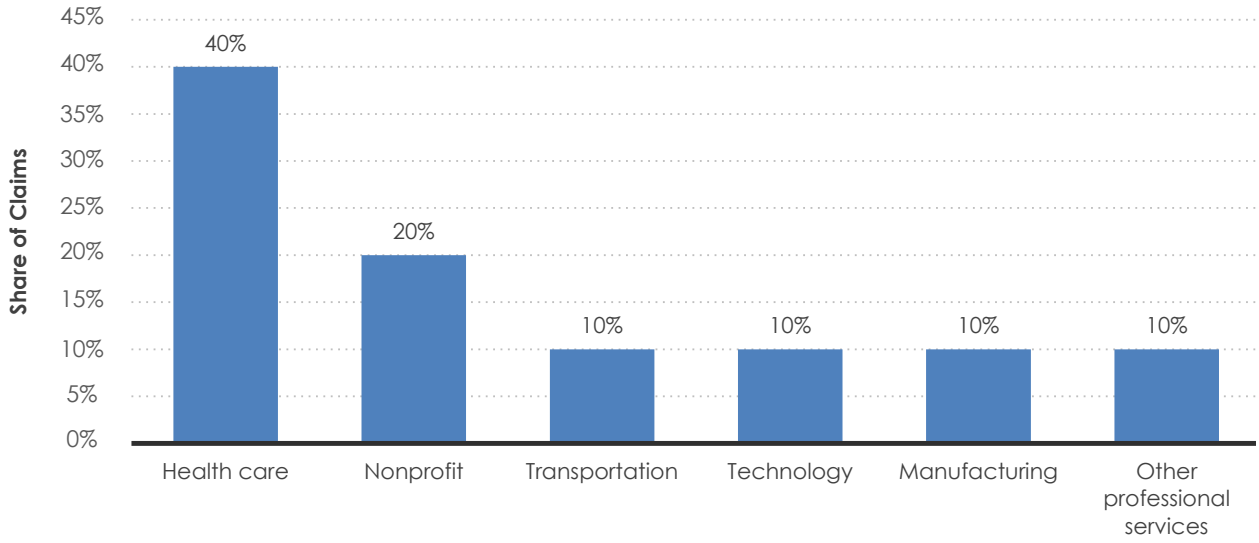
26 www.cyberrisknetwork.com/wp-content/uploads/2014/11/reputational-risk-does-it-have-a-bad-reputation-white-paper-2014-11-10.pdf

27 Advisen: Information Security And Cyber Risk Management The Sixth Annual Survey On The Current State Of And Trends In Information Security And Cyber Risk Management, p11, October 2016

Insurance is both a metric and a solution. The growth of the cyber liability insurance industry is clearly a symptom of a growing risk factor for business. Hyperbole aside, the number of businesses making claims demonstrates a need in the marketplace. Not surprisingly, the greatest share of liability claims appears to be coming from the health sector, which is recognized as a clear target and is often included in lists of critical infrastructure (as it is in Canada).

That said, claims are being made across all sectors (see: Figure 10 - Share of Cyber Liability Claims by Sector). While there are many precautions and solutions to improving business resilience to cybercrime described in this report, there is no bulletproof solution, and cyber liability insurance is an important consideration in cyber risk management. As one of our roundtable thought leaders put it, "There is a need to accept the inevitability of defeat."

Figure 10 - Share of Cyber Liability Claims in the U.S. 2014 (by sector)[28]



As noted by 2016 Netdiligence cyber claims study, "(t)he increase in the number of claims in the Nano-Rev and Micro-Rev offers strong indication that businesses of these sizes are becoming more attractive targets. It may also suggest that the number of law suits may increase and the need for both legal defense and cyber services will drive more companies of this size to obtain appropriate levels of cyber insurance."[29] The study also notes that 75% of claims costs are devoted to crisis services.

28 http://information.rjfagencies.com/acton/attachment/5250/f-0102/1/-/-/-/-/2014%20Cyber%20%26%20Data%20Security%20Risk%20Survey%20Report.pdf

29 https://netdiligence.com/portfolio/cyber-claims-study/ p6

ROUNDTABLE RESULTS

As a cornerstone of this examination, in October of 2016, we brought together thought leaders from across the country to consider what questions need to be asked, where should the focus of the Canadian Chamber of Commerce be and, finally, what is the path to improvement?

Here is what we heard:

Overview

Innovation and digital adoption are the buzzwords of the day. The Government of Canada has lead several related consultations on these subjects over the course of the past year. International organizations are crafting documents and recommendations intended to promote digitization and innovation by providing advice to national governments. As has been noted, the growth of the internet economy has created a wealth of opportunity for innovation, but the proliferation of highly publicized breaches has generated fear of its use.

As such, there is a great need for information and guidance, particularly for SMEs. Many SMEs recognize the need to do more to protect assets, but it is also true that the path to resilience is unclear for many of those businesses.

One of the key points of discussion during the roundtable was the "human factor." People are both the best resource and the weakest link in cyber resilience. Statistics have demonstrated that insider threats are the most common entry point for cyber criminals (up to 60%). But human error is also a major factor, either because of weakness in technology approaches or, more likely, a lack of awareness on the part of users. In addition to digital literacy training, cyber awareness training and technical solutions, there is a need to create a "human firewall" that transcends typical human behaviour and the need to click on that curious link that has enabled ransomware to become a rapidly emerging problem.

30 www.iso27001security.com/html/27001.html

31 www.iso27001security.com/html/27032.html

32 www.nist.gov/cyberframework

Canadian Chamber/International Cyber Security Protection Alliance Partnership

There are several internationally recognized certification guidelines and standards that are valuable in protecting business assets. The ISO 27001[30] certification standard and the ISO 27032 cyber security guideline[31] implemented together offer a robust approach to cyber standards. The NIST[32] cyber security framework offers an approach designed for critical infrastructure. Feedback from the roundtable suggested that while these approaches can be effective when meticulously applied, they are both too complicated and too costly for many businesses to achieve the desired level of risk management.

At the roundtable, we announced our partnership with the International Cyber Security Protection Alliance (ICSPA) to help deliver a certification standard that is both cost effective and achievable for any business.

The ICPSA acts as a conduit between the private and public sectors, centred on supply/value chain. The Cyber Essentials program is a certification framework focused on the problem. The process starts with health checks. CyberNB is also partnering with ICSPA to develop a number of related platforms.

Legal Issues

The proliferation of data breaches over the past few years has generated a significant reaction from both privacy advocates and governments attempting to reduce the impact of the theft of personal data on the general public. The result is generally a privacy legislation regime that focuses on the businesses that collect and store personal information rather than the perpetrators of data theft. In Canada, PIPEDA specifies the manner in which businesses can collect and use personal information, based on a balanced approach to consent.

Recent changes to PIPEDA will make breach notification and the recording of that breach in perpetuity mandatory. While the definition of a breach is clear, the threshold for reporting it is currently less so. The legal ambiguities of this new approach have caused concern within the business community, particularly as it pertains to the possibility of reactive class action suits. There is already a proliferation of litigation arising from breaches. Since late 2013 in particular, Canada has seen a significant increase in litigation activity, class action certifications and the potential for staggering damage awards for privacy and information security incidents. Dozens of data breach class action suits are currently pending in the courts, and a significant number of those cases have been certified.[33]

33 Cameron, Alex. Cyber Security in Canada: Trends and Legal Risks. Fasken Martineau Privacy and Information Law Group, February 2017

Issues for All Canadian Companies

All companies are targets for a cyber attack, and specific solutions change daily. Yet in many companies, there is a lack of ability to recognize these breaches. Today's attacks are about the data—not the company or person—and they are designed to be invisible. It was repeated several times during the discussion that the question is not "if you will be attacked." The question is "when will you be attacked?" Some went further as to say that "you have either been attacked or you do not know you have been attacked," and we are in a period of "cyber Armageddon." Yet while we are experiencing this "cyber Armageddon," most businesses lack the situational awareness, context and a common framework of understanding to adequately respond.

The corporate response to this issue, particularly in the event of an attack, is of major importance. There is a strong need for accountability and ownership of solutions. Yet for most boards of directors—that have the oversight function and responsibility—there remains the challenge of a lack of understanding and knowledge. For instance, banks cooperate and collaborate on information sharing, standards, practices and procedures. There is a need for similar thinking across all sectors.

SMEs

As will be further investigated below, SMEs were discussed at some length during the roundtable. The primary concern for SMEs is resources—most have no or limited financial or human resources (technical expertise) to address the challenges presented by cybercrime; therefore, there is little inclination to invest in protection.

SMEs often do not know how to answer basic control questions, which has significant implications for services and costs. Rather than approach the issue systemically, most SMEs go to one key question: how do we recover from an attack?

While some approaches can be part of a systemic solution, in isolation these approaches are insufficient. For instance, a big issue is the evolution to "the cloud" where the expectation is that "someone else" will look after the cyber risk. Yet exposure remains as there is no hiding in "the cloud." In the case of self-assessments and certification, budgets are strapped and infrastructure management is lacking. Similarly, in the case of cyber security, insurance affordability remains an issue and may not even be available without demonstrating certain precautions.

As many Canadian SMEs have a relationship in larger value chains, exposure at the SME level is worrisome at all levels of business.

Messages to Government

When asked about the role of government in cyber security, roundtable participants were quick to point out that there is no magic bullet. Governments have a clear leadership role to play in the protection of critical infrastructure and must actively protect national interests; industry cannot expect government to do everything. Government can facilitate improvements in how Canadian business addresses cybercrime through:

1. Grants and other financial incentives to make cyber literacy and cyber defence affordable
2. Tracking fraud and making enforcement a priority
3. Opening doors to sources of information and assistance
4. Activism and transparency
5. Establishing an information hub
6. Adopting a robust cyber security strategy—a secure Canada—and implementing it to improve credibility
7. Appointing a single ministry or agency to oversee the cyber file
8. Assuming a major role around related awareness and coordination

THE SME FACTOR

SMEs know they have to do more, but do not know how. There are many quality investigations into the Canadian cyber landscape. These do not always focus on a stand-out challenge for Canadian business—that of scale. A data breach costing $6 million would break many small businesses, and many of the reports generated to look at cybercrime are not telling the whole story.

As the Canadian economy is comprised primarily of SMEs (98%), the numbers for small business are particularly alarming. According to StaySafeOnline.org, 71% of data breaches happen to small businesses, and nearly half of all small businesses have been the victim of a cyber attack. Visa Inc. reports that 95% of the credit card breaches it discovers are from its smallest business customers.[34]

Criminals are attracted to small businesses for three reasons:

1. Due to a lack of resources, small businesses are less equipped to handle an attack.

2. The information hackers want—credit card credentials, intellectual property, personally identifiable information—is often less guarded on a small business's system.

3. Small businesses' partnerships—the value chain—with larger businesses provide back-channel access to a hacker's true targets.

34 Better Business Bureau, Cyber Security is Important for Small Business: http://bbbpnw.org/2015/03/20/cyber-security-is-important-for-small-businesses/

Small business is important to Canada. Here are some Canadian small business statistics to consider:

- In 2015, 70% (or 8.2 million people) of the labour force was employed by small businesses; mid-sized businesses accounted for 20% (or 2.3 million people) and large businesses accounted for 9.7% (1.1 million people).[35]

- In 2014, small businesses contributed 30% to the GDP of their province.[36]

- There are 1.2 million businesses in Canada. Of those, 98% have fewer than 100 employees, [37] 55% have fewer than four and 75% of all businesses in the country have fewer than 10.[38]

- An average of 130,000 new small businesses are created yearly, but only 35% survive five years.[39]

- Small businesses account for between 60-80% of all jobs created in Canada.[40]

- On average, small businesses with fewer than 100 employees contribute about 51% to Canada's GDP.[41]

35 www.ic.gc.ca/eic/site/061.nsf/eng/03020.html

36 www.ic.gc.ca/eic/site/061.nsf/eng/03020.html

37 http://canadianentrepreneurtraining.com/ten-canadian-entrepreneurship-facts/

38 www.bdc.ca/en/small-business-week/pages/smes-in-numbers.html

39 http://canadianentrepreneurtraining.com/ten-canadian-entrepreneurship-facts/

40 http://canadianentrepreneurtraining.com/ten-canadian-entrepreneurship-facts/

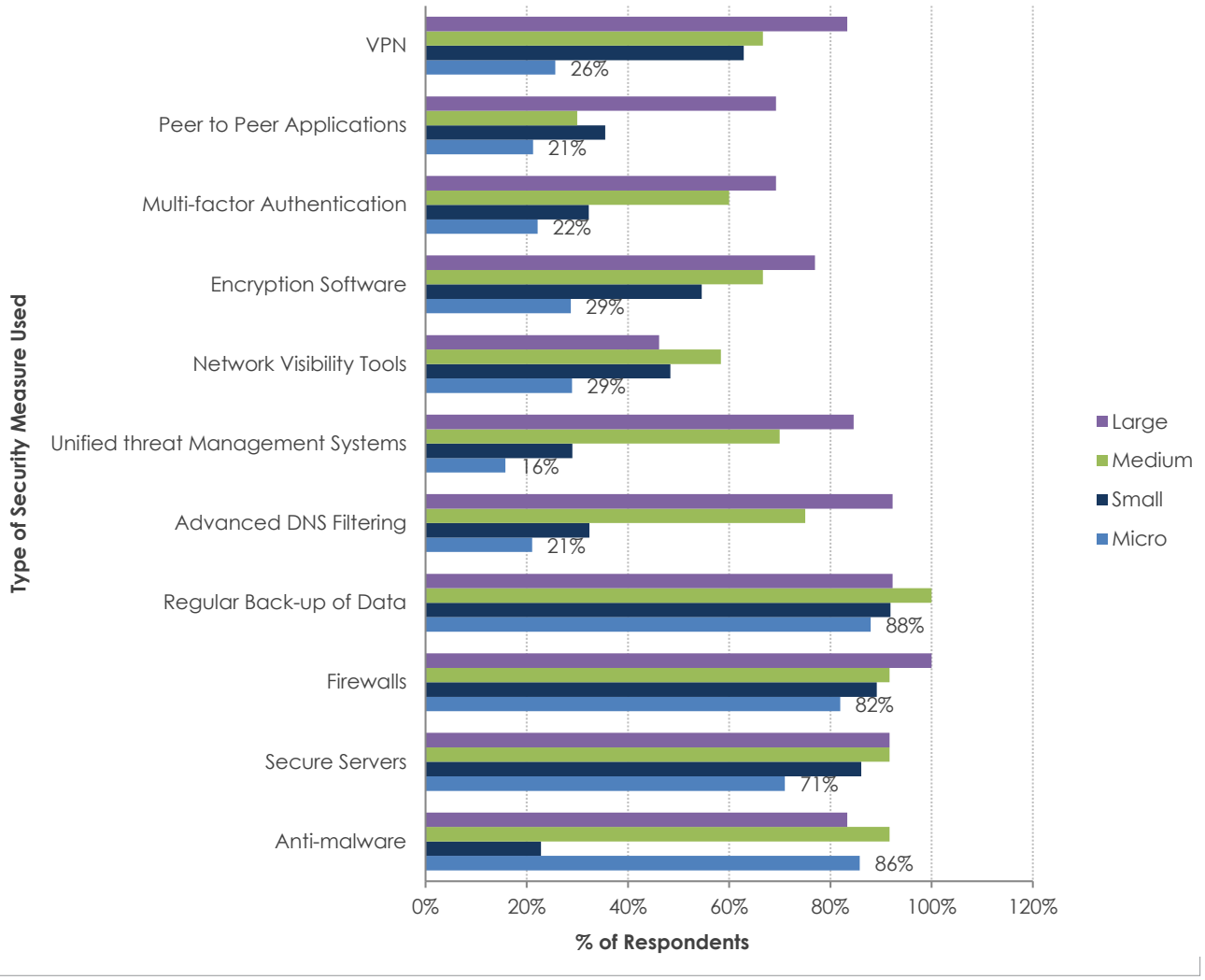
41 http://canadianentrepreneurtraining.com/ten-canadian-entrepreneurship-facts/

SURVEY RESULTS

In February 2017, we conducted a survey of approximately 260 businesses across the country to find out what cyber security tools they are using, if they are investing in training and the scale of investments in training and technology they are making.

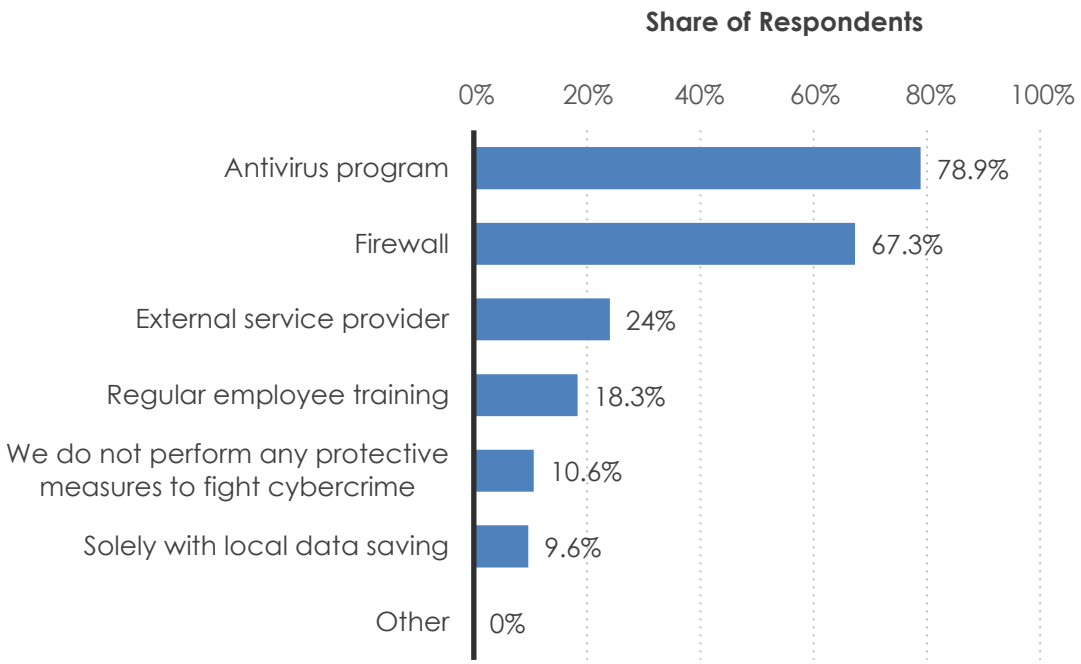
Results of Canadian SME use of anti-malware and firewalls compare favourably to U.S. results (88% vs. 79%). However, SMEs lag larger businesses with respect to most other measures.

Figure 11 - Businesses Employing Specific Cyber Security Measures[42]



42 Canadian Chamber of Commerce ICT Adoption Survey, February 2017

Figure 12 - U.S. SME Protections against Cybercrime 2016[43]



Large businesses are clearly more likely to have made (or will make) investments in cyber security training. Where 74% of micro-sized business are making no investments in cyber training, only 15% of large business plan no investments.

Large businesses are also more likely to make larger scale investments.

43 United States; Statista Survey; September 28 to October 7, 2016; 104 respondents; owners of small- and medium-sized enterprises with at least one employee

Figure 13 - Businesses Making No Cyber Security Training Investments over a Three-year Period[44]

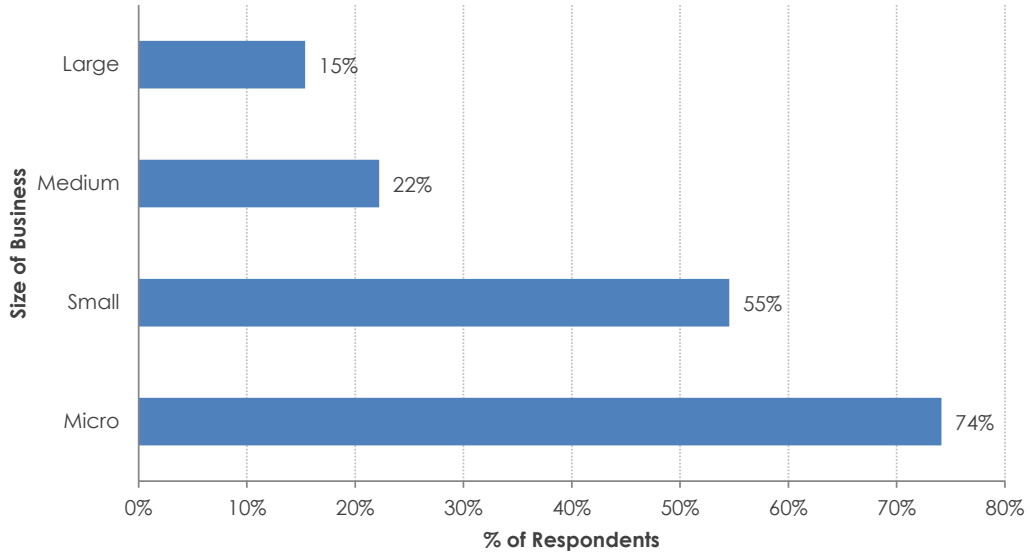
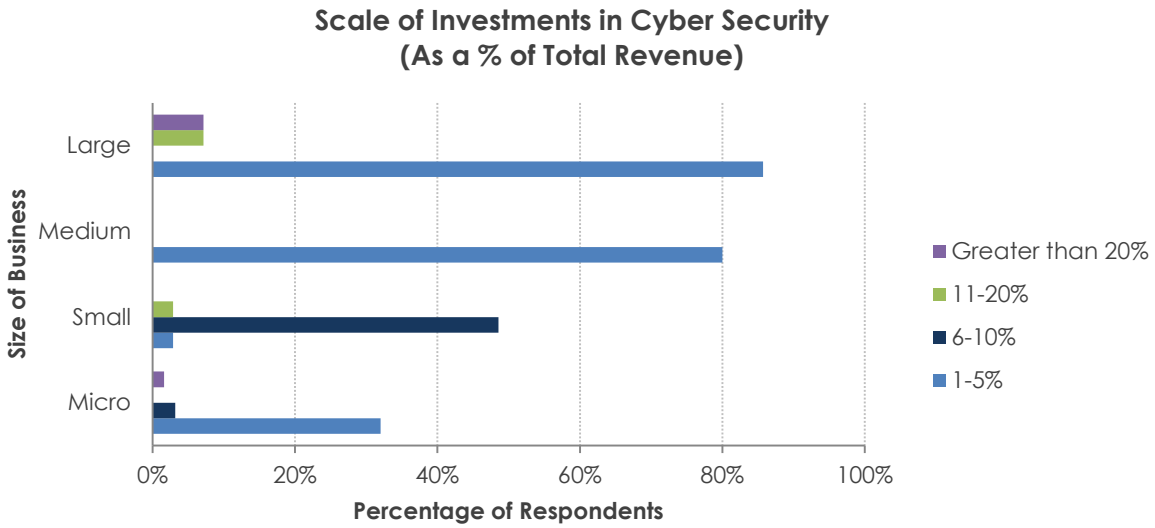


Figure 14 - Scale of Investment in Cyber Security[45]



44 Canadian Chamber of Commerce ICT Adoption Survey, February 2017

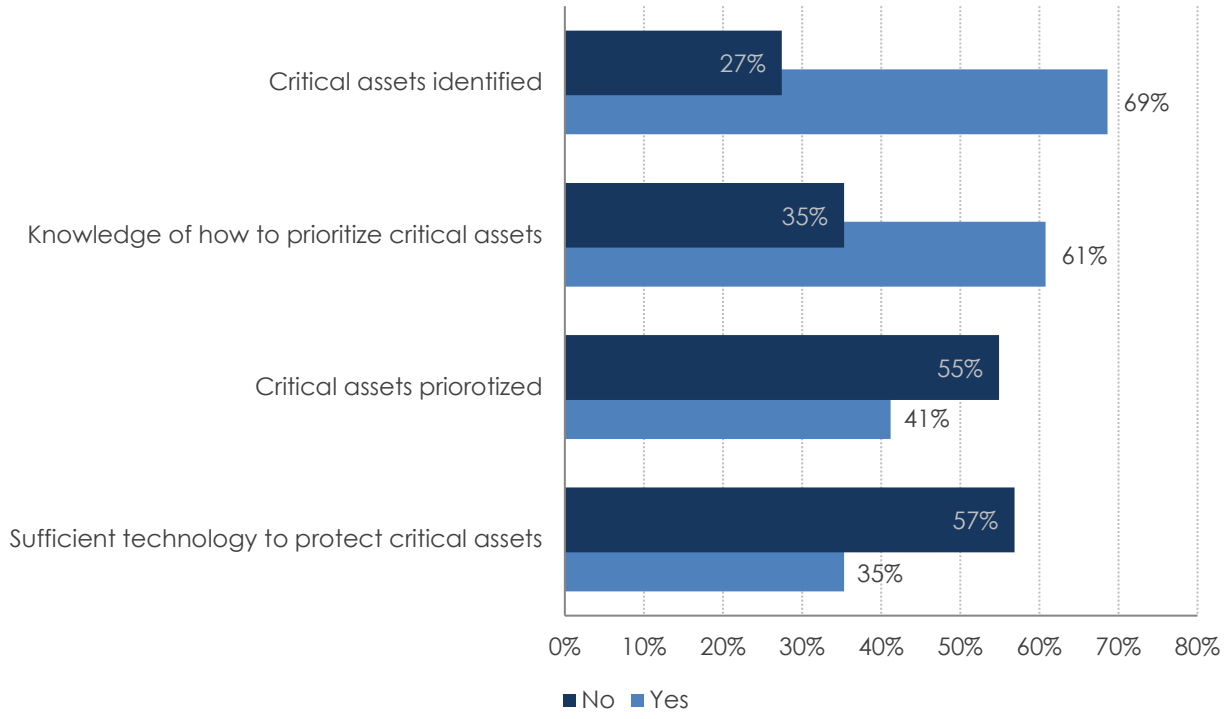
45 Canadian Chamber of Commerce ICT Adoption Survey, February 2017

RESULTS OF WORKSHOPS

In three separate workshops across the country, we asked a total of 75 businesses to respond to a series cyber "health checks." These health checks were designed by the ICSPA as a systematic approach to improving the way business approaches cyber risk management. The health checks are the first step in a cyber certification program called Cyber Essentials and Cyber Highway. The health check process allows prospective certification applicants to understand their circumstances and take measures to improve in each category.

We used the same health check process as a gauge of how business is doing. Workshop participants were asked 44 questions related to legislative compliance, public relations, technology, cyber awareness and cyber insurance. The results were very consistent with what has been observed in other research. Businesses know what they have (69%). Most businesses know the value of their data and what it would cost them to replicate it. They are also very aware of the reputational damage they would incur if the personal data they store got into the wrong hands. What they do not know is how to triage that data (55% said no) or what the appropriate technology choice was to protect that data (57% said no).

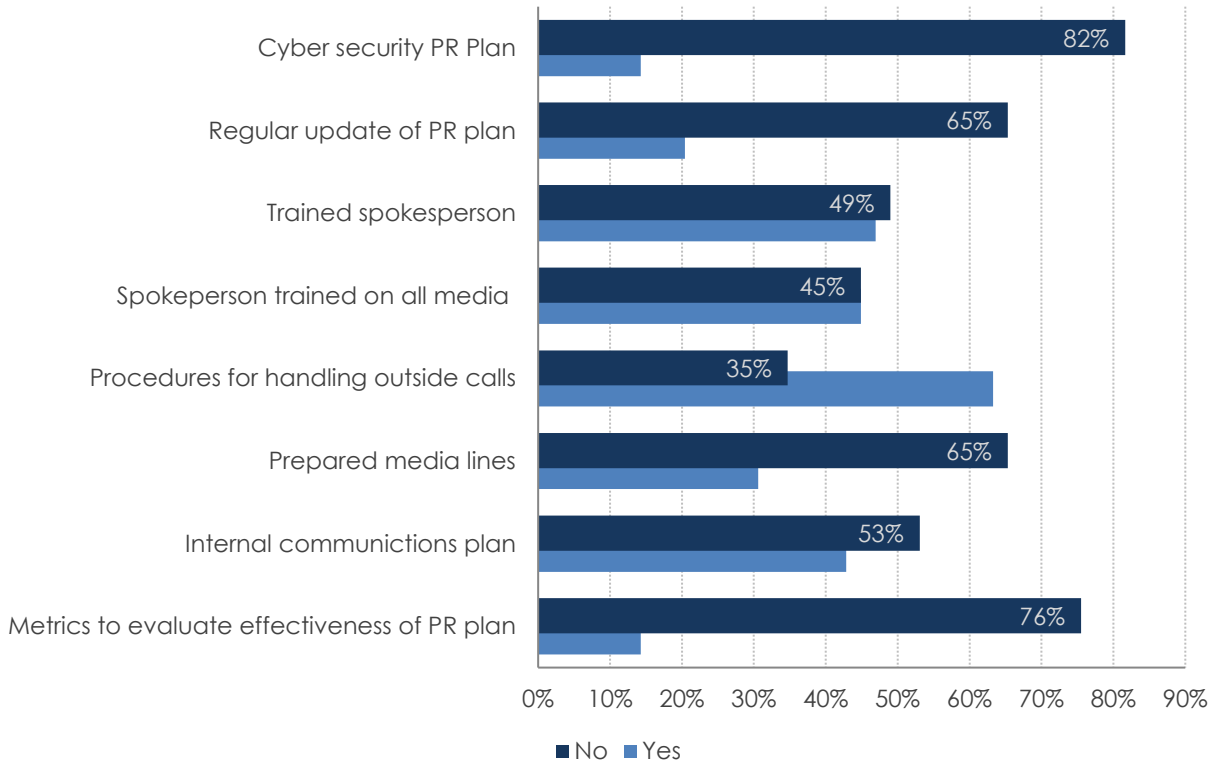
Figure 15 - Technology Health Check[46]



Knowing your assets is only the first step. The responsible approach to data management is knowing how to communicate your plan. Who to communicate with in the event of a breach is vital in protecting against reputational damage. Very few of our workshop participants had thought through the public relations component of a comprehensive cyber security plan.

46 Canadian Chamber of Commerce Cyber Security Workshop Series 2016

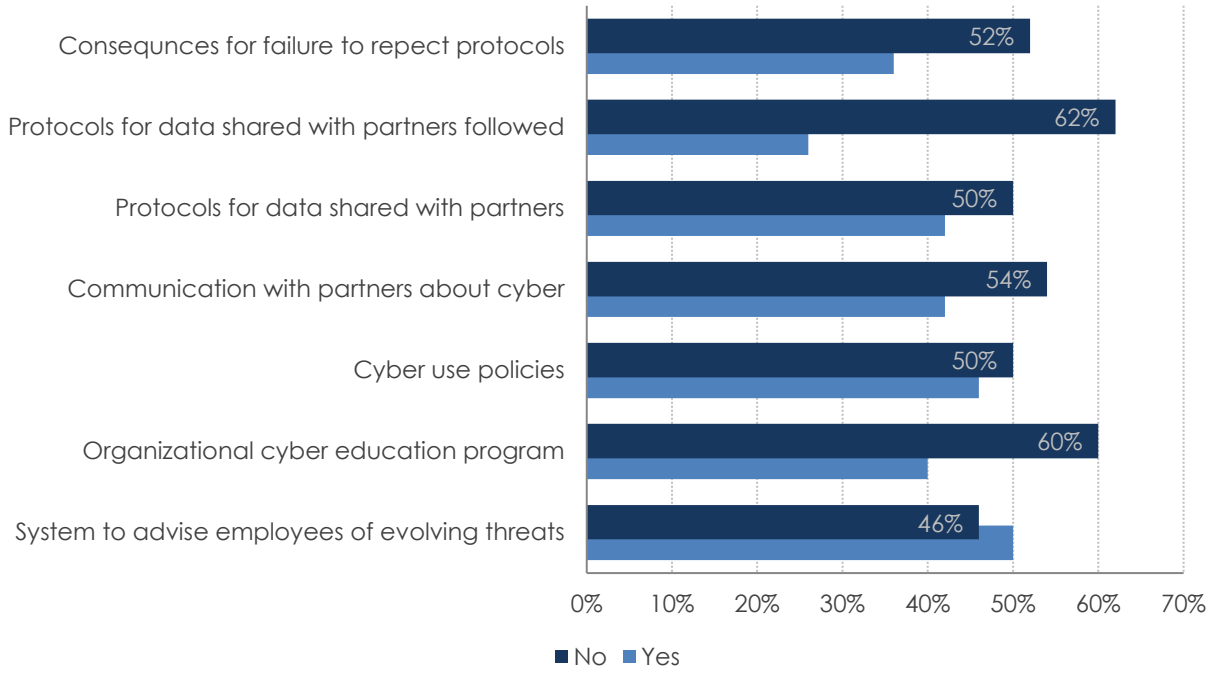
Figure 16 - Public Relations Health Check[47]



The response when asked about cyber awareness was a little more balanced, where roughly half the participants answered yes to each of the awareness related questions.

47 Canadian Chamber of Commerce Cyber Security Workshop Series 2016

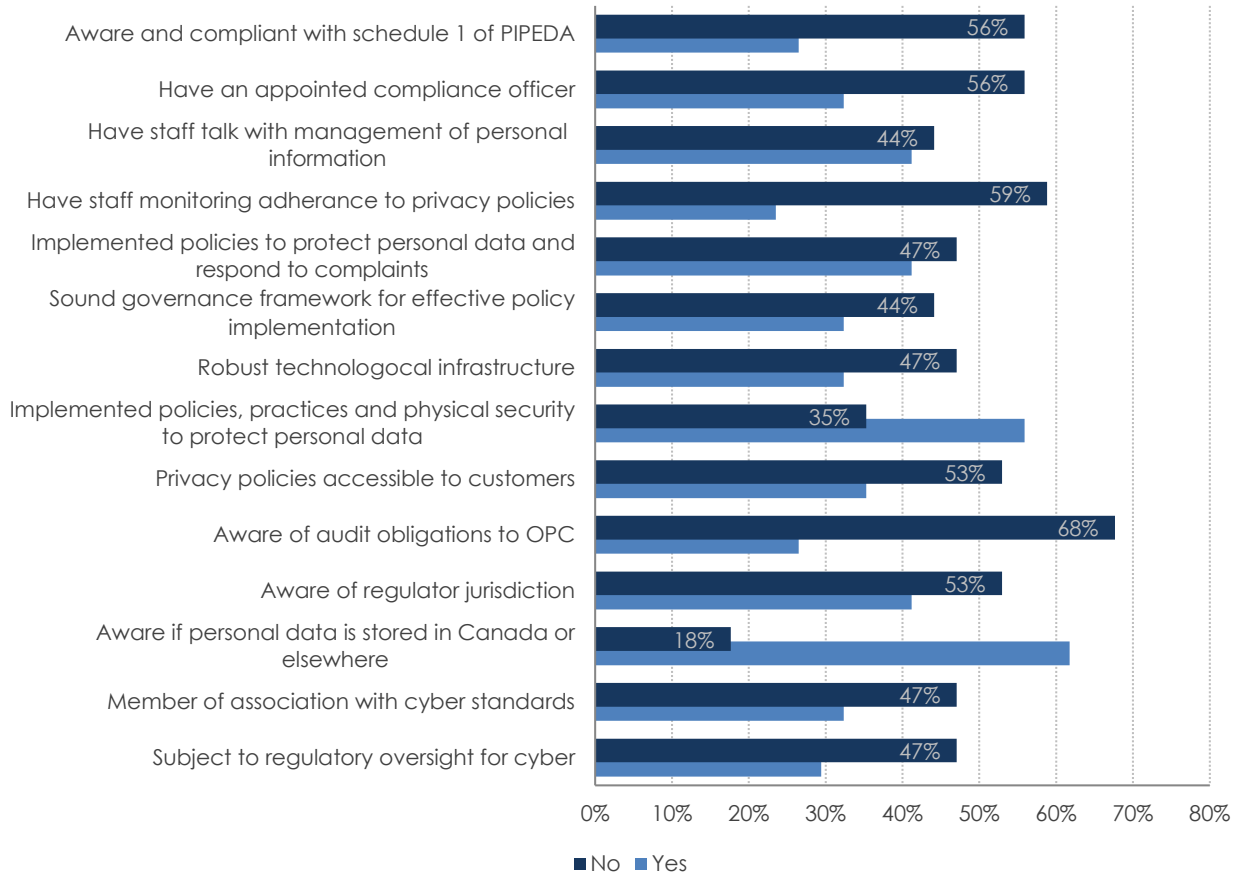
Figure 17 - Awareness Health Check[48]



The answers to questions about legislative awareness and compliance raise concerns. PIPEDA has been in place for 17 years. That over half of the businesses queried indicated they were unaware of responsibilities under the Act puts them at risk. With the advent of changes to the Act that require breach notification and record keeping, the matter is even more urgent.

48 Canadian Chamber of Commerce Cyber Security Workshop Series 2016

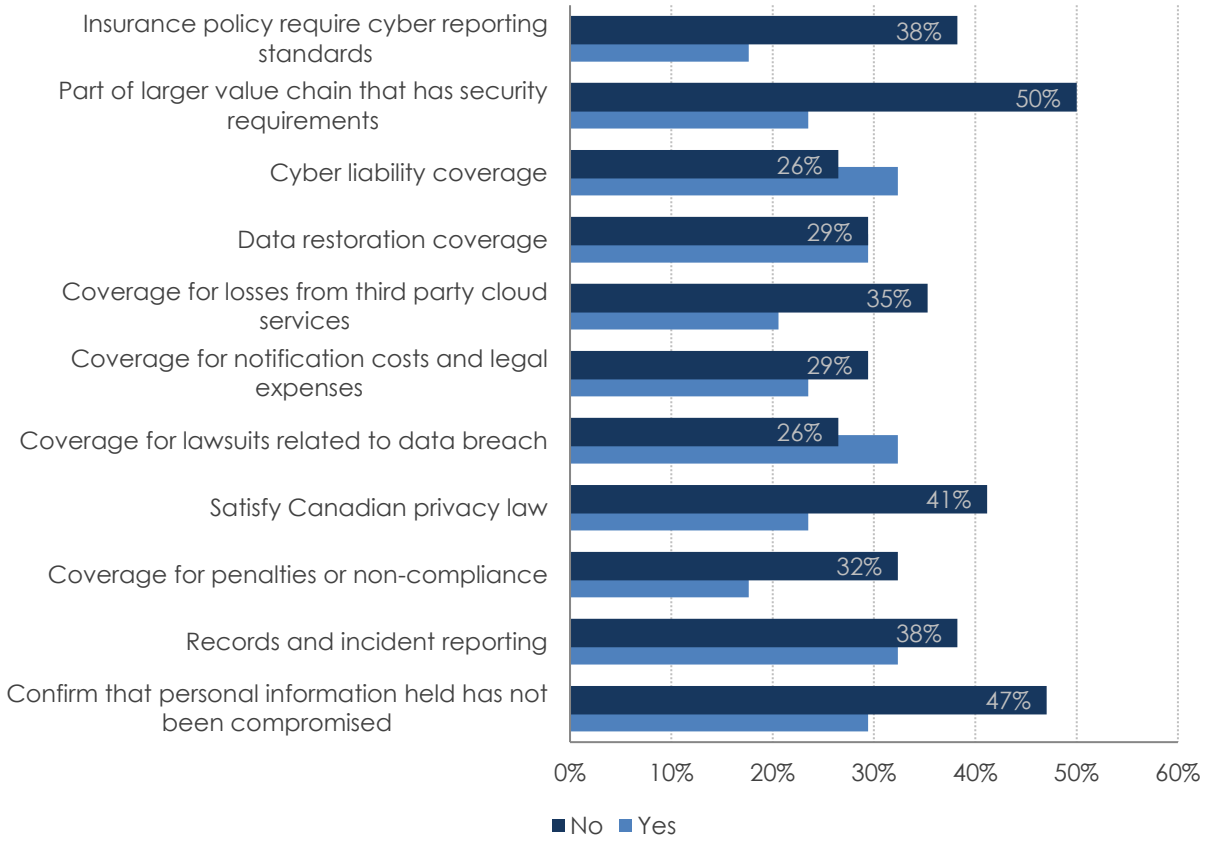
Figure 18 - Legislative Health Check[49]



The final piece of the puzzle (and this component was categorized separately for the purposes of this paper in contrast to how the health checks are designed by the ICSPA, purely for reporting purposes) is the insurance industry. In an earlier section of this paper, it was noted that cyber insurance was a rapidly growing business. Our workshops revealed that cyber insurance is not a well-known entity and is underutilized as a valuable risk management tool.

49 Canadian Chamber of Commerce Cyber Security Workshop Series 2016

Figure 19 - Insurance Health Check[50]



50 Canadian Chamber of Commerce Cyber Security Workshop Series 2016

DISCUSSION

Certification

Cyber security is a risk management exercise, like anything else. The two main things to consider are the value of the data (how much is it worth to the business, how much would it cost to recreate and could operations continue without it) and the sensitivity of the data (would anyone else get hurt, financially or otherwise, if the data was to get into the wrong hands). Once those questions are answered, it is much easier to figure out how much to spend to protect it and what tactics can be used to do that (training, software, off-site storage, cyber risk insurance policies, etc.).

One of the more common tactics criminals are using right now is ransomware. Inadvertently clicking on the wrong link in an email with malicious intent can cause data to be locked up (encrypted) until a ransom is paid to have it released. Criminals are adept at knowing the pain points of any given business—how much that business would be willing to spend to get the data back (a few hundred or a few million, depending on the sensitivity and urgency of what is locked up).

The easiest way to deal with this is to make sure data is regularly backed-up and stored outside of the businesses network. That way, a business can resume operations quickly and not be forced to pay up.

On data sensitivity, the real considerations are PIPEDA and reputational damage. If a business is considering a cyber liability policy, the best reasons to consider it are to recoup recovery costs. As an example, if a business experiences a breach and any sensitive personal information (such as credit card info) is lost, that business may be required to cover the cost of monitoring for a period of six months or a year. That can get expensive. As noted earlier, the average cost per record of a breach is $258.

Throughout the research for this project, some have suggested that a term like "cyber Armageddon" is hyperbole and that too people many are giving in to paranoia. In response, it should be said that the risks are real but manageable.

The easiest targets are small organizations that have not taken precautions (path of least resistance). Current stats suggest about one in 10 small businesses have had some sort of breach that they know about. That said, threats can exist on networks for a long time (average is 241 days) before businesses even become aware of the threat, causing a multitude of headaches.

The mantra in cyber security circles is there are two kinds of businesses, those that have experienced a breach and those that do not know they have experienced a breach. While that is a bit tongue-in-cheek, it is worth taking a few precautions.

Cybercrime has become a business unto itself. The cost to purchase malware that targets small enterprise is less than $100. Many "cybercriminals" are not coders and are really no more tech savvy than the rest of us. They have just figured out that if one chooses to break the law, this is a great way to make money because the risk of getting caught is low.

What we know is Canada has a very large segment of the population that derives a livelihood from small business. All business is at permanent risk from cybercrime. The biggest risk for most businesses is from loss of business following a breach, and the bulk of the risk comes from insider threats and criminal enterprise.

Small business is at significant risk resulting from resources challenges. Critical infrastructure, like our water supply, our electricity grids, our transportation infrastructure and our financial and defence industries, is also at significant risk because of the target value but also because of value chain relationships where networks, information and IP are shared across enterprises.

Information Sharing

As noted at the outset of this paper, sharing information among the key players—government, financial institutions, critical infrastructure operators, cyber security vendors and equipment manufacturers—is critical to the long-term success against cybercrime. Two examples of how this can be accomplished are:

CCTX: An independent, not-for-profit organization, the Canadian Cyber Threat Exchange (CCTX), will help Canadian businesses and consumers guard against cyber attacks. Launched in 2016, the CCTX works to share information about cyber threats and vulnerabilities among businesses, government and research institutions. It provides its members and the public with analyses of cyber security issues and acts as a point of contact for cyber information-sharing organizations in other countries.

FIRST: An exchange platform for improving cyber security, FIRST brings together a wide variety of security and incident response teams from the government, commercial and academic sectors. FIRST comprises more than 360 member organizations from 78 countries that pay an annual membership fee. The platform aims at information exchange and cooperation on issues of mutual interest, like new cyber vulnerabilities or wide-ranging cyber attacks—especially on core systems like the DNS servers or the internet as a critical infrastructure itself. Besides sharing information on cyber incidents, the members share best practices, tools, methodologies and processes to strengthen their cyber security activities. In 2014, FIRST established a collaboration on cyber security with the International Telecommunication Union (ITU) in order to facilitate the interaction between ITU and FIRST members.

Technology Outlook: A Few Quick Words on Future Tech That Could Change Everything.

Quantum computing: Quantum computing, in the truest sense, is still off in the future. While there are commercially available computers that take advantage of quantum principles (using probability), the true potential of quantum computing is yet to be realized. Quantum theory shows the position and the speed of a quantum, such as a photon or an electron, cannot both be known exactly. The more accurately we know the position, the more uncertain we are of the speed and vice versa. The uncertainty principle shows we can only calculate probabilities, not certainties. Thus, quantum computers can be very good at predicting outcomes based on probability from a very large number of variables. Quantum computers also perform calculations exponentially faster than conventional computers. They, therefore, have the potential to be very good at breaking current encryption technology.

Block chain: Since the first days of the internet, there has been a challenge in creating a foolproof way to conduct transactions digitally. Most of the conventional methods we are used to are fraught with vulnerabilities—it is way too easy to copy things in the digital world. Satoshi Nakmoto, the inventor of Bitcoin, figured out a way to create a digital currency that was virtually fool proof—it cannot be copied because too many people are watching. The big challenge was the storage intensity of the idea. Bitcoin is a digital currency that uses a technology called block chain, which essentially makes a copy of every transaction the currency is used across hundreds (or thousands) of databases. Each transaction has to agree with the previous one, making counterfeit virtually impossible. The efficient use of this technology has only been made possible by the exponential reduction in the cost of storage space per gigabyte. Block chain has potential across many applications that entail discretionary transactions, like real estate. Development and innovation in this technology will be useful in countering threats from cyber criminals.

Tokenization: Tokenization is another technology that will help reduce vulnerability to cybercrime**.** Tokenization, when applied to data security, is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value. The token is a reference that maps back to the sensitive data through a tokenization system. The mapping from original data to a token uses methods that render tokens infeasible to reverse in the absence of the tokenization system, for example using tokens created from random numbers.

IoT/IoE: Some call it the internet of things, others the internet of everything. What is important to remember is that just about everything we touch in the next decade will, in some way, be connected via a network. Our cars, our clothing, our refrigerators, our lightbulbs. An explosion in the number of connected devices is happening right now. Most of these devices, including the ones that are designed purely as industrial components, are not what is referred to as "security by design." The exploits we have heard about in our phones and TVs are set to occur in our thermostats, home security systems and our bicycles. Business needs to pay attention to the technology they are investing in for the purposes of efficiency and balance that with security risks.

RECOMMENDATIONS

Government Cannot Protect Everything but It Does Have Pivotal Responsibilities

Information sharing/transparency: take a 3P/coordinated approach to state-sponsored cyber attacks.

1. The balance between using known vulnerabilities as an exploitive tool to protect national security and being transparent about sharing known vulnerabilities with the companies that are building the products that are ubiquitous in the business marketplace needs to shift in order to close the back doors in these products.

2. Government needs to play a substantial role in critical infrastructure—keep the lights on, keep the water flowing, keep people fed and make sure money is safe.

3. Business would benefit from having a clear path to responsible government departments. This could be done by creating a government cyber czar that would coordinate activities of various departments, conduct outreach to stakeholders and provide input to international initiatives. Government would also benefit internally from having a single point of contact for resources and policy formation.

Outcome Based, Systemic/ Cohesive Approach and Common Model of Understanding

An accurate and current model is needed to test change before deploying new hardware or software that incorporates situational awareness and actionable intelligence. Just like a military sand table, situational awareness implies network visibility (see the whole picture), policy enforcement (no loopholes) and access (who gets in). Actionable intelligence requires both context (what are the most important things to protect and do the bad guys have access to those assets) and a robust framework for measurement and monitoring (you cannot manage what you cannot measure). As endorsed by the B20, the development of a harmonized cyber security baseline framework for efficient cyber risk management across economic sectors, as well as of cyber security norms for responsible state behaviour in cyberspace, is necessary. Cyber security policies that implement the baseline framework should not focus on compliance rules but should be outcome-based. By focusing on outcome-based policies, policy makers avoid frequent adaption needs to new digitalization scenarios while continuously ensuring the policies' purpose. While increasing the level of security, the baselines should also preserve personal privacy and minimize unintended surveillance by public and private organizations.

Develop a 'Secure Canada' Approach

Using a shared leadership approach, Canadian industry and government could improve Canada's cyber posture by creating and funding an entity charged with developing a 'Secure Canada' approach to security and privacy. This entity would collaborate with senior Government of Canada policy makers to develop a national framework for cyber competencies and roles and responsibilities at all levels of society—from consumers and small businesses to large corporations and government. In light of the recent consultations to update Canada's Cyber Security Strategy, the government should take into consideration the vulnerabilities of SMEs and the implications of cyber attacks on these businesses.

Develop a National Cyber Policy Framework

The Government of Canada and Canadian private and non-governmental organizations can turn challenge into opportunity by building a national cyber policy framework that supports cyber innovation and capacity building while helping businesses and consumers detect and mitigate cyber threats and vulnerabilities.

Adopt an Enterprise Risk Management Approach and Collaborate

Canada should work closely with G20 nations and develop a cyber security baseline framework for efficient cyber security risk management across economic sectors. Government and industry stakeholders must agree on network security priorities, identifying where and how critical data should be stored and how it should be shared among stakeholders. Collaboration will also be key in establishing sector risk profiles and corresponding security standards and protocols for the prevention of and response to security failures.

Increase Canadians' Cyber Savviness

Industry, government, non-governmental organizations and education stakeholders must demonstrate their commitment to cyber security and privacy by investing in programs that promote increased workforce capacity through digital literacy and technological awareness as well as greater personal responsibility for behaviours on devices and networks. For government and industry, this means working together to promote a cyber savvy workforce and cyber savvy consumers through targeted public awareness and education programs.

Industry Certification

Not everything can be protected, nor can everything be fixed. The goal is resilience. To achieve resilience, the combined challenges of external threats, network misconfiguration and human error must be addressed. Support/endorsement of an industry-led certification program that is manageable across multi-sectoral supply chains is needed. The International Cyber Security Protection Alliance has crafted a certification program—now deployed in the U.K.—called Cyber Essentials that is balanced, robust and affordable for industry. Government endorsement and support for the deployment of this program in Canada is important in building resilience within Canadian business and our long-term economic success.

Incentivize Security Innovations

The Government of Canada can show creativity and commitment by incentivizing industry to incorporate security features into IoT networks through tax credits and targeted funding. Industry can play a complementary role by leveraging its IoT networking presence in Canada to influence foreign IoT suppliers to adopt greater security consciousness in product design and production. To improve Canadian businesses' adoption of digital technology, the government should provide tax measures, such as allowing the Accelerated Capital Cost Allowance on technology to provide for software purchases and training for businesses.

Quantum-ready Strategy

Innovation in the development of quantum principles-based computing devices is moving quickly. Quantum computers are suited to the task of rendering conventional encryption obsolete. Both government and industry should take a proactive approach to addressing this inevitability.

For more information, please contact:

Scott Smith | Director, Intellectual Property & Innovation Policy
613.238.4000 (251) | ssmith@chamber.ca

THE CANADIAN CHAMBER OF COMMERCE

LA CHAMBRE DE COMMERCE DU CANADA

Chamber.ca | CanadianChamberofCommerce | @CdnChamberofCom