Adapting cybersecurity to the needs and capacities of SMEs:

A Canadian perspective

serene-risc

SMART CYBERSECURITY NETWORK

Authors

Fiona Westin

Project Lead

Smart Cybersecurity Network (SERENE-RISC)

Université de Montréal

Fyscillia Ream

Co-Executive Director

Smart Cybersecurity Network (SERENE-RISC)

Université de Montréal

Benoît Dupont

Scientific Director

Smart Cybersecurity Network (SERENE-RISC)

Université de Montréal

Montreal, February 28, 2022

This project is funded by Public Safety Canada

Public Safety Canada | Sécurité publique Canada

Serene-risc is funded by the Networks of Centres of Excellence and hosted by Université de Montréal

Université de Montréal

RCE NCE
Réseaux de centres d'excellence du Canada | Networks of Centres of Excellence of Canada

Table of Contents

Executive summary

Small and medium enterprises (SMEs) are vital components of the Canadian economy, making up 98% of businesses. Many are parts of critical infrastructure supply chains, or hold sensitive information relating to healthcare, children, and other vulnerable groups. They are also prime targets for cybercriminals. Rising trends in cyber-attacks are increasingly putting SMEs out of business due to unmanageable recovery costs and reputation damage and puts average Canadians' identities at risk with every data breach. Cybersecurity technologies such as firewalls, email security, and modern endpoint security are important tools in protecting businesses against attacks. Yet past research has shown SMEs' uptake of cybersecurity technologies is very low, especially regarding more innovative technologies which help protect against emerging threats. In our report we investigate the reasons for SMEs' lack of technological uptake and make recommendations to make cybersecurity technologies, both old and more innovative, more palatable for Canadian small- and medium-sized businesses.

We conducted data collection in three parts: i) a literature review of threats and challenges to SMEs' use of cybersecurity technologies, ii) interviews with 12 cybersecurity experts across Canada, and iii) a focus group with Canadian SMEs. We found, overwhelmingly, that technologies already exist to protect SMEs from the threats that they face, but that SMEs are not using them or not deploying them to their full extent. This was for several reasons, including limited resources, a misunderstanding of the role of technologies in an organization's cybersecurity infrastructure, technologies too complex to use for businesses without a dedicated cybersecurity or IT team, and, perhaps most interestingly, that SMEs do not know which vendors or service providers to trust in terms of cybersecurity solutions. Based on solutions discussed by participants and by the literature, we make the following six recommendations:

Mandate cybersecurity certification in high-risk organizations. SMEs that are part of critical infrastructure supply chains or that deal with particularly sensitive data, e.g., healthcare, financial data or data of vulnerable populations, should be required to complete a certification such as Cyber Secure Canada. This should include non-profits and charities. Enforcement should be proactive, *before* breaches happen. All other organizations should be strongly encouraged to become certified. For lower-risk organizations, a simplified certification could be offered to increase likelihood of uptake.

Make cybersecurity technologies more affordable for SMEs. Many cybersecurity technologies are inaccessible in cost to the average SME. SMEs should be provided with financial support to implement critical cybersecurity measures relative to their risks. This may be done through inclusion in business loans, tax rebates, or discounts on insurance. Lower-cost alternatives to existing cybersecurity technologies should also be made available to SMEs.

Create technologies that are easier to use. Many cybersecurity technologies are too complex to be operated by businesses without a dedicated cybersecurity or IT team. Developers should explore simpler but equally effective alternatives which can be operated by fewer people and adhere to usable design principles to ensure ease of use. Special attention should be given to areas where SMEs struggle the most, such as threat detection and quantum-safe encryption at rest.

Increase outreach efforts to businesses. Most SMEs do not find appropriate advice on their own and need to be met "where they are." SMEs should be proactively advised of where they can go for unbiased sources of cybersecurity advice. These efforts could include contacting businesses to offer informational sessions or on-site visits to help them

assess threats and implement measures, inviting businesses to information sharing calls, offering informational pamphlets about cybersecurity to businesses applying for or renewing a license, providing SMEs with a centralized hub of cybersecurity advice, and other awareness campaigns. Advice should be presented in a manner comprehensible to non-technical people.

Standardize technologies and encourage secure-by-design practices. SMEs do not know who to trust when it comes to cybersecurity solutions and often assume technologies are safe and secure when they are not. Technologies which are marketed as cybersecurity solutions in Canada should be required to be certified through standards such as Common Criteria. Other technologies which can introduce risks, such as data storage solutions and IoT devices, should indicate they have followed secure-by-design principles. Post-secondary institutions should include secure-by-design principles in their engineering curriculum.

Expand research on usability and outcomes of technologies. More research is needed about cybersecurity technologies used by SMEs, specifically in the areas of usability and outcomes on protection against attacks. These findings could be used to provide developers with advice for improving their technologies to meet SMEs' needs, and to provide businesses and policymakers with evidence-based advice on the effectiveness of various cybersecurity technologies. Efforts should also be made to consolidate existing information about cybersecurity threats and solutions from across Canada and to standardize related terminology and measurements.

Introduction

Small- and medium-sized enterprises (SMEs) make up 98% of all businesses in Canada [1], yet face much weaker uptake of cybersecurity measures than large businesses [2], particularly in regard to the use of innovative technologies [3]. Due to their lack of defenses, SMEs are often considered "easy targets" for cyber criminals [4] and can be used by attackers "as gateways through the supply chain to larger corporations," which includes critical infrastructure sectors [5]. The Canadian Federation of Independent Business' February 2021 report found one in 20 Canadian small- to medium-sized businesses had been the victim of cyberfraud in the previous six months and that they have spent an average additional $6,700 on cybersecurity during the COVID-19 pandemic [6]. They found 56% of entrepreneurs to be more worried about potential cyberattacks since March 2020. Despite well-founded concerns over attacks, two-thirds of business owners "reported they did not have the time, knowledge or resources to protect their business against cyberattacks" [6]. In fact, with an increase in attacks coinciding with the pandemic, only one in three Canadian workers expect to see an increase in human resources devoted to cybersecurity - and one-tenth expects to see a *decrease* in cybersecurity resources [7]. The Insurance Bureau of Canada reported in 2021 that fewer than *half* of small businesses surveyed had implemented defenses against cyber-attacks [8].

This is concerning given our increasingly digitized world, which creates new vulnerabilities for SMEs and makes them more likely to be attacked. According to the World Economic Forum's 2020 report [9], today's businesses face increasing entanglement of business and supply chain interdependencies, growing regulatory and related security attestation processes, networks, services, and data, increased speed of communications and data-processing, increased connectivity of systems and actors through both the organization itself and the supply chain, increased dynamism and complexity; monoculture of providers and interdependencies between sectors. SMEs are facing these challenges as are larger businesses, but solutions tend to be aimed at the latter, ignoring the unique needs and constraints of smaller businesses.

The Canadian Chamber of Commerce [10] recently identified cybersecurity investment in Canadian businesses as a high priority, including accelerating the competitiveness of Canada's cybersecurity industry, securing businesses, and increasing talent development. 2018 was a record year for investments in cybersecurity globally, with the industry "expected to grow to USD $177 billion by 2025" [11]. The Canadian federal government has committed to providing $500 million in funding by 2023 to businesses in order to help improve cybersecurity [12]. Such initiatives present Canadian organizations with an opportunity to innovate in the SME cybersecurity technology space, and to help put Canada on the map as a global leader in cybersecurity.

In this report, we investigate the reasons behind small- and medium-sized enterprises' lack of uptake of cybersecurity technologies relative to large businesses, and explore how these challenges may be overcome. We provide recommendations for stakeholders to help guide future innovation in regard to cybersecurity technologies for SMEs, on levels including government, industry, and research. This report is structured as follows: first, we describe the purpose of the study and the study methodology. Then, we present the findings, exploring the following themes: 1) the most pressing threats facing Canadian SMEs, 2) current technological adoption practices by Canadian SMEs, 3) the central challenges impacting SMEs' cybersecurity adoption practices, and 4) solutions and recommendations to stakeholders to help small and medium enterprises overcome these challenges, and to encourage useful innovation in this space.

Purpose of the study

The 2018 National Cyber Security Strategy highlights how digital innovation has become the engine of economic growth especially Canadian SMEs who constitute nearly 98% of Canadian businesses according to Innovation, Science and Economic Development Canada (ISED) [1]. In 2019, in terms of employment, small businesses were responsible for hiring 68.8% of Canadians, medium-sized businesses 19.7% and large businesses 11.5% [1]. In light of these statistics, it is possible to predict that digital innovation by SMEs is a fundamental component of Canadian economic growth. Yet despite being an important driver of innovation and growth, one-third of all breaches involve SMEs [13] and almost half of all SMEs (47%) have been victims of a cyberattack [14]. The results of Statistics Canada's Canadian Cybersecurity and Cybercrime Survey show that the size of a company directly influences the size of its cyber defense envelope. In 2019, on average, small businesses spent $11,000 on cybersecurity while large businesses spent $699,000 and medium-sized businesses spent $74,000 on average. Moreover, 32% of small businesses reported no direct expenditures on cyber security [14]. Thus, there is a clear need to help Canadian SMEs achieve a basic level of cybersecurity, giving their customers' greater confidence and giving them a competitive edge internationally. There is also a demonstrated need to support Canadian SMEs to grow and bring innovative cybersecurity technologies and services to the domestic and global marketplace.

The 2018 National Cyber Security Strategy emphasizes that cyber security is not only essential to protecting Canada's sources of digital innovation; it has become a source of innovation in itself. Various current and future initiatives support the technological innovation of Canadian SMEs and their cybersecurity initiatives. Among them, we can mention in particular: the creation of the Get Cyber Safe Guide for SMEs; the development of a certification program for SMEs, as well as various initiatives of the Information Technology Association of Canada (ITAC) to promote the development of talent and skills in the workforce.

This project originates from needs that have been reported to SERENE-RISC through various partners at the national level. In particular, this study will paint a portrait of cybersecurity service providers at the Canadian level. This project will provide these initiatives with an accurate portrait of tools, solutions and services related to innovation in order to identify existing best practices.

Across Canada, stakeholders are increasingly sensitive to SMEs innovation as they develop policies and programs to stimulate investment and encourage research regarding their cybersecurity innovations. However, despite a relatively favourable trend, gaps are to be filled to identify and disseminate efficient and innovative knowledge and practices enabling Canadian SMEs to position themselves in local, regional and global markets. To promote effective innovation strategies in cybersecurity for Canadian SMEs, SERENE-RISC delivered this project entitled "Knowledge mobilization on Innovation in Canadian SMEs." This project's primary goal was to establish a roadmap on of Canadian SMEs' cybersecurity innovation. This project had four objectives:

- Identify the technological gap of SMEs
- Identify the technological and organizational innovations used and marketed by Canadian SMEs
- Identify innovative practices and technologies that experts, cybersecurity researchers and governments recommend using
- Explore and anticipate the tools, innovative product solutions that strengthen the security of SMEs Canadian markets and support national growth and international competition

Methodology

This research project was conducted by SERENE-RISC on behalf of Public Safety Canada. We received the following ethics approval for our research project from the Université de Montréal: # CERSC-2021-011-D. The findings in this project derive from three data collection and analysis strategies: a targeted literature review, semi-structured interviews, and a focus group conducted in collaboration with a Canadian threat information sharing organization.

Literature review

We began our research by conducting a review of the existing literature about the state of cybersecurity in small- and -medium-sized businesses. We referred to academic journal and conference papers, white papers from governments and cybersecurity companies, and surveys and statistical studies from both inside and outside of Canada. We began our search on the ACM and IEEE digital libraries, Government of Canada websites, Google Scholar and Google using various combinations of search terms including *cyber security, SME, SMB, small medium business, small medium enterprise, attacks, threats, challenges, technology*, and then snowballed references from those sources. Our goal was to answer the following questions: *RQ1: What are the technological trends in cybersecurity and how are they used by SMEs?*, *RQ2: What are SMEs' needs and constraints in regard to cybersecurity,* and *RQ3: What are potential areas of technological innovation for Canadian SMEs?*

Once no new relevant sources were found, the researchers met to discuss the findings of the review and to identify gaps in existing literature, as well as areas which prompted additional questions.

Expert interviews

We created our interview guide based on the findings of our literature review, with the aim to both corroborate the findings of the literature review, and to address gaps in knowledge that had not been addressed by the existing literature. The main themes of the interviews included cyber-threats facing Canadian SMEs and the challenges that impede SMEs from implementing appropriate cybersecurity measures (see Appendix A for interview guide).

We recruited participants among the members and partners of the Smart Cybersecurity Network (SERENE-RISC) through emails describing the project goals. The inclusion criteria were as follow: to possess extensive subject matter expertise in cybersecurity (including technologies, processes, standards and regulations), to have been an active participant in the Canadian cybersecurity ecosystem for a number of years, and to represent an organization that interacts regularly with SMEs and understands their cybersecurity needs and the challenges they face.

We interviewed a total of 12 participants from across Canada, including the provinces of Ontario, Quebec, New Brunswick, and British Columbia. Interviews were conducted in English or in French, based on the first language of respondents.

Interviews were semi-structured and up to 60 minutes in duration. They were conducted remotely by one or more researchers in either French or English using the video conferencing platform Zoom. English-language interviews were transcribed using Zoom's built-in transcription service, and French-language interviews were transcribed by a research assistant. They were then translated into English using DeepL neural machine translation service and checked for accuracy by a bilingual researcher.

SME focus group

We conducted a focus group with members of a Canadian cybersecurity information sharing group to corroborate the findings of the expert interviews and to address gaps. The focus group was conducted remotely over Microsoft Teams and was led by one

of the researchers. 18 people were in attendance, primarily cybersecurity professionals in Canadian small- and medium-sized businesses. (See Appendix for interview guide).

Data analysis

All interviews, including both the expert interviews and focus group, were coded using NVivo 12 qualitative research software by one of the researchers. We used a mix of inductive and deductive coding, starting with deductive codes based on the main topics of the interview guide, and branching out to code emerging themes inductively. After a few interviews had been coded, the researchers met to discuss the inductive codes and to decide which among them would be added to the codebook for further coding. Once all interviews had been coded, we finalized groupings of code categories and identified the most salient themes, which we present in this report.

All participants were assigned a de-identified participant ID. Expert IDs appear as "P#". Focus group participants appear as "FGP#" and are numbered based on the order in which they first appear in the report. In the following section, we present the beginning of our findings.

Threats to Canadian SMEs: Not a matter of 'if', but 'when'

"No organization globally is immune to attack," stated one of the study's respondents, P3. Threats are ubiquitous in today's cyber landscape, and Canadians SMEs should prepare for the eventuality that they *will* be successfully targeted. The experts we interviewed were near-unanimous in their assessment regarding the inevitability of an attack. "This is not the problem of thinking "if you get attacked", but rather "when" [...] All Canadian SMEs are currently targets, and it is just a matter of time." (P11). "For this particular group, small, medium business: [the risk of being hit] is nearing 100%" (P3). So, what attacks are Canadian SMEs facing?

CIRA's 2020 Cybersecurity report [7] found the most common cyberattacks experienced by Canadian businesses in 2020 were malicious software (57%); unauthorized access, manipulation, or theft of data (55%); scams and fraud (55%); identity theft (42%); denial of service (33%); theft or compromise of software or hardware (30%); and disruption or defacing of web presence (30%). The Canadian Centre for Cyber Security predicted in its 2020 Threat Assessment [15] that the greatest emerging threats to Canadian organizations in the following two years would be the targeting of industrial control systems and critical infrastructure, ransomware and big game hunting, the stealing of data (both intellectual property and proprietary information, and customer and client data), and the exploitation of trusted business relationships, including retail payment systems, supply chains, and managed service providers.

The experts we interviewed tended to agree with the available literature regarding the range of threats facing Canadian organizations today. They named an array including malware, website defacement, DDoS (distributed denial of service) attacks, and "relatively rarer" threats such as insider attacks. Some forms of attack were seen as more pressing issues for SMEs than others. We outline the most significant threats, according to the experts we interviewed, in the subsections below.

Ransomware

"I think ransomware is the most serious threat that Canadian organizations of all kinds are encountering right now [...] It's growing in intensity and in pervasiveness" (P2). This threat was a constant theme in our interviews with experts, who nearly unanimously answered "ransomware" when asked about the biggest threat facing Canadian SMEs today. Ransomware first arrived on the global scene in 1989 but recently has experienced massive growth thanks to the emergence of the Ransomware-as-a-Service (RaaS) business model [16]. Not only has ransomware become increasingly common in recent years, but it is also the "most pernicious," says P12, "That [...] can further endanger the viability of SMEs." Worldwide, the average cost of recovering from a ransomware incident in 2021 was $2.3 million CAD [17].

This type of threat, at its most basic, is where "I [the attacker] either have your information or I've messed with your information and you're going to pay me to get it back" (P1). Many associate ransomware with the traditional "locking down your computer" scenario, where one's data is encrypted by the attacker and the victim pays to regain access. In such cases, restoring from backup can prevent the need to pay the ransom while regaining access to one's data. However, as the importance of keeping backups begins to get through to businesses, attackers are becoming increasingly creative. One such form is "extortionware," which can bring ethical, and legal, implications to the forefront: "[T]he bad guys realize that if you have backups, you're not going to be willing to pay. So now they threaten to post your information online. This takes it to a whole different level. Once the data is exfiltrated, the damage is done, so now it's just about: do you pay to hold that information, usually of your clients [...] from being divulged. Now this isn't about your own ethics and morals as a company

anymore; [...] this is about, okay, is there something else that you can do to prevent your customers' sensitive information from being exposed? [...] Backups aren't going to save you in that particular case" (P3). When businesses refuse to pay, threat actors may even escalate cases of extortionware by threatening to go directly to the media about the stolen or leaked data (P1).

Another form of ransomware is the covert corruption of select files. This can have dire outcomes in critical infrastructure. "The worst type of threat now is [...]: 'I'm gonna corrupt a couple of files. I'm just not going to tell you which ones.' And we are starting to see that happen and that's the biggest risk in settings like healthcare. Because you can imagine what happens when you corrupt a couple of files" (P1).

Ransomware attacks are also becoming more "sophisticated," say experts, with attackers quietly infiltrating and then moving laterally across networks, undetected, before making their move. P6 refers to this as attackers being "there for the long haul" or "persistent." "The more sophisticated hackers are really very patient in knowing the environment before attacking," says P8, explaining that they can intrude, for example, through a malicious link, and then lurk in the shadows for quite some time as they explore the businesses' systems and "find out where the vulnerabilities are, how they are able to transfer the funds, how they are capable of stealing personal data." When it comes to more targeted attacks, threat actors will do whatever it takes to damage a business where it counts, whether it be through direct cost, negative impacts to operation, or reputation.

Ransomware is costly when businesses are unprepared, which in the current environment is often as "[SMEs] do not necessarily have the minimum to protect themselves from this kind of threat" (P12). The experts we talked to recounted experiences with Canadian companies who had not made investments in cybersecurity "caught in situations where the ransom will be $500,000, $1M" being forced to pay consultants to negotiate ransom fees – the success of which is not guaranteed. "If the ransom doesn't work, you have to rebuild the environment. There is money that is spent when there is ransomware, malware that affects a large percentage of environments" (P11). Prevention is key. "When I invest dollars in cybersecurity, it is not dollars that I throw in a well. These are dollars that go directly to prevention. So, I make sure I don't pay a fortune either in ransomware or outside advisers who will have to rebuild my environment. [...] [R]ansomware costs more than prevention" (P11).

Phishing and social engineering

Experts divided phishing into two categories: "sophisticated," or targeted (also known as spear-phishing), and unsophisticated: "There are the 'phishing' attacks that go fishing. So there is a sending of millions of emails and people take the bait. And there are others that are much more targeted, much rarer, who will take control of the company, that will usurp the names of the company people, etc. for emails to have an impact on the organization" (P9). This may also be known as "business email compromise [BEC]." "[T]hey'll be based on a combination of information that people can put together about a business. They can call and get one piece of information, and combine that with other information that they get online" (P5). The latter type of attack is becoming more sophisticated than in the past, says P5, as a means to defraud businesses or to have them pay fake invoices. This makes them "much less clear" to identify. "For a lot of these small and medium-sized businesses when they have so much going on, it's hard to always keep your guard up to kind of guard against these types of attacks, I think it's a challenge" (P5).

Supply chain attacks and threats to critical infrastructure

Using a similar approach to attackers who move laterally within businesses before attacking, supply

chain attacks are also using one business as the "soft target for entry" (P6) into another, leveraging the linkages across digital infrastructures that make supply chains more efficient. According to the World Economic Forum's 2020 report [9], today's businesses face increasing entanglement of business and supply chain interdependencies, which makes this type of attack increasingly likely. "So many SMEs today are part of a supply chain. So practically every SME is a supplier to some other business" (P7). This makes them the perfect "soft" target, as their defenses are usually not as advanced as those of the larger companies to which they are connected. "SMEs that are parts of supply chains can be implicated in much larger attacks. A small or medium-sized business that happens to be a vendor to e.g., an electricity generator or transmitter; a municipality transit system… Attackers will often seek the most vulnerable place to attack. And so small and medium sized businesses, though we may not immediately think, okay, 'they're going to be targets,' they can be targets to attackers who want to attack larger connected systems." (P2).

Experts expressed concern about supply chain attacks' ability to interfere with Canada's critical infrastructures. "What we see is that [as] SMEs become [more integrated] into the digital supply chain of larger entities like critical infrastructure operators like hospitals, etc., they're increasingly targeted as the soft target for entry into that supply chain and eventually obviously into that larger entity or that large organization. While [smaller businesses] were ignored in the past, other than the basic dialing for dollars ransomware stuff, they're now seen as an access point into the larger organizations via the supply chain" (P6).

Supply chain attacks make it important "to raise the security water level across Canada. Because if you think about it in this current state of hyper connectedness, even if you're doing the right things around security, another organization that is connected to you may cause you problems" (P3). P7 thinks SMEs have a duty to protect themselves on behalf of the businesses with which they deal. "[B]ecause they are part of a supply chain that necessarily needs to be secure, every time they drop the ball on security, they weaken the entire web of trust." (P7). A security failure for one vendor is a security failure for the whole supply chain.

"Sophistication" … real or imagined? Sophisticated actors, simple threats

There was controversy amongst experts when it came to the word "sophisticated" to describe most attacks against SMEs, with some calling use of the term "bullsh—t" (P3). Companies often publicly use the term "sophisticated attack" as a justification for situations where they have failed to do even the bare minimum to protect their data, P3 explains. While there has been much popular media buzz surrounding more "sophisticated" attacks, there was consensus amongst experts that the vast majority of successful attacks against SMEs comes down to basic threats which have existed for quite some time. These include tactics such as simple phishing, social engineering, or brute force attacks (P6). "Attackers will always look for the easiest cracks and entry points," says P9. "What we've seen is that it's usually simpler techniques that have worked for a long time; the taking advantage of the human aspect that seems to be the easiest way to steal information or to get into something" (P4). "The real problem is always going to be between the chair and the keyboard. That's going to be your number one vulnerability every time" (P1).

While the attacks themselves may be relatively simple from a technical standpoint, the planning behind them is becoming more complex. Attackers now have "a different modus operandi" to go after bigger dollars, says P6. "[SMEs are] facing more complex threat actors. Whereas before it might be a low-level organized crime group or somebody looking to make a buck off an entity that's soft from a cyber security perspective, it's now a more complex threat actor who is out there, looking at the supply chain of a large entity or organization or a government agency

and looking downstream into their suppliers and figuring out who might be [a good entry point]. You're not dealing with low level threat actors anymore; they're moving higher up that complexity chain" (P6).

Why are age-old simplistic attack mechanisms still working? The answer is that organizations are still not prepared to prevent or defend themselves against cyber-attacks. With many SMEs failing to put even the basic recommended controls in place, it is a field day for cyber criminals. "I don't need to bring a complex attack process to your organization when the front door is left open," analogizes P6, "I can just push and come in."

The current state of cybersecurity technological adoption by SMEs

Low adoption rates of technologies by SMEs

The Canadian Centre for Cyber Security recommends 13 baseline controls for small- and medium-sized businesses. Amongst its technological recommendations are automatic patching, enabling anti-malware and firewalls, backing up and encrypting, and using two-factor authentication where possible [18]. The Government of British Columbia website recommends minimum controls including email security (email is "the vector used most often by attackers" (P11)), modern endpoint security, security awareness training, and multi-factor authentication [19]. But according to experts, SMEs are already "struggling with and they can't implement" such basic security advice. "I think you'd be challenged to find an organization that even does those four" (P3). Past research has shown that SMEs are inadequate in their implementation and design of security controls [20] and that most small businesses meet the criteria for only level one, or "initial/ad hoc" of COBIT's[1] capability model [20]. However, implementing the above-mentioned base controls would "go a long way" in protecting those businesses against common threats such as phishing, ransomware, and extortionware. It is estimated that 80% of cybersecurity benefits can be achieved through 20% of the effort [18].

In addition to the basic measures already mentioned, experts discussed other useful technological controls, including "next generation firewalls" with intrusion prevention, web content filtering ("something that determines whether you're going to good or bad websites"), up-to-date email content filtering that includes anti-malware, "and then maybe if being online is really important to you, anti DDoS [Distributed Denial of Service attacks]" (P3). P11 explains how Endpoint Detection and Responses [EDR] can complement more classic signature-based protection. [S]ignature-based protection […] works very well, it's like a vaccine in the background. If the threat is known, we can block [it] immediately. The EDR component will come in against everything which is unknown; detection by behaviour." With ubiquitous quantum computing on the horizon, experts also urged that it is vital to start using quantum-safe encryption *now*. "[I]f somebody steals the information that I have today, they don't have to do anything with it. […] They just have to wait for quantum computing to come along and break my encryption and the information still has value. [I]t doesn't have to be used today" (P1). Unfortunately, in the current climate many of these technical controls are "totally [and] completely well beyond anything [SMEs] could ever fathom," says P3. "[F]or SMEs, the technological portion is a black box for them" (P12).

Recent surveys show that between 2017 and 2019, the types of technologies that Canadian companies used largely stayed the same. In 2019, 76% of Canadian businesses used anti-malware software, 73% used email security applications, and 69% used network security solutions. However, they were noticeably lacking in other areas. 65% of businesses did not install security updates on a regular basis [14]. As a response to increased attacks during the COVID-19 pandemic, more organizations (an increase of 41% from the previous year) are making cybersecurity awareness training mandatory [7]. 2020 also saw an increase in phishing simulations, and one-third conducted lunch-and-learn workshops [7]. However, training is not conducted on a regular basis: 40% conduct it annually or less often, and only half do it quarterly. CIRA survey respondents "showed limited awareness of [training platform] vendors" [7].

The majority of large Canadian enterprises reported using most cyber security measures asked about on the 2019 Statistics Canada survey [2]. Meanwhile,

[1] https://www.isaca.org/resources/cobit

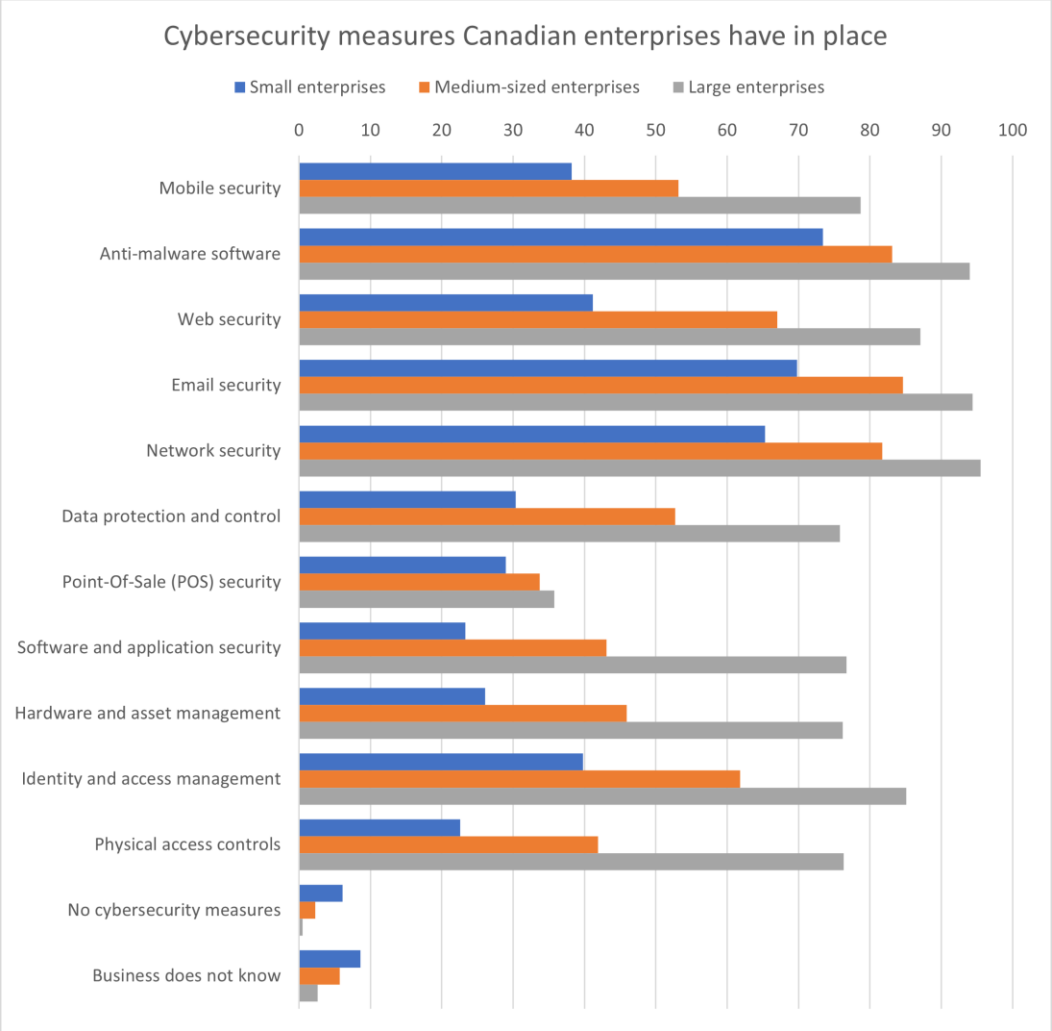


Figure 1. Measures used by small, medium, and large businesses in 2019 by percentage. Data from Statistics Canada's 2019 Canadian Survey of Cyber Security and Cybercrime.

medium and small enterprises were much less thorough. See Figure 1.

While smaller businesses have relatively high adoption rates for anti-malware software, email security, network security, and Point-of-Sale security, there is much more of a disparity between them and large businesses when it comes to other forms of security. A case study of UK small businesses found that most respondents' cybersecurity measures culminated in easy-to-implement "ad hoc" measures including endpoint security measures, antivirus, configuring devices to automatically accept security updates, and regular back-ups [21], with other measures out of scope.

Two areas where small businesses are particularly lacking are detection and encryption. Intrusion detection has been a known challenge for SMEs for several years [22]. The Better Business Bureau reports 10% of surveyed small North American businesses did not know if they had been the target of a cyberattack [5]. Small businesses face the problem of both the complexity and expense of detecting Advanced Persistent Threats (APT) [5]. The ability to detect attacks is becoming more vital as

attacks are getting more targeted, sophisticated, and severe [23].

"That's the biggest issue today, it's detection, it's having proper monitoring in place so that if you get infected, for example, you can reduce the window of opportunity of a cybercriminal that gets into your system. If you don't detect that person for the entire 272 days that it takes on average to detect someone in your systems, then they'll have an opportunity to download all of your movies, released and unreleased, and all of your emails and all of that stuff." (P7). On the other hand, says P7, if the window of detection is reduced to detect, for instance, within a few minutes, the company is able to respond nearly immediately. In such a case, "chances are there [wouldn't be] very much time to exfiltrate information or to damage any information assets" (P7).

Companies may not realize they've been the victim of an incident until months or years later (P4). "Right now, the biggest challenge in business and in security in general is the detection of breaches. Companies have no idea when they're breached, they have no idea when they are owned, they have no idea when they are remotely controlled [...] If you don't know how to detect incidents, you cannot correct them. You can't fix what you don't think is broken." (P7). A lack of detection capacities can undermine the effectiveness of other security controls. "Corrective and compensating controls are largely useless in organizations that do not have detective controls. And focusing exclusively on preventive controls means you can only detect what you know exists. You don't know what you don't know" (P7).

Another major challenge facing SMEs today, considering the prevalence of ransomware attacks and other attempts at data theft, is encryption. SMEs are struggling with "even things like basic encryption, at rest and in transit" (P3). Our focus group members mentioned that while in-flight encryption is "standard" in most organizations, at-rest encryption is much more rarely implemented in smaller businesses. When businesses do have encryption, it is often outsourced: "I think the focus would probably be Cloud, rather than on-premises" (FGP13). With the exception of regulated industries, say our participants, rates of adoption of at-rest encryption amongst SMEs are very low." [I]n our customer base, very few of our SMBs actually show any maturity in terms of encryption for data at rest. [...] [W]ith a few exceptions, your typical SMB would know and do very little about encryption, and even more so, not be so interested in data encryption solutions because it's a mess," says FGP2, suggesting a lack of trusted data encryption solutions for SMEs. Past research on certain consumer-level encryption solutions has found them to be too confusing for average users to use successfully [24], which does not bode well for the encryption of small businesses that may lack specialized cybersecurity-related knowledge and skills.

Shelfware and the 'technological mirage': the importance of proper configuration

We asked experts if SMEs' failure to protect themselves in areas such as detection and encryption was due to a lack of appropriate available technologies in those areas. But experts assured us it is not a supply problem, but rather a demand challenge. SMEs are either not using available technologies at all, or they are using them but not configuring them properly.

Before investing in new technologies, SMEs should start by configuring and using the basic technologies to which they already have access. "[A]t the technological level, there are a lot of tools that are already available in companies, but which have not been put into operation" (P9). 80% of a company's cybersecurity can come from "activat[ing] what they already have in place," says P8. "Configure the office suite correctly, it doesn't cost anything; we are already paying for it and things are already moving [...] Then later on we can bring in new technologies depending on the type of business and the needs" (P9). Logging, authentication, and regular backups are examples P9 gives that can easily be

implemented using technology to which most SMEs likely already have access, e.g., via cloud providers such as Microsoft or Google. Without correctly deploying, managing, and maintaining such basic controls, "the base is not there," says P9. Many of our participants emphasized the importance of maintenance once tools are in place, via patching, updates, etc. "You have to maintain it, which is another problem. This isn't a piece of furniture, folks. You don't put the sofa in your front lobby and only address it when one of the legs falls off, you need to update it" (P3).

When organizations misguidedly invest in new technologies to solve their cybersecurity problems before correctly leveraging what is already there, they are falling prey to the "technological mirage" (P8): "Learn how to close your windows properly before investing in the purchase of an armoured door. Buying the armoured door when the windows are open is what I call a technological mirage." The importance of deploying properly was echoed by our focus group participants: "[Make] sure that you are procuring things and operationalizing them in the way that actually gets the most value out of the tool, because otherwise you end up with shelfware" (FGP3). Shelfware is a colloquial term for software that has been bought or licensed by a business but never installed or implemented to the extent that it should be. "[It's] less about purchasing significant technology, and more about adopting readily available technology that's part of usual software and hardware usage and making sure it's up to date and you're using it. […] So for small and medium-sized businesses, it's less, in my view, about saying to folks 'Okay, you need to go out and buy X'" (P2).

Prioritizing non-technological solutions

Experts were adamant that organizations should be reminded that cybersecurity technologies are not the be-all and end-all against cyberattacks. "It's not all about the technology," says P3. Non-technological solutions can be just as important. P3 lists five "absolute minimum" non-technological controls which organizations should have. These consist of a security risk register ("Folks, know the things that would take you out"), an information security policy, a risk assessment, a security incident response plan, and a security course. "[W]hen you do one of these things on that list, you get a cascading benefit across all of the different audits, whether it's a COBIT[2], a ITGC [Information Technology General Controls] or [even] PCI[3]" (P3).

Tech adoption is "the last piece," states P2. Non-technological solutions should be considered before technological ones. People misunderstand that there are more aspects to cyber security. "Most people run immediately to technology, [thinking,] Okay, this is a technology issue, Cyber Security. And it's going to be solved by a technology solution, some device, or some technology; some software. And that is not so. It's going to be solved by a clear recognition of exactly what the vulnerabilities are and the implementation of training or process, and then the last resort of the technology necessary to protect that vulnerability."

[2] https://www.isaca.org/resources/cobit
[3] https://www.pcisecuritystandards.org/

Challenges to the adoption of technologies by SMEs

As discussed in the previous section, SMEs are woefully underprepared for cyber-attacks and have poor uptake of existing cybersecurity tools compared to larger businesses. What are the driving factors behind this? SMEs have specific characteristics relative to large enterprises which affect their needs and constraints. Previous research suggests cost, need, know how, and availability as the main factors affecting the adoption of cybersecurity tools by small businesses [4]. Limited resources are a well-known and often cited constraint for SMEs when it comes to investing in security. Heidt et al. [3] found that lack of investment in security measures by SMEs was due to limited budget (SMEs perceive IT security as a large financial cost), time (to learn about and implement solutions), and workforce (lack of personnel with sufficient security expertise or time to appropriately handle the SME's security).

Governance and managerial issues are another constraint, including managerial skills, managerial knowledge and awareness of IT or security, attitude and values of management, and short-term focus [3]. Businesses may suffer from a workplace culture lacking cybersecurity awareness, in part due to employees' lack of interaction with websites or information systems, leading to the phenomenon of "out of sight, out of mind" [20]. The effectiveness of companies' cybersecurity may be further dragged down due to employees willfully ignoring security policies [7], the adoption of shadow IT [7], and struggles to comply with recent updates to PIPEDA [7].

Increased digitization without proper consideration of cybersecurity is another challenge. Businesses today are facing an exponential growth of connected devices, networks, services, and data [9]. Many businesses have BYOD policies, which means employees are using their often much less secure personal devices for work [7]. In 2017, 67% of businesses were "concerned" or "very concerned" about the vulnerability of IoT devices in relation to their business [23]. While 2017 saw an increase in the use of password or biometric authentication to secure their devices [23], out of the 37% of businesses that used internet-connected smart devices or IoT devices, only 17% of SMEs assessed the security of those devices [14]. This is an increasingly growing vector of attack. "As a general rule, the more internet connected assets an organization has, the greater the cyber threat it faces" [15]. With most workers working from home, COVID-19 has accelerated this trend and made it increasingly complex when combined with at-home network setups and distance from IT staff.

Lack of appropriate defences happens even with businesses rating technology-rated risks among their most critical [25]. Even with basic tools in place, they are likely to "lack the policies, procedures, and training to secure their information resources" [25]. Often, they simply do not know what to protect [26]. In the following subsections we present the most prominent current challenges discussed by our expert and focus group participants.

Opening the perimeter and hastening digitization: COVID-19 and a changing cyber landscape

The COVID-19 pandemic has created several new challenges for Canadian businesses, leading their IT workers to feel even less control within their organizations and exhibit an increased concern about cybersecurity [7]. CIRA's 2020 report describes the current cybersecurity landscape in Canadian companies as "[a picture] of stretched IT resources and IT workers that have less influence over employees" [7]. Experts have seen a "pretty significant increase" (P10) in cyberattacks since March 2020. "The consensus is about 350% increase" (P8). "[T]he majority of SMBs were not ready, did not have the necessary technologies to protect their workers remotely or to protect themselves against threats that could "originate" outside the network." Below we delve into the main

challenges, according to experts, which emerged during the COVID-19 pandemic.

COVID-19 has greatly accelerated the push towards digitization, which has opened up additional risks for SMEs. "COVID [has been] an accelerator of the digital transformation of businesses. […] [W]ithin a year we probably did what we would normally have done in 5 years" (P10). With an increased demand for online services, 12% of businesses began accepting online payments for the first time, 10% online orders, 3% online reservations and 4% developed their first website [6]. While adopting technologies can make SMEs more efficient and reduce costs [27], they also introduce new vulnerabilities. During the rush to digitize, managers prioritized capacity and "cut corners" when it came to cybersecurity, says P10. But it is critical for SMEs to be "thoughtful about how they are digitizing," says P2. "The rush to push digital process into places where it wasn't before in an effort to drive productivity needs to be done in a thoughtful way that is recognizing of the cyber security risks."

A hurdle towards thoughtful digitization is that many SMEs "have vulnerabilities they don't understand" (P2). While an all-cash dry cleaners that does not keep Personal Identifiable Information (PII) and whose computer system amounts to a register likely does not have to invest in cybersecurity, a restaurant with an online reservation system does. Any system "that is critical to the continued functioning of the business, but may not be in the first instance well understood by the owners or operators of that business to be vulnerable to attack, is a serious concern." An inventory is an indispensable first step in recognizing vulnerabilities and thinking about how to counteract them. "[U]nless [technology adoption] is done with a recognition of the cyber security risks that it creates, it's just a massive new vulnerability" (P2). If companies are not willing to address cybersecurity risks, "don't connect," recommends P3. "If you're not willing to do this stuff, reconsider your business approach and don't do it online."

With most workers transitioning to a work-from-home set-up [7], there has been greater vulnerabilty to attacks due to insecure home Wi-Fi networks, removal from nearby technical support, and heightened levels of anxiety leading to greater risk of falling prey to phishing. COVID "opened up the perimeter" of cybersecurity, says P11, moving from the prior "well-defined" perimeter, marked by physical separation of work and home infrastructure, to a situation where "businesses are impacted by employees' home system" (P1). "[Now] I have entry points into my distributed infrastructure all over the place. That's a lot of entry vectors into my business that can be used to compromise me" (P11). One of the issues is lax standards surrounding the use of insecure home devices (e.g., personal laptops) and network setups (e.g., home Wi-Fi), says P6. Though P11 points out there has lately been a trend of installing agents, antivirus and Endpoint Detection and Response (EDR) on work laptops before sending them to employees, P6 explains that for the most part IT teams weren't going to employees' homes to help configure their firewalls or other technologies. "Standards [were] going all over the map. [H]ow secure is your home?" (P6).

The problem is also social. With employees dispersed and less likely to talk to each other, there are more opportunities for social engineering and ransomware attacks, says P2. "If [companies] don't have adequate controls to prevent it, then all basically the attackers need is an effective lure" (P3). What has been an effective lure during COVID? Pandemic-related emails. "We did a phishing campaign on my security branch of roughly 50 people. […] [It] was on a COVID exposure notification. Let's just say that somewhere in and around 47 out of the 50 people clicked on it. That's the security team. So, what is the likelihood otherwise?" (P3).

Promisingly, SMEs are becoming more aware of the importance of cybersecurity in response to increased attacks during the pandemic. "There really was a 'wake-up call' with COVID. [Before], you had to knock on [companies'] doors to convince them that

cybersecurity is important. Now it's the opposite, my voicemail is overflowing right now. In several sectors, they are practically in panic mode" (P10). This suggests SMEs may be more receptive than ever when it comes to advice about securing their environments. "We no longer run after them to convince them that cybersecurity is important. Now they're in "Oh my" mode [...] Everyone is talking about cybersecurity these days. This was absolutely not the case 18 months ago" (P10).

Lack of resources

Canadian SMEs may be in "Oh my" mode, but this doesn't change a central obstacle they have always faced: a lack of resources. "It's critically important for all organizations to do the right thing; to patch, to look after their systems, to ensure that their systems are built on those principles of confidentiality and integrity... but smaller companies often have more challenges in that area. They don't have teams of people to do these things. They are limited in budget, they're limited in their capability, and they're limited in their ability and so they are a weak point in the system" (P1). Running a business is "often extremely intensive" (P2), taking a lot of time and energy. "Capacity is a serious issue," says P2. "Small and medium sized businesses, by definition, do not have capacity to do a lot more than run their businesses."

Costs

Cost was considered the most "obvious" (P5) challenge by experts and was most frequently cited as a reason for why SMEs do not implement sufficient cyber controls. When SMEs invest in a technology, they not only have to consider the cost of the tool itself, but the costs to operate it, as well. SMEs "cannot typically afford significant outlays in technology or in highly trained personnel to operate those technologies. [...] [I]f it costs a lot and/or it's complex it's not going to work" (P2). Some tools are far beyond the realm of possibility for SMEs for this reason. Advanced threat detection systems, for instance, "are inaccessible in cost. Pricing is not consistent with the reality of SMEs" (P10).

Even if a tool is within the realm of possibility budget-wise, costs associated with cybersecurity may be considered optional or lower priority relative to other operational costs. "Money. It's expensive. [...] I've seen small, medium businesses that have been told by their service contractor, you need to do these things. You need to replace all of your equipment on a three-year cycle, we need to patch everything and bring all of your licenses up to date and do all that and it's going to be expensive. And small, medium businesses run on a tight margin usually" (P1). Furthermore, SMEs may be "completely oblivious" to cybersecurity issues because "[t]hey're focused on, 'are we going to be able to make our bills at the end of the month?'" (P3). "I think the basic thing is when you're just struggling to survive as a small business, these extra costs, or what are perceived to be extra costs, are just hard to swallow when they don't necessarily seem directly related to what you're doing" (P5).

Lack of expertise and staff

Lack of expertise negatively affects all areas of cybersecurity, including recognizing risks, operationalizing tools, filling out security audits, and disclosing incidents. Most business owners are not technologists themselves, says P2, meaning their knowledge about cybersecurity is limited to begin with. On top of that, "[SMEs] don't have the size and scale typically to foster even a single dedicated person focused on security, let alone a team" (P3). "[They] rely on outside service contractors or depending on the size of the business, a guy, it's not even a full contract, it's just 'a guy' to do all of this work for them" (P1). SMEs, if they have the budget and knowledge to do so, may share a CISO with several other companies. "Why do we think it's reasonable to expect that every organization is going to have their own chief information security officer?" P3 asks, pointing out that SMEs are often

unreasonably held to the same standards as larger companies.

Budget restrictions aren't the only thing holding SMEs back from hiring cybersecurity personnel. There is also a lack of cybersecurity personnel available for hire in Canada. This may be especially true for SMEs in rural areas [3]. Though P11 says ideally every company would have at least one dedicated security person, in 2021 it "would be impossible" due to a lack of resources and experience in the market. However, at the very least, says P11, companies should "have access to external resources that they can do business with" such as consultants or advisers to know their needs.

New tech requires more hands-on deck, explained focus group participants, but this fact is typically ignored in SMEs. "[I]t's very rare for an organization to go out and hire new bodies to manage [new technologies]. It's going to be going along the paradigm of doing more with less. […] [That responsibility] will just be tacked on to the long list of things that the operational teams are currently responsible for" (FGP4). Putting the brunt of responsibility on individuals who are already overwhelmed makes SMEs more vulnerable to attacks by translating into oversights such as large lapses of time in detection (P4).

Outsourcing in the wrong ways

Unable to support many, or any, in-house staff, SMEs tend to "outsource heavily" to meet their cybersecurity needs, says P3. But they are not necessarily outsourcing in the right ways. Because SMEs "don't know what questions they need to be asking" service providers to ensure their business is secure (P1), small businesses often end up hiring local IT firms or general tech support services who "don't know sh—t" about security, says P3. Such service providers are generally unfamiliar with cybersecurity frameworks (e.g., ISO or NIST) as well as other available guidance such as CyberSecure Canada, P3 clarifies. Focus group participants also mused that IT providers only have "a tangential understanding of security" (FGP5). On the other end of the spectrum, more widely trusted firms can be far beyond the budget of the SME. "The cost of remediating an incident [via a larger firm] will put them out of business" (P3). It does not help that many incident response service companies that are within reach of some SMEs' budgets have been "totally overwhelmed" since the start of the pandemic, turning away new customers. "We see SMEs calling, e.g., XXX or YYY [respondent names two well-known local cybersecurity companies] saying "We are the victim of ransomware" and then the answer is, 'No, we are overwhelmed'" (P8).

Another issue is that SMEs may misunderstand the risks associated with outsourcing. Many SMEs may wrongly assume that by outsourcing cybersecurity, they are also outsourcing accountability. "When you are hiring a company to manage your systems, you're not buying insurance," says P7, "That company does not actually accept any responsibility for mishandling your systems." One focus group participant felt uneasy about outsourced providers' lack of investment in the company. "Sometimes there's a motivation from an outsourced provider to just get the ticket closed, to tick off the boxes and then move onto the next client kind of thing. […] When it all boils down to the bottom, they're not actually part of your organization, they're an outsourced team" (FGP6).

This is especially important to remember when it comes to outsourcing some particularly sensitive functions, such as information security management. "As far as introducing and maintaining controls that protect your organization and the assets that you are handling on behalf of clients and customers, no one else should have access to that" (P7). He warns SMEs that they will not be off the hook for any data breaches that occur to the outsourced provider. "Your clients don't give a [damn] about that. […] The buck stops with you; you had their information. They didn't authorize you to give it away to people."

To help reduce the likelihood that they are introducing new vulnerabilities into their business by outsourcing, some cyber-savvy SME focus group participants explained their vetting and onboarding process, which included assessing how potential outsourced providers are hosting, storing, and securing their data (FGP7). FGP6's business conducts a bi-annual Request for Quote (RFQ) for an IT security assessment, and FGP8's business runs through their service-level agreement and operational matrix with new outsourced vendors, as well as setting out objectives and key results. Many businesses today will have to complete a security or risk assessment as part of a supply contract with a larger organization, but FGP16 infers these should be taken with a grain of salt as they are "always a race to the bottom line. How can I get the right number of ticks on the page so that I don't risk losing the contract?"

Misunderstandings by SMES as to the responsibilities of Managed Service Providers (MSPs) can also lead to tensions between the two when it comes time for the business to complete surveys, audits, or requirements for cybersecurity certification, explain P5 and P6. Business owners may feel overwhelmed and have a lack of understanding and time necessary to fill out "15 or 50 pages of controls," while MSPs may feel that filling out such forms is additional work not part of the original agreement (P6). It may come as a shock to SMEs (and their wallets) when they are hit with additional charges for such a service.

To avoid the downsides that come with outsourcing, focus group participants expressed a preference for keeping in-house cybersecurity staff where possible. "Someone on the inside who understands as much of the technology and the policies and all that would be able to see if we're getting the value that we're paying for, is the idea. And to just be in control of our own security [...] We want to make sure that security is at the forefront, is most important to us. So, it's easiest to keep that in-house" (FGP6).

Attitudes and governance: A dismissal of cybersecurity and accountability

SMES face low levels of formalization when it comes to cybersecurity. This takes the forms of lack of budget planning for IT or security, mixing of roles and responsibilities in a single position leading to a de-prioritization of security, and undocumented organizational and technological processes [3]. In 2019 only 12.4% of small Canadian businesses had a written cybersecurity policy in place compared to 54% of large businesses [14]. SMEs also see a low uptake of cyber insurance, low executive oversight or chief information security officers, inadequate data encryption measures, and very few are following best practices guideline [28]. Embedded in SMEs' governance across Canada is a lack of prioritization of cybersecurity. "It's innocence [...] You may not think [the information you are holding] has value. Somebody else might" (P1). Many SMEs won't have this realization until it's "too late," says P2. Whether or not SMEs consider themselves a target is inconsequential to cybercriminals, as illustrated by respondent P3: "Flying under the radar is not a successful strategy. Neither is hope. And also, pretending: 'Well, why would they want to attack us? We're just X distributor' isn't going to save them either."

A top-down dismissal of the importance of cybersecurity is a chief obstacle when it comes to implementing cybersecurity technologies to their full abilities. "Coming from a financial services organization, there really isn't any technology that's been easy to deploy," says FGP9. "The actual technology implementations themselves haven't necessarily been complicated [...] [but] getting the businesses to use that [technology] is a different kind of sales job that needs to be done." Communicating threats to boards, managers, and executives is vital, says P11. "There is no point in going crazy with the people in IT if the management, the admin, the head of the company does not understand the problem and does not buy into it" (P10). There is a "lack of ability to explain the needs to managers, costs versus return, what we will see in

terms of risk minimization or even understand how governance can help them develop robust business strategies, but which will also dictate the technological choices they will make" (P11).

One challenge is convincing business owners to allot the money, and the other is to use the technology to its full capability. This requires factoring in the "entire lifecycle" of the tool, as well as resources such as personnel needed to operationalize the tool effectively, says FGP3. "Containers, tuning, maintenance, alerting maintenance, working with other stakeholders. This is not just putting the tool in, [but] more 'how do you configure it the right way?'" (FGP10). It's all part of a "proactive learning perspective," he says. "[It is] the management of how we want to apply these technologies, how that is going to affect the weekly operations, how is that going to change the business methodology a little. And that, if there is no commitment from the board or the executive, it becomes an impossible challenge to meet" (P11). Getting cooperation from business members on access control measures can be a constant hurdle because people don't like to have to change the way they work, says FGP16. Even something as simple as patching can become a "monumental task" (P11). SME cybersecurity staff face friction during deployment, implementation, configuration and tuning, "and enabling the business to the point where you're not completely crippling the tool" (FGP3). Without business owner buy-in, SMEs will be hard-pressed to deploy solutions such as Data Loss Prevention, which require "a huge amount of process up front" (i.e., identifying, tagging, and categorizing all data assets), says FGP11. "[M]ost organizations just don't have the appetite or resources to do it thoroughly."

Subpar cybersecurity governance can also take the form of poor choices when it comes to vendors or partners. Business owners may underestimate the importance of compliance to security requirements. "They're like, 'but Bob and Mary in Chilliwack can't afford to do that [the security requirement].' And I'm like, […] 'Folks. Have you ever considered that there are some companies that we can't afford to do business with?"' (P3). In an attempt to be "responsible for nothing," P7 has had experiences with companies who purchase cyber-insurance hoping it absolves them of any responsibility to establish their own cybersecurity measures (P7). However, as P3 puts it, "that's not going to make you whole after an incident." Neither is it going to return customers' and clients' stolen identities, says P7. By facilitating such events via breaches of their data, companies have "done [clients] a terrible disservice. [I]t's irreparable. It's not something that's reversible" (P7). Companies will only be able to "seek solace in the fact that so many other companies are equally negligent." SMEs should hold themselves accountable for the data they generate, store and transfer, before it's too late.

Our respondents were insistent that it is time for Canadian SMEs to become more mature in their cybersecurity governance. "[W]e're still in the Stone Age of business in general and, specifically, in the adoption of proper information security practices, says P7. "Up until literally months ago, it was not well understood that security and to a large extent privacy […] needs to be handled by the business, as a business process, as an operational part of doing business" (P7). Cybersecurity needs to be seen as more than just an "add-on" (P11) and should be part of the "management structure of the company," says P9. Businesses should be working to create a culture of cyberawareness, says P1. "[S]ecurity should take precedence over infrastructure choices" (P11). Many larger companies have already had this change in mentality, but SMEs are lagging. P11 says this means SMEs should be thinking: "Every time we make an operational change, either a business process or a technology, it has to go through security first."" "You have to address the initial problem of educating governance and the rest will follow" (P10). SMEs can get started by creating a written cybersecurity policy. "[H]aving that communication and cohesion throughout the business, even if it's small, can add a lot of value in terms of keeping the business safe" (P4).

The problem of trust: distinguishing marketing from usefulness

One crucial component of being able to make decisions surrounding cybersecurity technology and service adoption is knowing who to trust. Due to budget constraints, small business owners fear buying tools they don't need [4] and feel they "don't have access to reliable unbiased sources for advice" [4] [21]. Compared to large enterprises, SMEs rely more heavily on trust formed within personal relationships, over provider recommendations or third-party advice [3], when making IT security investment decisions. Both our expert interviewees and focus group participants discussed the issue of trust in depth.

"[SMEs] don't know who they can trust," says P3. "The biggest problem [is] 'what's real and what's not?' There's all kinds of tools that you hear about, and you don't even know if they're just hoping to be bought by somebody or if they're actually working in the wild" (FGP12). SMEs on the market for new cybersecurity technologies are bombarded with jargon like "AI," "military-grade," "big-data," and "next-generation," as well as fancy Graphical User Interfaces, say our expert and focus group participants. "Everyone is positioned as a 'magic bullet," says P11. "[I]t can be a challenge to separate what is useful from what is just marketing." Misleading marketing practices take advantage of people's assumptions of best practices being in place, says P7. "[P]eople just make assumptions based on how good a logo looks or how many times a business repeats its marketing message. Or the fact that they're actually saying, 'we have the most secure platform in the business,' when in fact it could be deceptive practice that comes with any number of unverifiable claims that are sustaining it" (P7).

SMEs can be swept away by promises of convenience, pricing and innovation (the three "enemies of cybersecurity"), says P7, but need to be "more skeptical" when hearing about them. Focus group participants had a range of strategies for judging legitimacy of potential vendors and partners, including using a third-party risk group to look into "historical business dealings," "red flags," viability, and policies and procedures regarding cybersecurity and disaster recovery (FGP13), or conferring with an already outsourced IT provider (FGP6). FGP14 recommended SMEs coming prepared to demos with a particular problem they need solved. If a vendor is not able to demonstrate how their product would fix it, "that's a good indicator that it's probably not for you." FGP15 agrees: "The salespeople will sell you everything and anything. But when it actually comes to the demo, that's where the rubber hits the road, right?"

Unfortunately, doing these checks can be difficult for many SMEs lacking expertise. "A lot of small, medium business operators or leaders simply rely on their service provider to just guide them in the right place. [...] And they don't know what questions they need to be asking [to ensure their systems are as secure as possible]" (P1). "When adopters aren't experts, they have to put their faith in the security of the technology," says P7. P6 says many small business owners assume many devices, such as routers, are secure out of the box, which is often not the reality. This can lead them to introduce new vulnerabilities to their business without even realizing it. P6 blames a lack of technological standards, saying owners should not have to worry that they have to "become a cyber expert as a business owner too" (P6).

When we asked how confident focus group participants felt when it came to making informed choices regarding technological investments in cybersecurity, their answers ranged from "80-85%" (larger company) to "a constant state of terror" (smaller company). "There are a lot of unknowns," says FGP6. Those experiencing the Dunning-Kruger effect (a cognitive bias where people overestimate

their own knowledge in a given domain[4]), on the other hand, may feel completely confident. "[P]eople who really have no clue what their risks are might feel that they're making great decisions! Did my research, spent a couple hours on Google, bought the systems I need, we're good! And I speak from experience, because that was me. It's not until you realize that you're not [secure] that you start to question things" (FGP16).

SMEs do not know where to start

"[SMEs] are ill prepared. They don't know what to do, they don't know how to do it, they don't know who they can call for help." This is especially true for non-profits and charities, says P3. Although SMEs are lacking in preparation and knowledge, experts we interviewed described an increasing trend of Canadian SMEs caring about being cybersecure. "I can tell you this: SMEs *want* to become secure. They want to" (P6).

Unfortunately, wanting, in itself, is not enough. Plainly put, the vast majority of SMEs do not know where to start. "They're just not sure what are the first steps that they need to take - some of them have made the jump that, 'Okay, we know that cyber security is now important, that there are all these cyber threats,' but they're just not sure what to do about it" (P5). Even if SMEs have an idea of how to start, they do not feel they have the support they need to get there. "They want to, but – it's a hard road to get there, it's a heavy lift and they don't feel like they're being helped. We have almost never seen a company say 'oh I don't believe in cyber hygiene'... They all want to get there, they just don't feel they have the support mechanisms or the incentives in place to get there" (P6). P3 echoed this sentiment. "[T]his is a big problem area. It is the area of the folks that are screwed and there's nobody helping them."

A cybersecure-positive attitude is only the beginning of a long road to becoming cybersecure. "[SMEs] need to have sufficient curiosity to at least say, well, what is it that I need to be asking? How do I select a tool, other than by copying the phone number down from the side of a bus? So yes, they don't know what questions to ask, and for the most part that's an easily remediated problem. We just need to have more awareness around this issue" (P7).

[4] https://www.britannica.com/science/Dunning-Kruger-effect

Solutions and Recommendations

In this section, we discuss solutions to respond to the threats and challenges presented previously. Following each subsection is a set of recommendations based on our respondents' insights.

Creating technologies better suited to SMEs: lower cost and easier to use

Despite the fact that small and medium-sized enterprises make up the vast majority of both the Canadian and international business landscapes and face many of the same types of threats as larger companies, many security tools continue to be designed primarily with large businesses in mind, which have "complex IT infrastructures" [4] and large budgets. SMEs are often treated as "little big firms," incorrectly assuming that SMEs have access to the same resources as large enterprises [3]. This ignores the unique constraints of smaller businesses. Although freeware tools exist, they are often too complicated for SMEs with limited IT knowledge to implement effectively [4], and certain types of tools, such as those on the network layer, are scarce for SMEs [4]. Experts attribute lack of encryption (P7) and lack of investment in advanced threat detection (P10) largely to costs considerations. "How do we adapt them when we know that they don't have security or technology managers? [...] [Y]ou have to look at cybersecurity differently for SMEs" (P12).

"[T]wo key determinants that I think are really important for SMEs are cost and simplicity, says P2. "[I]f it costs a lot and/or it's complex, it's not going to work" (P2). The current market offerings do not reflect these needs. For one, the costs of cybersecurity tools are often beyond the reach of SMEs' budgets. "There is really a disconnect between what [SMEs] have an ability to pay as customers and what is offered to them" (P10). One possible solution to initial costs would be to encourage innovation in open-source tools for SMEs – something that the Australian government is already doing in regard to open-source software in general [29]. Nevertheless, additional costs are required for ongoing management of the tools. Current tools, open- and closed-source, are rarely compatible with the employee configurations of smaller businesses. "[T]ech folks are developing tools that are made for big companies with 2-3 cybersecurity staff who are knowledgeable, who are always up to date. But that does not correspond to the IT person of an SME who does almost everything" (P8). It is "a complexity thing," agrees P4. Large businesses can afford the dedicated cyber staff to deploy complicated technologies, but smaller businesses are looking for simple solutions. "[We need] to have technologies adapted to the realities of SMEs, therefore equally effective, but cheaper, simpler" (P8).

Beyond requiring too many staff to operate, many pieces of security software are riddled with poor usability which can include reliance upon technical terminology, unclear and confusing functionalities, lack of visible status and feedback, forced uninformed decisions, and lack of integration [30]. One technology that may have room for improvement in the usability space is multi-factor authentication (MFA). Although it is implemented in "almost all internet services," says P9, "its use is not so widespread." MFA apps can be "clunky," "a hassle" (P6), or cause "hiccup[s]" (P1) in a workday. "It's one of those things that nobody wants to do because, ugh, one more place to log into" (P1). "People just can't be bothered waiting for the code to be sent to them," says P6, leading to employees using unsecured communication channels as a workaround. But P1 looks forward to a day when multi-factor authentication becomes "as normal as putting on a seatbelt."

The prox card reader is a "ubiquitous and useful" technology which has reached such widely accepted status today. "Where would we be without them?" P6 asks. "Everyone has them dangling from their hips, they're all encrypted data in terms of who owns the card and you come up and you get close to the

reader and bing, the door opens. Nobody questions the value of that technology or the security of that technology or the cost of it." Focus group participants gave more examples of easy-to-use and effective technologies, naming phishing simulation and education products and services – "there's very little integration and [little to] nothing touches your systems" (FGP17), and Web Application Firewall or "WAF" technology (FGP13) – "[I]t's super easy. Just get the DNS set up et voila. Basically, there's no implementation worries into pushing that type of solution in production." Although experts and focus group participants agreed that SMEs tend to have very poor uptake of encryption at rest, since COVID, FGP2 has seen an exception in the exchange of encrypted documents via electronic signature platforms (e.g., DocuSign), suggesting it is also relatively easy to use. Canadian SMEs also have a high uptake of anti-malware and email security. The latter is an easy win for smaller businesses because it "is pretty much built into everything anyway," says P4. Whether a technology is an "easy off-the-shelf solution" or "involve(s) a little bit more investment or thought" to implement can make the difference as to whether SMEs adopt it or not, says P5.

Designing cybersecurity technologies in a human-centric way is key to getting uptake from smaller businesses, says P6. "Facial recognition to login takes you 30 seconds to set up and then you never touch it again. That's beautiful. [U]nless technologies are like that, you're going to struggle to get the average business folks to use it." The importance of human-centric cybersecurity has been gaining increased traction in Canada: in the past year alone, it was declared one of the areas of focus by ISED's budding Cyber Security Innovation Network[5] and is the main focus of the SSHRC-supported Human-Centric Cybersecurity Partnership (HC2P) [31], which aims to generate research and mobilize knowledge through the collaboration of scholars, government, industry, and non-profits. These recent initiatives offer exciting prospects for innovation of more human-centric cybersecurity solutions in the near future, and could be leveraged to help create easy to use technologies for SMEs. P10 thinks "there is a lot of effort being made" by Quebec companies "who are actively working to develop much cheaper products that are much more suited to the reality of SMEs," but says the current effort is "not yet adequate"; Canada requires many more companies with the same aim. Canadian cybersecurity innovators can ensure they are following established usability guidelines [32] which can help make security software easier for smaller businesses to use. "If it's really intuitive and customer centric, human centric, they will use it" (P6).

RECOMMENDATIONS

- **Offer** lower cost alternatives to the tools that have been designed for larger businesses (e.g., by encouraging SME-centred innovation in open-source software, or by leveraging government subsidies to Canadian cybersecurity technology creators and buyers) ;
- **Create** tools which are less complex, more usable and can be operated by fewer people;
- **Fund** more usability research dedicated to the cybersecurity technologies heavily used by SMEs, and support independent research or benchmarks comparing the tools and services offered by different providers in an unbiased manner.

[5] https://ncc-cnc.ca/

Standardizing and regulating cybersecurity technologies

As discussed in the Trust section (Challenges), SMEs find it difficult to know who to trust when it comes to cybersecurity products and services. Making technologies lower cost and easier to use will only solve part of the puzzle. Another part is ensuring those technologies are trustworthy. "There are a lot of charlatans out there," warns P9. "It is clear that [SMEs] need programs that can help them, that can ensure that they have the right services when it comes to cybersecurity." P3 voices a similar sentiment. "Who is that unbiased third party that's going to give them the straight goods?"

This can be done through the standardization of technologies. P6 illustrates why standards are so important to establish. When building a house or buying an electrical appliance, "you won't buy anything that goes into your wall or plugs into your wall that's not CSA[6] or ULC[7] certified," he says. Such certifications indicate that an engineering review has been done to ensure the product meets national safety standards and will not create a "fire hazard" in the user's home. They are required for electrical products in Canada [33]. Without certified products, "no one's going to build your house and no one's going to insure your house, as you're likely to have an incident." However, there is no comparable standard in Canada in terms of the security of technologies and services such as IoT devices and online data storage, says P6. This leaves SMEs in a vulnerable position. "There is no: 'I can trust that I can use that company, because they have the xyz standard on data protection'" (P6).

The lack of standards is particularly concerning, given that many business owners may assume technologies sold in Canada *are* being government-checked and secure-by-design. "[I]'m trusting a lot in government to make sure that those standards are in place," says P6. Regulation can help protect SMEs from vendors or service providers with dubious security practices. "[T]he reason we don't have a bank on every street corner owned by local people is because there are rules around starting a bank. And so, to start a website (FINtech) that calls itself a bank is deceptive and dangerous" (P7). However, there are no rules in Canada when it comes to declaring one's business a cybersecurity entity or in making claims about the level of security that one's product provides. A compulsory standard similar to that which exists for banks or electrical products should be put in place for cybersecurity technologies, say experts. "[These are] things that I believe the Federal Government can actually mandate, so you could demand that any consumer products coming into this country that are IT enabled or Internet enabled will be done with security by design principles and it will come out with factory settings that are secure, not insecure" (P6).

Within Canada, there are currently efforts to make these technological standards more widespread. The Canadian Centre for Cyber Security (CCCS) works towards certifying IT products against public cybersecurity specifications and standards such as Common Criteria [34]. CyberNB also provides Common Criteria testing and certification, as well as cryptographic algorithm and cryptographic module validation in collaboration with NIST [35]. Such programs ensure technologies are tested for safety and security as they are been developed so that those aspects can be built into them – something known as "security by design." P6 thinks this should be a component of degree programs: "How do we make sure that when we're going to the software engineering faculty and we're including code testing

[6] https://www.csagroup.org/

[7] https://canada.ul.com/aboutus/ulcmarkproductcertification/

and code validation and pentesting as a part of an actual engineer's learning, and part of their degree program – Versus: they know how to build some cool tech, and they can stamp their drawings. But what about testing and validating of a technology against active threat actors?" (P6).

Making technologies secure out of the box (e.g., the router that comes with a complex password, rather than a password that can be easily guessed) will be much more effective than education in this aspect of cybersecurity. "If we spend all the time in the world trying to educate [SMEs] so that they make proper selections [...] versus just mak[ing] the damn devices secure, I think [where] you're going to find better uptake, is to make the devices secure" (P6).

RECOMMENDATIONS

- **Create** Canada-wide standard for secure/secure-by-design technologies, or widely adopt existing one such as Common Criteria;
- **Require** vendors to certify their products in order to sell or market their products as "cybersecurity" solutions/technologies;
- **Create** easily-accessible up-to-date database of available tools that have received certification;
- **Add** education about security-by-design to university or college curriculum; train software engineers to design more secure products and services.

The carrot and the stick: Mandating and funding minimum cybersecurity measures for Canadian SMEs

"We are 10 years behind the United States" in terms of privacy and security legislation, P7 stated. In 2009 [36], the U.S. adopted a law mandating companies to report data breaches to victims and regulators; in Canada, similar legislation did not come into effect until 2018 [37]. This was an amendment to the Personal Information Protection and Electronic Documents Act (PIPEDA), which applies to private-sector organizations in Canada that engage in commercial activity [38]. PIPEDA requires organizations to report security breaches of personal information "if it is reasonable in the circumstances to believe that the breach of security safeguards creates a real risk of significant harm (RRoSH) to an individual" [37]. However, as discussed in earlier sections, SMEs often do not know they have been breached, and if they do, likely lack the knowledge to accurately determine RRoSH. Combined with the threat of reputational damage from making data breaches public and the cost necessary to invest in cybersecurity measures to prevent them, SMEs may prefer to stay in the dark about breaches altogether. "[C]ompanies, of course, will say, well, if I don't invest in technology to detect data breaches, then I don't have to report it!" (P7)

PIPEDA has been criticized in the past for its primarily reactive complaint-based enforcement system, with some questioning the effectiveness of this approach to regulatory compliance [39]. Research shows that average Canadians' understanding of privacy may not align with PIPEDA's Fair Information Principles (FIPs) and that consumers "have low efficacy to hold organizations accountable for privacy violations" [40], meaning violations may be underreported. Additionally, many SMEs hope for the best until they have a breach, when customers', clients', or employees' data has already been exposed. "In Canada, we don't have enforceable privacy compliance, even though we have over 20 different privacy laws. This gives Canadians a false sense of privacy" (P7). P3 agrees: "[W]hat's really missing here is the regulator, the compliance or enforcement arm" (P3).

PIPEDA states that businesses must adhere to its 10 Fair Information Principles (FIPs) to protect personal information, which include the limitation of data collection, use, disclosure, and retention, and the safeguarding of information. However, the latter does not specify what safeguards must be used; this is left up to the discretion of the individual organization [41], no matter their level of cyber-awareness. Given the lack of capacity that characterizes most SMEs, this is concerning: "Compliance means different things to different people. [...] Some people might be using a self-assessment to basically pat themselves on the back for doing the right thing, and others might use a professional external independent auditor to validate the existence and effectiveness of cyber security controls" (P7). The lack of proactive checks for compliance is especially unsettling in businesses which deal with healthcare data or data involving children, says P7. Other SME vulnerable groups may be even more at risk: PIPEDA does not cover non-profits and charities at all, unless they conduct commercial activities [42].

Countries around the world have been developing simplified frameworks to help smaller businesses meet recommended cybersecurity guidelines. The UK government created "Cyber Essentials," a simplified version of the ISO 27001, consisting of five basic controls [43]. The US Department of Defence's Cybersecurity Maturity Model Certification (CMMC) is based on NIST standards and has 3 different levels of maturity to help match a business' risk level [44]. Canada's equivalent is ISED's CyberSecure Canada, a cybersecurity certification program designed especially for SMEs [45]. While the former two are mandatory for certain government contracts and businesses in the defense supply chain, respectively, CyberSecure Canada is still completely voluntary. P6 says this may be harming uptake, especially given CyberSecure

has more controls than its UK counterpart, which struggled to get uptake before it became mandatory following the WannaCry ransomware incident at the NHS [46]. "[I would] caution trying to put too many controls in place or too many mandatory early controls" (P6). Simplicity is key to avoid overwhelming SMEs. Currently, "a voluntary Cyber Security certification initiative for small and mid-sized companies is just not getting the uptake that we need" (P6).

Most SMEs will not put measures into place until "they get breached into oblivion or there's legislation," says P3. Voluntary investment will not happen until the "pain point becomes too great," echoes P7. As long as companies do not have to pay for data breaches except with "people's identities," he says, data breaches will continue. And indeed, SMEs may be underestimating the importance of cybersecurity *because* it is not mandatory. Businesses have an expectation that important measures would be the law. "[SMEs] are looking for, well if this was really important, we would be legislated to have it, like our insurance" (P3). Until it's "forced onto companies to become compliant, they just won't do it" (P6). Mandatory does not mean the transition has to be sudden. P3 envisions a gradual prompting for businesses when they go to renew their license, starting with an educational pamphlet the first year, and a reminder the second year. "And then the third year is like, if you haven't done your cyber security stuff, no business license for you" (P3). Additionally, the federal or provincial governments could make CSC certification mandatory for RFPs, says P6. However, when mandates are put in place, they must be enforceable. "[F]rom a compliance perspective, it needs to have teeth, like GDPR does," says P7.

For the most part, Canada is currently relying on the compliance requirements of larger businesses for SMEs to implement minimum recommended security measures. SMEs may find that they are unable to do business with a growing number of companies if their security is lacking. Currently, "the only thing that will motivate behavioural change in the SME sector towards better cyber security practices is pressure from their clients," says P7. "They are all requesting evidence of independent audit, they're all requesting proof that they are compliant and, of course, evidence that they have a privacy policy that's being enforced" (P7). P9 agrees in the power of compliance requirements from clients. "[W]hat spurs small businesses the most is when their big customer asks them to fill out cybersecurity questionnaires to move forward with the sale. So, there it becomes a priority" (P9).

Canada's current uptake of cyber security certification programs is "very weak," says P6. He compares it to the formerly voluntary uptake of physical supply chain certifications (i.e., C-TPAT[8], FAST[9]). "[T]hen 9/11 happened. […] Well guess what? Everyone now found religion in a real big hurry, and they all went and got C-TPAT certified, because the shipments weren't going [through]" (P6). Canada has a chance to learn from its own past mistakes (e.g., physical supply chain certifications) and from the mistakes of other countries (e.g., NHS' WannaCry attack [46]), in mandating minimum security measures *before* a major crisis hits. But experts are worried measures won't be put in place proactively. "I don't think we're going to get here with legislation until people get pissed off and raise this as a material issue of concern. And when that's going to happen is after they've been breached like seven times, or more, every single person out there, so. it's painting a pretty bleak picture" (P3). "Our big fear is that unless this is made mandatory, or some type of financial benefits to a company, […] there will be no uptake until the next cyber 9/11 happens and then it'll be far too late" (P6). SMEs who get cyber

[8] https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat
[9] https://www.cbsa-asfc.gc.ca/prog/fast-expres/menu-eng.html

certified now will be ahead of the curve. "[Cybersecurity is] not just a risk; it's an opportunity. If a small business adopts the proper cybersecurity protocols and can prove it, that creates a competitive advantage for them, because suppliers and vendors are looking to source from secure operations." (P2).

When mandates do happen, they need to be implemented in tandem with supports to help businesses get the measures in place. SMEs are, after all, limited in resources. This could be in the form of financial incentives, or tax rebates (e.g., SR&ED[10]), although participants explained many SMEs find the latter too time-consuming. P6 describes a hypothetical scenario in which businesses approach an institution such as the Business Development Bank of Canada (BDC[11]) for a loan, and are subsequently asked about their cyber security needs and presented with a list of approved providers. "[I]f there's more cost now because I have to be cyber hygiene compliant, then when BDC writes me a check as a loan, it gives me enough money so I can actually do it the right way. Otherwise, I'm underfunded, and now you're telling me I need to get up to this level, but I didn't receive the money to do it. I can't do it until I'm cashflow positive and that could be two or three years from now, and that could be too late" (P6).

Instigating legal requirements for minimum cybersecurity controls could help offset recent rises in successful cyberattacks and breaches of Canadians' personal data. "[W]e saw the threat environment increase during COVID," says P6, "but it's fixable if there's a base standard of hygiene that's been made mandatory in the organizations."

RECOMMENDATIONS

- **Create** legislation with proactive compliance and enforcement to catch problems before they happen, e.g., by performing audits of cybersecurity controls;
- **Provide** clear guidelines of what measures are to be put in place, e.g., mandate Cyber Secure certification to prove minimum adherence to recommended controls;
- **Increase** fines or punishment for non-compliance;
- **Make** Cyber Secure Canada certification mandatory when applying for business loans, licenses and/or government funding/contracts;
- **Provide** discounts on insurance for those who have completed cybersecurity certification
- **Provide** financial support to businesses to help them implement minimum cybersecurity measures.

[10] https://www.canada.ca/en/revenue-agency/services/scientific-research-experimental-development-tax-incentive-program/claim-sred-tax-incentive-how-claim.html

[11] https://www.bdc.ca/en

Ramping up knowledge mobilization efforts

"[For an SME], computers are a tool to doing the business. And I think [that] in some cases, […] they're afraid of the word, 'cyber,' because it sounds like you're impeding the tool. [I]t's just a scary word. And it doesn't need to be. […] We need to start taking away that sense of fear and instead replacing it with a sense of empowerment. And knowledge. Knowledge is empowerment," says P1. As SMEs do not know where to start, improving messaging and advice surrounding cybersecurity for them is vital. "They need to know that they need to do something. Then they need to know what they need to do. Then, how to do it," says P3. Below, we present ways in which participants indicated that Canadian knowledge dissemination efforts could be improved.

Outreach: Getting existing cybersecurity advice in front of SMEs

Experts and focus group participants pointed out that several informational resources are already available to Canadian SMEs looking to improve their cybersecurity, including resources from the Canadian Centre for Cyber Security (CCCS)[12], Ryerson's Cybersecure Catalyst[13], the Canadian Cyber Threat Exchange (CCTX)[14], and the Canadian Internet Registration Authority (CIRA)[15]. However, there is a missing link in terms of communicating the existence of these resources to SMEs, they say. "The problem is that a lot of people don't know [about these resources]. […] A lot of times I meet companies and tell them, look, go look on the CCCS site, you'll be surprised at how much information you'll find. When they go, they're happy, but they don't know about it" (P10). Experts explained that SMEs simply are not coming across this information on their own, instead going to other business owners, Google, and generally "less reliable sources" (P1). "I don't think people go to government sources as readily as they could or should."

The expectation that SMEs will find this information on their own goes counter to what we know about these businesses' lack of time and knowledge. "[I]t's not enough for us to have good information. […] It's up to governments, chambers of commerce, industry associations and others to put that information in front of small businesses, not wait for small businesses to go and sort of figure it out for themselves" (P2). "I think people need to be aware that there are reliable places to go for these things," says P1. We should not expect "that small business people are going to just wake up one morning and say 'you know what, I should be more cyber secure' and then go off and try to find for themselves. We've got to meet small and medium-sized businesses where they are" (P2).

Current guidance is "mostly preaching to the converted," said one SME focus group participant. "People who already know a lot about security would go there and find this information. But if you're a small or medium sized business, you have no idea about anything to do with security; you wouldn't even know where to look and what to look for. So, I think the problem is, it's very passive information; you have to actively look for it. And you have to know what you have to look for. Whereas if there was some sort of outreach; if someone was actively reaching out and saying, 'This is guidance, this is how you go about setting up your security program or your IT infrastructure,' I think that would be more helpful in this space" (FGP14).

P6 calls for a "massive education process" of entrepreneurs and business owners; P2 likens it to "a public health problem." "It's about massive education of people and the small things that people can do to help themselves, and help their businesses.

[12] https://cyber.gc.ca/en/
[13] https://www.cybersecurecatalyst.ca/
[14] https://cctx.ca/
[15] https://www.cira.ca/

And that I think is informational, it's about recognition of threats, and it's about people, process and, at the very last, it's about technology" (P2).

SMEs should be taught the value of cybersecurity from business, competitive advantage, and ethical perspectives, and be encouraged to get certified through venues such as Cyber Secure Canada. Even if companies do not reach the end of the process, it is still valuable to their cybersecurity maturation, says P10. More efforts could also be made to encourage SMEs to join information sharing groups such as the CCTX, which can be powerful tools for raising awareness around better security practices, learning from other members' successes and failures and staying up to date on emerging threats and solutions. In fact, being part of an information sharing group is already required in the U.S. as part of the CMMC[16]. Awareness campaigns in the form of conferences are important, too. The Government of British Columbia hosts two "Security Days" a year [47], providing a free conference to help raise awareness and encourage cybersecurity in the workplace, and have visited local businesses to encourage better cybersecurity practices.

P11 thinks it "would benefit SMES a lot" to have "consultants or advisers who would be available and know their needs," even if SMEs are unable to afford full-time in-house personnel. In-Sec-M, in collaboration with the NRC, conducts cybersecurity "interventions" at eligible SMEs, which includes 25 hours of consulting services to help improve a business' cybersecurity practices, comply with legislation and standards, to develop innovative cybersecurity solutions, and/or to integrate privacy and security by design [48]. Other services offered by the non-profit organization include helping Quebec businesses get certified and providing 90-minute information sessions to inform SMEs of cybersecurity risks and to diagnose potential threats to companies. Abroad, an innovative outreach effort is taking place at the University of Western Australia, which recently received funding to establish the Cybersecurity Aid Centre. The centre plans to provide a hotline for small businesses seeking cybersecurity assistance, with the help of students [49].

Making cybersecurity advice make sense

Participants thought that there is room for improvement in making cybersecurity advice more consumable by SMEs. There is a "lack of clarity" in current advice to businesses," says P4. Firstly, most cybersecurity advice is much too technical for average business owners to understand. P9 suggests targeting information to various actors based on their level of knowledge and familiarity with information technologies. "[We could] have dictionaries or documents that are made for decision makers and other documents which are more technical [for those who] already have [achieved] the level of essential cybersecurity" (P9). "These are not people who have a lot of time to read in depth about cyber security," P2 reminds us. A "critical challenge" is "how to get information that is easily understandable and usable in front of small business owners and operators in a way that they can implement changes quickly and effectively and cheaply" (P2). Cybersecurity education of SMEs should cater to their unique strengths relative to large businesses, which include agility, networking with other business owners, and suitability to zero trust models [29].

Experts called for a streamlining of Canadian cybersecurity information. Conflicting advice from various sources and inconsistent terminology can cause confusion. P11 proposes a simplified, "unified repository" of information about threats and cybersecurity controls for SMEs. Similarly, P10 suggests creating a catalog of existing solutions by Canadian businesses, organizing it by the 13 criteria of Cyber Secure Canada. Creating a shared language of cybersecurity across sectors is also important, says P4. For example, "[SMEs] don't seem to

[16] https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/level-3/sa-3-169/

quantify recovery in the same way that academics or researchers might like to think of it [...] I think, just in general, quantifying costs related to cyber security is a big definitional challenge." (P4). Critical infrastructure also lacks a "nice and tidy definition." This can create barriers to gathering data to assess the current state of SME cybersecurity, and to creating relevant policy. "It's a real challenge for government and law enforcement response. Without getting information about those types of attacks, it's really hard to build policy that can address it" (P5). Difficulties collecting accurate and consistent data on SMEs, especially small and micro-enterprises, have been discussed by researchers in the past, with blame pointing to disparate technical terms, poor sampling including under-representation of non-technical respondents, and self-reporting fallacies (e.g., respondents must be aware of breaches to report them) [29], By centralizing cybersecurity related resources and streamlining definitions for SMEs, we can "put everyone on a level playing field in terms of knowledge," says P4. Focus group participants expressed interest in a centralized place to find comprehensive cybersecurity advice. "I personally would love if there was a one-stop shop [...] to get all my answers [about securing my business]," says FGP6.

More straightforward advice needs to be given to Canadian SMEs when it comes to investing in technologies. P11 suggests helping SMEs "to be able to understand what the risks are that can be minimized by each technology. Not necessarily to make a comparison between the technologies, but to really see, in a real way, the technology 'does what, it minimizes what risk.'" This would help businesses make decisions applicable to their needs. Both SMEs and policy makers are looking for more straightforward outcomes, evidence-based advice, says P5, to help people visualize how technologies or controls will make an impact, and to know it has worked for others in the past. "[I]f there was more simple advice that you could give to small businesses, looking at this evidence trail of: if you were to implement these three simple fixes [...] the outcomes for those firms are much better in a cyber security context, than for those that don't" (P5).

In general, experts agreed they would like to see more Canadian-specific data on the state of cybersecurity in relation to SMEs. "I think the data on the state of play, a portrait, there are a lot of them right now [but] we make a lot of association with the American reality. Purely Canadian [...] data, I admit, there is not much" (P10). "It would be nice if we had a little more data. The difficulty is collecting this data. Because, who can answer these questions at the level of SMEs? I would tell you, it's really difficult at the SME level" (P12).

Experts reiterated the importance of knowledge as a first step to becoming cybersecure. "Step one, make sure people know what they need to do and how to do it. Step two is to provide access to skilled resources to allow it [...] What do you think step number three is? Just like Nike, 'Just do it,'" says P3. "If you know what your assets are, if you know that there's some baseline processes that you can go through to protect your assets [...] and you know what your appetite for risk is because you've sat down, you had the conversation, you've thought about it, then you don't need to be afraid. And that's the empowerment" (P1).

RECOMMENDATIONS

- **Increase** outreach efforts, getting existing cybersecurity advice in front of SMEs;
- **Provide** simpler, "usable" cybersecurity advice aimed at non-technical people;
- **Gather** more data on the state of cybersecurity in Canadian SMEs, especially very small businesses; gather more data about effectiveness of technologies on cybersecurity outcomes;
- **Provide** SMEs with people to consult at low cost;
- **Streamline** and centralize information about threats and solutions and standardize terminology.

Limitations

Due to how we recruited focus group participants (through an existing cybersecurity information sharing group), our SME sample was skewed towards those businesses who already possessed a fair amount of knowledge about cybersecurity, with most having at least one dedicated cybersecurity staff. While we believe many of our findings here can also be extrapolated to smaller businesses with lower cybersecurity maturity, our sample size may not accurately reflect all the challenges faced by very small or micro-businesses with extremely low levels of maturity. Future work would likely benefit from additional studies specifically targeting Canadian micro-businesses without dedicated cybersecurity staff.

Additionally, due to the extent of the current gap in basic technology adoption by SMEs, we found both experts and focus group participants continuously emphasized that a) SMEs are not putting available technologies into place, and b) other factors beyond technical difficulties are central contributors to the problem, e.g., governance. For this reason, data collection about specific up-and-coming technologies was relatively limited. A future study could explore specific technologies in depth, comparing the effectiveness and usability of solutions from various vendors. This could further aid businesses and policy makers in making decisions about what technologies to use, promote, and fund.

Conclusion

In this report, we discussed threats, challenges, and solutions surrounding SMEs' use of cybersecurity technologies. We found, overwhelmingly, that technologies already exist to protect SMEs from the threats that they face, but that SMEs are not using them or not deploying them to their full extent. This was for several reasons, including limited resources, a misunderstanding of the role of technologies in an organization's cybersecurity, that technologies are too complex to use for businesses without a dedicated cybersecurity or IT team, and that SMEs do not know which vendors or service providers to trust in terms of cybersecurity solutions. Our findings made it clear that current cybersecurity technologies are not being presented or designed with the unique constraints of SMEs in mind. SMEs must be better supported in their journeys to become cybersecure, on technical, policy, monetary, and educative fronts. Canada can only be competitive on the world stage once it has secured this vital component of our economy. We reiterate our primary recommendations:

Mandate cybersecurity certification in high-risk organizations. SMEs that are part of critical infrastructure supply chains or that deal with particularly sensitive data, e.g., healthcare, financial data or data of vulnerable populations, should be required to complete a certification such as Cyber Secure Canada. This should include non-profits and charities. Enforcement should be proactive, before breaches happen. All other organizations should be strongly encouraged to become certified. For lower-risk organizations, a simplified certification could be offered to increase likelihood of uptake.

Make cybersecurity technologies more affordable for SMEs. Many cybersecurity technologies are inaccessible in cost to the average SME. SMEs should be provided with financial support to implement critical cybersecurity measures relative to their risks. This may be done through inclusion in business loans, tax rebates, or discounts on insurance. Lower-cost alternatives to existing cybersecurity technologies should also be made available to SMEs.

Create technologies that are easier to use. Many cybersecurity technologies are too complex to be operated by businesses without a dedicated cybersecurity or IT team. Developers should explore simpler but equally effective alternatives which can be operated by fewer people and adhere to usable design principles to ensure ease of use. Special attention should be given to areas where SMEs struggle the most, such as detection and quantum-safe encryption at rest.

Increase outreach efforts to businesses. Most SMEs do not find appropriate advice on their own and need to be to met "where they are." SMEs should be proactively advised of where they can go for unbiased sources of cybersecurity advice. These efforts could include contacting businesses to offer informational sessions or on-site visits to help them assess threats and implement measures, inviting businesses to information sharing calls, offering informational pamphlets about cybersecurity to businesses applying for or renewing a license, providing SMEs with a centralized hub of cybersecurity advice, and other awareness campaigns. Advice should be presented in a manner comprehensible to non-technical people.

Standardize technologies and encourage secure-by-design practices. SMEs do not know who to trust when it comes to cybersecurity solutions and often assume technologies are safe and secure when they are not. Technologies which are marketed as cybersecurity solutions in Canada should be required to be certified through standards such as Common Criteria. Other technologies which can introduce risks, such as data storage solutions and IoT devices, should indicate they have followed secure-by-design principles. Post-secondary

institutions should include secure-by-design principles in their engineering curriculum.

Expand research on usability and outcomes of technologies. More research is needed about cybersecurity technologies used by SMEs, specifically in the areas of usability and outcomes on protection against attacks. These findings could be used to provide developers with advice for improving their technologies to meet SMEs' needs, and to provide businesses and policymakers with evidence-based advice on the effectiveness of various cybersecurity technologies. Efforts should also be made to consolidate existing information about cybersecurity threats and solutions from across Canada and to standardize related terminology and measurements.

To further guide in the implementation of these recommendations, in our final section of this report, we offer a map of Canadian start-ups and small-medium businesses which offer cybersecurity solutions and technologies.

A look at the future of cybersecurity technological innovation in Canada

Recent literature has identified certain subsegments of cybersecurity as "transformative technologies" [9] and rich in growth potential [11] . These include enterprise security operations management, cloud security, threat detection and intelligence leveraging machine learning, identity and access management ("one of the top product segments by size and growth prospects" with technologies such as two-factor, decentralized, biometric, and passwordless authentication [11]), and IoT security. Quantum computing is also posited as strategically important as "the most significant implications of the quantum arms race are already being felt by the global cybersecurity community" [9].

While businesses are expected to see the emergence of new types of threats in the next 5-10 years [9], it is important to remember that Canadian SMEs continue to fall behind in even the most basic measures. Our interviews showed that upcoming cyber trends are largely not on the radar of Canadian SMEs, and even if they are, SMEs are not able to afford relevant technologies. "The brand-new stuff, machine learning and neural networks and stuff, it all starts at 'world class'; it's the banks that can afford it. But over time it slips down [to SMEs]" (P3).

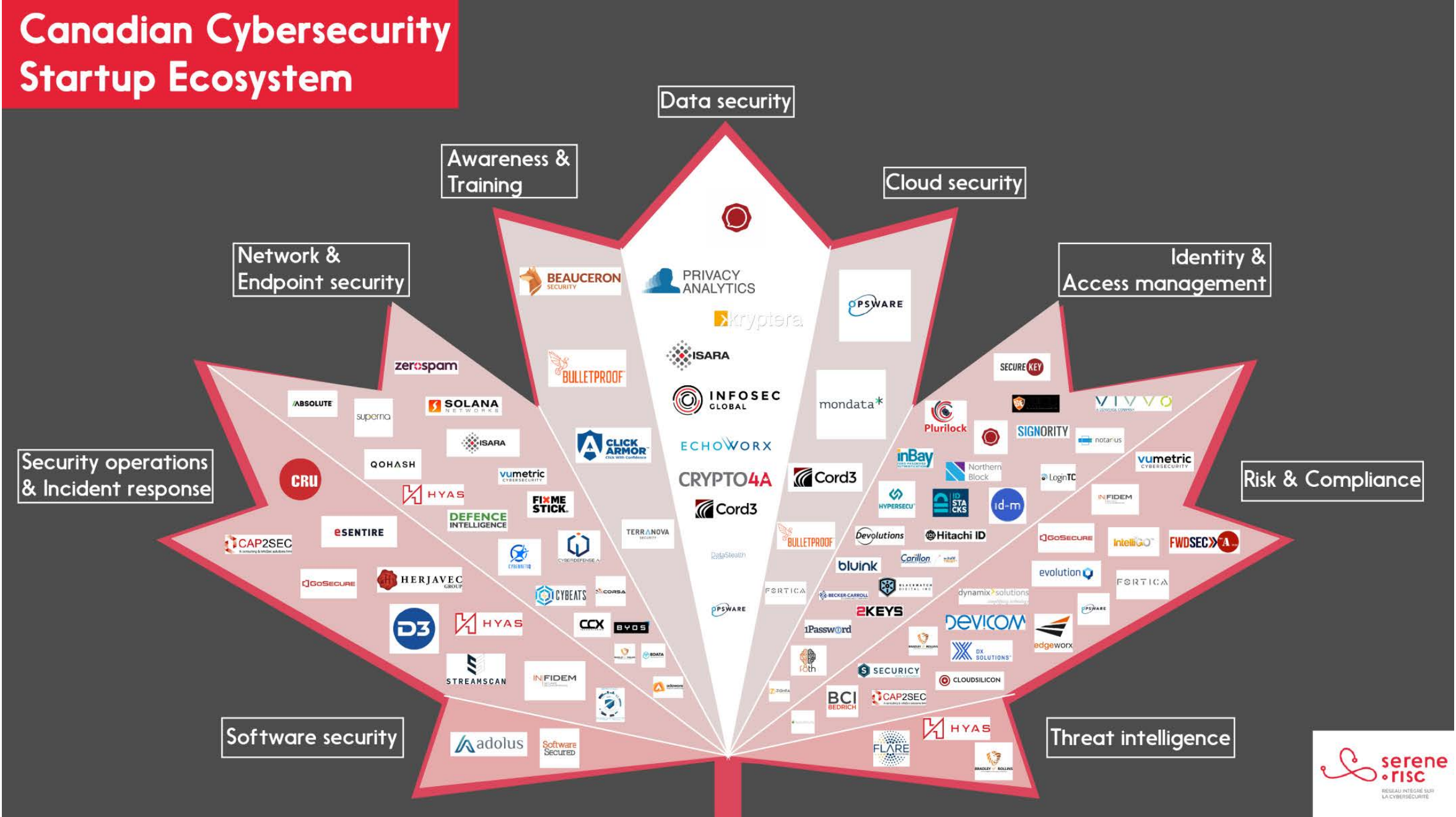
Therefore, we recommend focusing innovation efforts on how existing technologies can be made more accessible to SMEs, and how emerging technologies can be leveraged to address SMEs' unique needs. For example, artificial intelligence can be useful in businesses with a lack of human resources, and is already used in modern endpoint detection solutions to detect emerging threats. Creating a SME-friendly solution could help address SMEs' gap in detection. Additionally, putting research and development into creating more usable ways of encrypting data at rest (using quantum-safe cryptography) can help ensure Canadians' data will be safe against attacks now and in the future.

To help identify gaps and opportunities in the Canadian innovative space, on the following page we present a map of cybersecurity technology SMEs from across Canada. We invite stakeholders to use our map as a reference while considering our recommendations and identifying which areas may require additional funding, support, or research. The map is also available for download on the SERENE-RISC website[17].

Current funding and support initiatives for innovative cybersecurity technologies include programs such as PROMPT's QCIP in Quebec [50], FedEv in Ontario [51], and CyberNB's CyberHatch in New Brunswick [52]. Canada-wide funding options includes programs through the Government of Canada's ISED (who is providing $80 million to fund the pan-Canadian Cyber Security Innovation Network [53]) and NRC IRAP [54], and the Ryerson-Rogers Cybersecure Catalyst Cyber Accelerator [55]. SERENE-RISC is also providing an update of the CLOSER database (see Appendix C), which includes over 400 cybersecurity researchers across Canadian universities. This should be helpful in identifying appropriate individuals to conduct research or partner with industry or government in creating innovative, SME-friendly technologies.

[17] https://www.serene-risc.ca/en/canadian-cybersecurity-startup-ecosystem

Canadian Cybersecurity Startup Ecosystem



References

[1] Innovation, Science and Economic Development Canada, "Key Small Business Statistics — 2020," 10 12 2020. [Online]. Available: https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03126.html. [Accessed 2022].

[2] Statistics Canada, "Table 22-10-0001-01 Cyber security measures enterprises have in place by industry and size of enterprise," 2019. [Online]. Available: https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210000101.

[3] M. Heidt, J. P. Gerlach and P. Buxmann, "Investigating the security divide between sme and large companies: How sme characteristics influence organizational it security investments," *Information Systems Frontiers,* p. 21(6):1285– 1305, 2019.

[4] M. Watad, S. Washah, Perez and Cesar, "It security threats and challenges for small firms: Managers' perceptions," *International journal of the academic business world,* p. 12(1):23–30, 2018.

[5] Council of Better Business Bureaus, "State of Cybersecurity Among Small Businesses in North America," 2017.

[6] Canadian Federation of Independent Business (CFIB), "Cyberfraud in Small Business: How small businesses are coping with cyberattacks during the pandemic.," 2021.

[7] Canadian Internet Registration Authority (CIRA), "2020 CIRA Cybersecurity Report," 2020.

[8] Insurance Bureau of Canada, "Many small businesses vulnerable to cyber attacks," *Insurance Bureau of Canada Media Releases,* 5 October 2021.

[9] S. Creese, J. Saunders, L. Axon and W. Dixon, "Future Series: Cybersecurity, emerging technology and systemic risk," World Economic Forum, 2020.

[10] Canadian Chamber of Commerce, "Cyber. Right. Now. Leading the Global Cybersecurity Future," [Online]. Available: https://chamber.ca/campaign/cyber-right-now/. [Accessed 2022 February].

[11] OMERS Ventures, "Cybersecurity: OV Investment Thesis, Business Models, & Market Segments," Omers Ventures, 9 April 2019. [Online]. Available: https://medium.com/omers-ventures/cybersecurity-ov-investment-thesis-business-models-market-segments-f4957db2357d.

[12] Public Safety Canada, "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age," Government of Canada, 28 05 2019. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

[13] Canadian Chamber of Commerce, "Assisting Small Business with Minimizing the Risk," 2020.

[14] Statistics Canada, "About one-fifth of Canadian businesses were impacted by cyber security incidents in 2019".

[15] Canadian Centre for Cyber Security, "National cyber threat assessment 2020".

[16] Canadian Centre for Cyber Security, "Cyber threat bulletin: The ransomware threat in 2021," 2021.

[17] Sophos, "The State of Ransomware 2021," 2021.

[18] Canadian Centre for Cyber Security, "Baseline Cyber Security Controls for Small and Medium Organizations," Government of Canada, 2021.

[19] Government of British Columbia, "Defensible Security," [Online]. Available: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security. [Accessed February 2022].

[20] E. Rohn, G. Sabari and G. Leshem, "Explaining small business infosec posture using social theories," *Information & Computer Security,* 2016.

[21] E. Osborn and A. Simpson, "Risk and the small-scale cyber security decision making dialogue—a UK case study," *The Computer Journal,* vol. 61, no. 4, pp. 472-495, 2018.

[22] C. Kent, M. Tanner and S. Kabanda, "How South African SMEs address cyber security: The case of web server logs and intrusion detection," in *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, 2016.

[23] Ponemon Institute, "2017 state of cybersecurity in small & medium-sized businesses".

[24] S. Sheng, L. Broderick, C. A. Koranda and J. J. & Hyland, "Sheng,Steve, et al. "Why johnny still can't encrypt: evaluating the usability of email encryption software," in *Symposium On Usable Privacy and Security*, 2006.

[25] C. T. Berry and R. L. Berry, "An initial assessment of small business risk management approaches for cyber security threats," *International Journal of Business Continuity and Risk Management,* p. 8(1):1–10, 2018.

[26] C. Paulsen, "Cybersecuring small businesses," *Computer,* p. 49(8):92–97, 2016.

[27] A. Mohammed, B. Idris, G. Saridakis and V. Benson, "Information and communication technologies: a curse or blessing for SMEs?," in *Emerging Cyber threats and cognitive vulnerabilities*, Academic Press, 2020, pp. 163-174.

[28] Cassel & Graydon LLP Blake, "Canadian cybersecurity trends study 2020," 2020.

[29] T. Tam, A. Rao and J. & Hall, "The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses," *Computers & Security,* vol. 109, p. 102385, 2021.

[30] S. Furnell, A. Jusoh, D. Katsabas and P. Dowland, "Considering the usability of end-user security software," in *IFIP International Information Security Conference*, Boston, MA, 2006.

[31] Human-Centric Cybersecurity Partnership (HC2P), "About," 2022. [Online]. Available: https://www.hc2p.ca/. [Accessed February 2022].

[32] Nielsen Norman Group, "10 Usability Heuristics for User Interface Design," [Online]. Available: https://www.nngroup.com/articles/ten-usability-heuristics/. [Accessed 2022].

[33] Government of Canada, "Electrical product safety," 16 11 2020. [Online]. Available: https://www.canada.ca/en/health-canada/services/home-safety/electrical-products.html. [Accessed February 2022].

[34] Canadian Centre for Cyber Security, "Common criteria," [Online]. Available: https://cyber.gc.ca/en/common-criteria. [Accessed February 2022].

[35] CyberNB, "Transparency Centre," [Online]. Available: https://cybernb.ca/TransparencyCentre.htm. [Accessed February 2022].

[36] United States Congress, "S.1490 - Personal Data Privacy and Security Act of 2009," 22 07 2009. [Online]. Available: https://www.congress.gov/bill/111th-congress/senate-bill/1490. [Accessed February 2022].

[37] Officer of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards," 13 August 2021. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/. [Accessed February 2022].

[38] Office of the Privacy Commissioner of Canada, "PIPEDA in brief," 31 May 2019. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. [Accessed February 2022].

[39] C. Berzins, "Three Years Under the PIPEDA: A Disappointing Beginning," *Canadian Journal of Law and Technology,* vol. 3, no. 3, pp. 113-126, 2004.

[40] L. Zhang Kennedy and S. Chiasson, "Whether it's moral is a whole other story": Consumer perspectives on privacy regulations and corporate data practices," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 2021.

[41] Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principle 7 – Safeguards," 13 August 2021. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/. [Accessed February 2022].

[42] Office of the Privacy Commissioner of Canada, "How PIPEDA applies to charitable and non-profit organizations," 25 June 2019. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_19/. [Accessed February 2022].

[43] National Cyber Security Centre, "About Cyber Essentials," [Online]. Available: https://www.ncsc.gov.uk/cyberessentials/overview. [Accessed February 2022].

[44] Office of the Under Secretary of Defense Acquisition and Sustainment, "About CMMC," [Online]. Available: https://www.acq.osd.mil/cmmc/about-us.html. [Accessed February 2022].

[45] Innovation, Science and Economic Development Canada, "CyberSecure Canada," [Online]. Available: https://ic.gc.ca/eic/site/137.nsf/eng/h_00000.html. [Accessed February 2022].

[46] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi and P. Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS," *NPJ digital medicine,* vol. 2, no. 1, pp. 1-7, 2019.

[47] Government of British Columbia, "Security Day," [Online]. Available: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/security-day. [Accessed 2022 February].

[48] In-Sec-M, "SME Cyber Security Support Program," [Online]. Available: https://insecm.ca/our-services/security/. [Accessed 2022 February].

[49] D. Thompson, "Federal Government delivers funding to establish Cybersecurity Aid Centre in Parramatta," *Western Sydney University News Centre,* 10 May 2021.

[50] prompt, "PROMPT: Who we are," [Online]. Available: https://promptinnov.com/en/prompt/who-we-are-missions-objectives-history-partners/.

[51] Federal Economic Development Agency for Southern Ontario, "Federal Economic Development Agency for Southern Ontario," [Online]. Available: https://www.feddevontario.gc.ca/eic/site/723.nsf/eng/home. [Accessed 2022 February].

[52] CyberNB, "CyberHatch Incubator & Accelerator to Grow Cybersecurity Talent in New Brunswick," 3 December 2020. [Online]. Available: https://cybernb.ca/blog/cyberhatch-incubator-accelerator-to-grow-cybersecurity-talent-in-new-brunswick.htm. [Accessed February 2022].

[53] Innovation, Science and Economic Development Canada, "Government of Canada announces next phase to strengthen Cyber Security Innovation Network," 17 February 2022. [Online]. Available: https://www.canada.ca/en/innovation-science-economic-development/news/2022/02/government-of-canada-announces-next-phase-to-strengthen-cyber-security-innovation-network.html.

[54] National Research Council Canada, "Support for technology innovation," 19 01 2022. [Online]. Available: https://nrc.canada.ca/en/support-technology-innovation. [Accessed February 2022].

[55] Cybersecure Catalyst, "Catalyst Cyber Accelerator," [Online]. Available: https://www.cybersecurecatalyst.ca/accelerator-overview. [Accessed 2022 February].

Appendix A: Interview Guide (Experts)

Threats

- In your opinion, what are the upcoming cyber-threats that Canadian companies/SMEs face?
    - Can you tell us more about your assessment of the probability and severity of these threats?
- Do you have experience with the following cyber-threats, and what is your company doing to protect against them?:
    - Ransomware
    - Data theft
    - Online fraud
    - Targeting of critical infrastructure (if applicable)
    - Supply chain attacks/exploiting business relationships
- Do you have any lessons from a technological standpoint learnt from identifying, protecting, detecting, responding to, and recovering from past cyberattacks?
    - How confident do you feel you could protect your company from a similar attack in the future?
- What has been the most important thing you have learnt about cybersecurity relating to SMEs in the past year? Words of wisdom for SMEs?
- What aspects of cybersecurity (threats, technologies) do we need more evidence about to help you make decisions about what technologies to purchase and to use?

Challenges

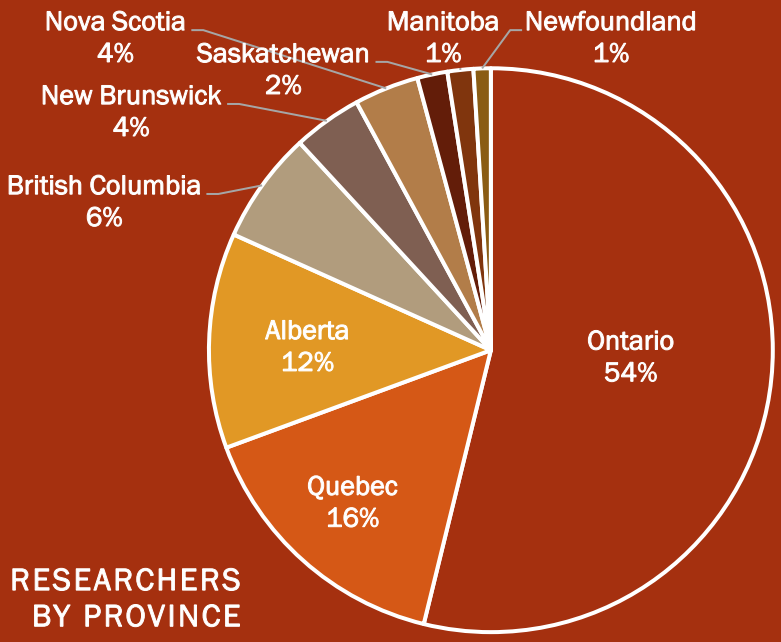
- In your opinion, what challenges in understanding the cyberthreat landscape do SMEs face?
    - assessing threats & vulnerabilities
    - estimating cybercrime cost
    - industry-specific challenges
    - Accessing cybersecurity expertise
- In your opinion, what are the challenges in implementing technologies SMEs face?
    - In your opinion, what could be improved to help overcome these challenges?
- Can you give us some examples of technologies that help SMEs and how they work?
- In your opinion, what other challenges, on top of the technological one, do SMEs face? (legal, HR, Organizational and infrastructure to implement those technologies, etc.)
- Has the COVID-19 pandemic/remote work affected the cybersecurity challenges you face? How so?
- There's been a lot of talk lately about emerging technologies such as AI, Quantum, and IoT. How does your company foresee Canadian businesses using these technologies in the next 5-10 years?
- **Wrap-up question: Is there any aspect of SMEs, cybersecurity technologies, etc., we haven't asked you about that you would like to comment on?**

Appendix B: SME Focus group questions

- Can you tell me about a cybersecurity measure that you found:
    - Relatively easy to implement and effective in terms of outcomes? Why?
    - Relatively difficult to implement? Why?
- Are there any cybersecurity technologies you'd like to use but haven't yet done so?
    - Why? What were the barriers to adoption?
- What do you want to know before investing in a cybersecurity technology?
- Do you feel you have access to the guidance necessary to make informed decisions regarding technological investments in cybersecurity?
    - How do you decide who to trust to provide you with cybersecurity advice?
    - How confident do you feel in your ability to discern useful cybersecurity technology or services from well-marketed but less useful technology/services?

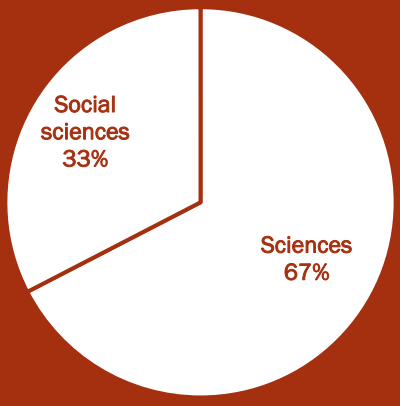
Appendix C: Canada's academic cybersecurity researcher landscape

We present select numbers from CLOSER, a database of cybersecurity and privacy professors working at Canadian universities, created by SERENE-RISC. We have updated it for this report, adding 156 new professors since 2018. This brings the total to **405 academic researchers** including **28 Canada Research Chairs**. The full database can be obtained from SERENE-RISC by emailing benoit.dupont@umontreal.ca.



RESEARCHERS BY PROVINCE

TOP KEYWORDS



RESEARCHERS BY DISCIPLINE

TOP 12 UNIVERSITIVES BY # OF RESEARCHERS