University of Guelph, Gordon S. Lang School of Business and Economics, Department of Management

Securing Privacy: Examining the tension between push and pull of cybersecurity adoption

Cite as: "Hoong, Y & Rezania, D. (2023). Securing Privacy: Examining the tension between the push and pull of cybersecurity adoption."

Yang Hoong and Davar Rezania
3-14-2023

This research study was made possible by the financial contributions and support from the Office of the Privacy Commissioner of Canada's contributions program. The opinions expressed in the summary and report(s) are those of the authors and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada. We are extremely grateful to all participants who graciously extended their time and resources to be a part of this study. We look forward to comments from various stakeholders from the first iteration of this paper that is to be perfected, and where applicable, we will address the comments in a final edition of the paper.

Table of Contents

List of Tables and Figures

In this study, we explore the tension between external (the "push") and internal (the "pull") forces impacting cybersecurity for privacy adoption by SMEs and discover the relationship between the two. We interviewed SME managers, policy influencers, and organizations supporting SMEs to examine how they view cybersecurity for privacy and how they practice it. We identify some of the factors that dictate the pace and direction of cybersecurity adoption in SMEs.

Cybersecurity: What we already knew

The 4th Industrial Revolution (Industry 4.0) has ushered in a new age. In this (current) period that we live in, information systems (IS) and information technology (IT) is no longer a nice to have for a vast majority of businesses, but rather a must have – otherwise they face being left behind competitively. Businesses are able to utilize the technology (by making their information and services available round-the-clock online) in order to bring down operating costs, and to increase their efficiency [1]. However, this would also increase a company's vulnerability level as it would mean that they are constantly at risk of an attack, due to their round-the-clock presence. Cyberattacks and cyber breaches have been on the rise in businesses across the globe, making cybersecurity and the protection of organizational data one of the most pressing issues for businesses today [2]. Indeed, researchers have identified one of the most significant issues facing organizations today: namely, how they defend themselves against these attacks and breaches [2].

Organizations are increasingly aware of the importance of cybersecurity. This is because the damages from cyber breaches can be quite severe. According to IBM and the Ponemon Institute's 2020 Cost of a Data Breach report, it was determined that the average total cost of cybersecurity breaches in the world in 2020 was $3,860,000 [3]. Indeed, successful cyberattacks can damage an organization not just financially, but reputationally as well – this could negatively affect the organization's ability to attract and retain talent [4]. This leads to the organization's overall competitive edge being negatively impacted [5]. As a result, organizations have begun to adopt and invest in technical cybersecurity IT and IS measures such as firewalls, encryption and biometrics in order to protect against data breaches [6].

Investing in, and adopting just technical cybersecurity measures as a form of defence against cyber breaches is not enough [7]. Researchers have identified a need for organizations to adopt cybersecurity measures and policies that address the human factor, as humans have been generally found to be the weakest link in cybersecurity [8]. Employees need to be trained in cybersecurity measures, so that they do not unknowingly (or knowingly) cause a cyber breach [9]. For instance, a computer analyst ignored alerts that signalled a cyber breach in Target's network; a network security officer at JP Morgan did doubly authenticate an entry into a JP Morgan server; and a Sony employee chose to move sensitive data into a system that was not authorized [10]. These choices all served to make the companies more vulnerable to a cyber breach.

The introduction of these new cyber threats stresses the importance of cybersecurity governance. Within the literature, there is a scarcity of definitions regarding cybersecurity governance, largely due to its fluid nature and is still a relatively immature topic. Von Solms and von Solms [11] have defined cybersecurity governance as "as part of information security governance, and is the process of directing and controlling the protection of a company's digital information assets from the risks that are related to using the internet". However, we argue that this definition is too narrow – under this

definition of cybersecurity, a human breach would not be considered a cybersecurity breach. Indeed, as von Solms and von Solms [11] elaborate: if an employee were to copy sensitive company information onto a USB drive and sell the USB drive, it would not be a cybersecurity breach. Given that humans have been identified as one of the main causes of cybersecurity breaches, we argue that cybersecurity governance should cover the human dimension as well.

It is important to note at this juncture the difference between information security governance (ISG), and cybersecurity governance. Information security has been defined as "the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user" [12]. This information largely manifests itself in the form of data. Cybersecurity, on the other hand, has been described by the United Nations as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets" [13]. Cybersecurity can thus be seen as a comprehensive concept that encompasses ISG.

Cybersecurity governance has been defined as "the approaches used by multiple stakeholders to identify, frame and coordinate proactive and reactive responses to potential threats to the confidentiality, integrity, or availability of the computers, networks, and information that together constitute cyberspace – the conceptual space that affords digitised and networked human and organisational activities" [14]. This definition of cybersecurity governance involves not just the digital internet governance proposed by von Solms and von Solms [11], but also the activities (like the human factor) taking place in/facilitated by cyberspace.

In the Canadian context, over 500 million Canadian dollars was allocated into cybersecurity technology research and development (R&D), along with multiple initiatives including increased collaboration between the public and private sector, increased partnerships with international partners [15]. Despite the large investments made towards cybersecurity R&D, there is recognition that any significant improvement is also dependant on the human element of cybersecurity [16].

Canadian SMEs: a key cog in the Canadian economy

Existing scholarly research has largely focused on the impacts of cybersecurity breaches on large corporations and multi-national corporations (MNCs). For instance, prior cybersecurity reviews largely focus on the economic consequences of cybersecurity incidents on MNCs (e.g. market reaction and firm performance), and ranges from hypothetical scenarios to using actual breach data [1], [17].

It remains unclear who, or what affects the rate and direction of cybersecurity adoption in SMEs in general. Indeed, all we know for certain, from the existing research that has been conducted, is that SMEs have been found to be particularly reluctant to adopt cybersecurity measures [18]. Researchers surmise that this could be due to a myriad of reasons, which include, but are not limited to: cost, low levels of expertise, the feeling that a cyber breach is inevitable, and the assumption that their data is not of significance to anyone [19]. What is clear, however, is that there is uncertainty, particularly in SMEs, over what or who contributes to their decision to adopt cybersecurity measures.

Existing trends and evidence suggest that SMEs in Canada are not exempt from cyber breaches, and from the reluctance to adopt cybersecurity measures. In a study done by the Insurance Bureau of Canada (IBC) in 2019, they found that roughly one-in-five SMEs (18%) polled have been impacted by a

data breach in the past two years, with this percentage jumping to 42% for organizations with 100 to 499 employees [20]. Nearly half (46%) of the small-to-medium sized business owners surveyed that suffered a cyber attack, and are familiar with its associated costs, stated that the breach cost them more than $100,000 [20]. Although this information suggests that SMEs are just as vulnerable to cybersecurity threats as MNCs, the poll shows that 44% of small businesses do not have any defences against possible cyber attacks, and 60% have no insurance to help them recover if an attack occurs [20].

Small and medium-sized enterprises (SMEs) play a key role in the Canadian economy. Between 2013 and 2017, for example, SMEs accounted for 85.3 percent of net job creation in the private sector, while in 2017 SMEs employed 89.6 percent of the private sector workforce [21]. Therefore, determining the factors and relationships that contribute to a Canadian SMEs' decision to adopt cybersecurity measures is of significant importance in today's day and age.

Examining adoption from a push. Vs pull perspective

In today's digital age, businesses have a responsibility to ensure that the hardware and software that they use to process, store and analyse identifiable information has an adequate level of security to protect the users who have access to those systems. Indeed, within the Canadian context, the Personal Information Protection and Electronic Documents Act (PIPEDA) serves as an external push factor for businesses, with guiding principles such as the accountability principle holding organizations responsible for information under their control. Businesses must also protect the confidentiality and privacy of individuals data held within those systems, initiating the appropriate safeguards (Principle 7 of PIPEDA). In other words, one of the main considerations for businesses when adopting cybersecurity measures is the ethical dimension. For businesses to have any chance of achieving this, they must be aware of the threat landscape. In knowing the main threats, businesses can allocate sufficient resources to protect themselves, it is an efficient use of resources, and it has the potential to reduce the likelihood of a successful attack. Every organisation that stores personal and sensitive data has a responsibility to ensure that ethics are interwoven throughout the company, from the boardroom to the interns and grads. Ethical decision-making promotes transparency and honesty, and the pursuit of such laudable values leads to both greater trust in the marketplace and greater profits [22].

One of the concerns that arises with cybersecurity adoption is the problem of overemphasizing cybersecurity. Overemphasizing cybersecurity measures designed to negate the privacy issues from cyber breaches may ironically violate ethical values like privacy that it was designed to protect [23]. Cookies is a good example. Cookies are small data files that are stored on the hard of disk of the user whenever the user visits the site. Within a cybersecurity context, cookies function as a unique identifier used to verify and authenticate a person's identity on a website, which adds a layer of security when accessing sensitive data. However, when overemphasized, these cookies can track the online activities of what the user did while on that site. To use eBay as an example, eBay would be able to track if a user preferred Nike over Adidas, for example. It would then be able to tailor specific advertisements for the user or suggest more Nike products to them as part of their marking policy. It has been argued that this overemphasis violates consumer privacy [24].

Extant literature posits that whilst it would be harmful to overemphasize cybersecurity, underemphasizing cybersecurity would be disastrous – it could undermine users' trust and confidence in ICT and IT systems that are fundamental to business operations in Industry 4.0 [23]. If we are to avoid illegal access to sensitive information by outside hacks and breaches, organizations would need some

type of cybersecurity measure in place [25]. These measures would naturally involve some monitoring of cyber traffic and information. The alternative would be the sensitive information being freely accessible to anyone in the cyber space. In other words, applying cybersecurity measures is essential in the protection of digital assets of all kinds and belonging [26].

As previously alluded to, one of the internal drivers of cybersecurity is the ethical dimension – specifically one of privacy – and businesses have a responsibility to ensure that they have the capability to protect sensitive data from privacy violations via cyber breaches. However, existing literature also warns us that businesses have a challenge of balancing over and underemphasizing cybersecurity measures. Underemphasize cybersecurity measures, and sensitive data is freely available to anyone with an internet connection. Overemphasize cybersecurity measures, and you risk violating consumer privacy. By understanding how organizations make sense of these privacy tensions, it will allow researchers, policy makers, and cybersecurity providers to better understand how Canadian small and medium enterprises (SMEs) view and practice privacy considerations when adopting cybersecurity measures, from which the appropriate policies, and cybersecurity measures can be generated.

Refocusing on SMEs

At the end of the day, it seems that it is not always clear what contributes to an SMEs decision to adopt cybersecurity measures. If so, what steps can we take to uncover the factors behind adoption, and once we know the factors, how can we help SMEs (specifically Canadian SMEs) increase cybersecurity adoption and allow for more protection over their data? Several other organizations, from different countries, have addressed this in different ways - with this particular puzzle in mind.

- In the United States, the Federal Trade Commissioner's Safeguards rule requires every business, regardless of size, to develop, implement, and maintain a comprehensive cybersecurity program to protect consumer information and data [27].
- Also in the United States, the National Institute of Standards and Technology (NIST) offers a wide range of guides for small businesses [28].
- In Canada, *CyberSecure Canada,* which specifically targets Canadian SMEs, is a certification program designed to help guide and secure Canadian SMEs from cyber threats [29].
- Another initiative in Canada, Simply Secure, is part of Rogers CyberSecure Catalyst Program. This initiative provides training, advice and accessible cybersecurity resources to empower Canadian SMEs to tackle cybersecurity challenges [30].
- In Europe, the European Union Agency for Cybersecurity (ENISA) regularly organizes workshops and guides for European SMEs to assist SMEs in integrating cybersecurity into their digital environments [31].

These examples illustrate how in many different jurisdictions and contexts, both the government and civil society organizations prioritize cybersecurity measures to help protect and safeguard data – especially for SMEs.

Methodology

From August 2022 to March 2023, we conducted 37 interviews: 24 SMEs, 2 policy influencers, and 11 organizations supporting SMEs (5 cyber providers, 3 associations, and 3 educators and experts). Participants were recruited through purposive sampling with the help of community organizations, such as In-Sec-M. This research project received ethics approval from the University of Guelph's Office of Research Ethics: Project #21-10-014.

Humans are generally found to the be the weakest link in cybersecurity [8]. Consequently, the literature has identified a need for more research on the human and socio-political aspect of cybersecurity [16]. Discourse analysis (DA) is a method of studying the interactions (e.g. values, assumptions, rules and norms) of social groups via the analysis of language [32]. Additionally, language is embedded in the sensemaking processes of any organization; it is one of the components that facilitates the diffusion and adoption of technology [33]. Given that we are interested in the sensemaking process of cybersecurity measures amongst humans and technology in Canadian SMEs, aspects of DA are well positioned to help us analyze this. This is especially so since discourses around cybersecurity have evolved in recent years, from purely technical and computer science subjects to issues of values, meaning and ethics [34]. Therefore, DA would allow us to identify how organizations make sense of these shifts, and how (or if) that translates into their decision-making process.

Interviews were used as the primary method of data collection. The interviews consisted of semi-structured open-ended questions to investigate the interviewee's views on cybersecurity and privacy, and the discourses surrounding it. The interviews, which ran for approximately 45mins to 60mins each, gave participants an opportunity to share their thoughts and experience on the current cyber and privacy landscape for SMEs in Canada. Each session began with an introductory explanation from the interviewer that provided participants on the purpose of the research study, an overview of the research study, and their rights to privacy and consent. Participants were also provided a consent form with the same information said in the introductory explanation.

The introductory explanation was then followed by a brief discussion of the interviewee's knowledge of, experience and views regarding cybersecurity and privacy in Canadian SMEs. We asked interviewees:

- How do Canadian SME decision-makers view cybersecurity and privacy, and who are the stakeholders involved?
- What are the issues that Canadian SME decision-makers face when implementing cybersecurity for privacy measures?
- What are the challenges that Canadian SME decision-makers face for securing their operations?

With participant permission, the interviews were audio recorded and transcribed for analysis. All identifying information was removed in this report to safeguard participant anonymity. Data was then coded following Fleming et al. (2018) DA method [35], with elements of Corbin & Strauss (1990) [36]. The data was coded and verified by multiple researchers, ensuring validity and reliability of the data.

The interviews revealed the following:

- Observations and views from SMEs, the industry, and organizations supporting SMEs about current cyber and privacy controversies;
- Suggestions from SMEs and organizations supporting SMEs on how to improve current measures, and address current cyber and privacy controversies.

Controversies and Issues surrounding Cybersecurity and Privacy in Canadian SMEs

CONTROVERSY #1: Cybersecurity for Privacy. Despite calls to think of cybersecurity and privacy as "interconnected" [37], [38], our study finds that gaps remain in how stakeholders view cybersecurity and privacy. We find that cybersecurity is still largely viewed through a technical lens by a significant portion of the cybersecurity community, with experts and SMEs expressing that cybersecurity is more than just technical solutions. Results from the study suggests that cybersecurity providers and other 3rd parties typically take a cyber-oriented approach towards cybersecurity and privacy, which means that they tend to see and prioritize other cyber measures such as securing critical infrastructure, and protecting systems and networks. SMEs, on the other hand, tend to take a privacy-oriented approach towards cybersecurity and privacy, meaning that they tend to prioritize cybersecurity for privacy requirements such as measures to safeguard personally identifiable information.

Quotes from SME: "We are dealing with a lot of information about our clients, like, you know, very unique identifiers to them, like address and contact information. we want to make sure that people don't have easy access to all that valuable information. Like, you know, we have a list of people's licensed addresses, telephone numbers, email addresses. It's pretty sensitive information. It's very important for us to keep that information secure."

Quote from cyber-oriented professional: "cyber security and privacy, in my mind are two different constructs. I would say that cybersecurity is of higher importance than privacy at this point. And privacy, privacy is a subset of data. The main intent of cybersecurity is to protect, protect the confidentiality, integrity and availability of data. Whereas privacy is more about protecting the user data or personal data."

Quote from privacy-oriented professional: "Personally, I've had people say to me, you're not a cyber professional. You're a privacy professional. I do both. But at the same time, I'm like, as a privacy professional, that should be enough for me to say I'm a cyber professional like I shouldn't have to also justify I've definitely had people roll their eyes and like I have nothing against other professionals at all, but they'll be like, oh, you're just some lawyer that does privacy. And I'm like, actually, I am coming from the technical side of this. But I shouldn't have to justify it, it's frustrating. Like I shouldn't have to justify anything... I should just show up and say hi, I'm here to talk to you about privacy and cybersecurity and people should just say sure, I shouldn't have to like defend it."

Quote from cybersecurity expert: "The biggest challenge I have around some of the tools and the resources is how they are situated. Right? They have not yet penetrated into the minds of business leaders. They're still very much at the CIO CISO, CTO, and cyber security and maybe some IT folks, but that normally those are the people that understand or think about cybersecurity, and guess what, that's not the right place, or that's a place but that's not the right place. Those people are about technical solutions. They're not about cybersecurity. Right, because cybersecurity is about people processes and

technology. And the people and processes are often not within the IT space. Right? You need good solid minute management and governance; you need good solid people and user behaviors you need. You need a lot of people doing a lot of things and handling information in a consistent way. So, you need a lot of stuff within an organization that has nothing to do with the technology."

Quote from SME: "First of all, cybersecurity is dominated by the technical community, right? It is not, it is not a business thing. And you've run through a business program, how much did you hear about cybersecurity in your business program? Right? So, so if cybersecurity is dominated by the technical, and I'm not a technical guy, my education is elsewhere, so I'm automatically not a cybersecurity guy. It bothers me because the technical people have no idea how to link it back to aspects outside of the technical. What is telling a business how much bytes you can save going to do for them?"

As technology is becoming increasing ubiquitous in more and more businesses today, more and more businesses embed technology into their businesses processes, and are becoming increasingly dependent on it [39]. However, discourses from this study reveal that SMEs do not fully think about risks associated with cyber breaches and technology as a business-critical risk.

Quote from SME: "I don't think cyber risks and technology issues applies to our organization. We use technology in our business, like most other business do, but the way we operate is very old school. We don't do a lot of like online things, and we don't ever to advertise ourselves on the internet. So things are very close knit and word of mouth."

CONTROVERSY #2: Education levels. There are many pushes by various organizations to increase overall education levels of cybersecurity importance and the impacts of cyber breaches [40], [41]. Our study reveals a controversy with regards to education levels of cybersecurity and privacy in Canadian SMEs. If education levels are too low, it is problematic because it leaves individuals and organizations vulnerable to cyber and privacy threats. Without an understanding of basic cybersecurity practices, SMEs are vulnerable to the multitude of cyber threats that exist. On the other hand, if education and noise levels are too high on cybersecurity and privacy threats, it can also be problematic. Participants in this study indicate that it can lead to an excessive focus on security resulting in measures that might not be effective or necessary, such as implementing overly complex or burdensome security measures, from multiple providers, that could end up conflicting with one another. It could also lead to a culture of fear and paralysis where individuals and SMEs are hesitant to embrace cybersecurity because of the fear of security risks.

Quote from SME with low levels of education on cybersecurity for privacy: "I'm not gonna lie, I have no idea. I don't think I've in terms of business wise, I don't think it's ever crossed my mind. Not because like, I don't care. More so because like, my me, and my colleagues aren't really like, familiar with benefits of cybersecurity through like through our business. So I just think they just, they just choose not to like not to care."

"For me, it (media) seems to hype a lot of stuff, but at some point in time, you have to wonder about how much of it (cybersecurity breaches) is hype?"

Quote from SME with too high levels of education on cybersecurity for privacy: "I mean, in some cases, you have people who, like the owner is one of them, he inadvertently put two different protection programs on his computer at home, thinking he was giving himself double the protection and in actual

fact, they kind of blocked each other out. So he got hacked, he got broken into."

"First of all, I think it's, it's really, actually quite terrifying. The amount of people out there that will try and hack into I mean, you hear about it all the time, they hack into far more private information, like in hospitals and schools and stuff like that, that is actually very worrisome, and then they hold information for ransom. If they can hack into bigger and more resourceful organizations like that, what chance do I have?"

CONTROVERSY #3: Cybersecurity for privacy viewed as unnecessary costs. The study finds that SMEs often view cybersecurity as a cost, that does not provide any immediate visible return on investment to their business. This has led to SMEs viewing cybersecurity as an unnecessary burden, that takes time and resources away from their core business activities, and negatively impacts their competitive standing. This perceived lack of benefit from adopting cybersecurity for privacy makes it difficult for them to justify the costs of cybersecurity measures.

Quotes from SMEs: "There's a lot of other kinds of systems and processes that I feel are more vital to put in place first before cybersecurity. You know, I'm going to, I'm not going to be able to compete as it is with the, you know, the Home Depot's of the world. And now if I've got to go spend money on cybersecurity, where they're already going to have an entire department throughout, you know, their stores, their head offices, etc. It really, really, you know, makes me lose any competitive edge that I have."

CONTOVERSY #4: Misaligned understanding of roles, responsibilities, and priorities between SMEs and industry. SMEs have a heavy reliance on 3rd parties for cybersecurity services [42]. This study finds that the roles and responsibilities of SMEs and their 3rd party providers are not clearly defined. For example, discourses reveal that SMEs assume that the 3rd party vendor will take responsibility of all cybersecurity and privacy aspects, whilst the vendor may assume that the SME is bears the ultimate responsibility. This leads to misunderstandings with very real cybersecurity and privacy consequences. For example, SMEs may assume that compliance with requirements are met by the third-party vendor, while the vendor may assume that the SME is responsible for ensuring compliance.

Quote from cyber provider: "We have to be careful. We just make recommendations on cybersecurity measures, right? And they (SMEs) have to do their own due diligence, because there are liabilities (compliance with regulation) associated with the work in this sector, and we have to just be careful, right?"

Quote from cyber provider: "These are general guidelines that are issued, your, your compliance specific needs are something that you (a Canadian SME) have to own and manage separately, and link back to how these baseline security controls support that level of compliance."

Quote from SME: "I think we leave that (cybersecurity measures for my organization) up to our IT people, okay. And I can honestly say none of us think of that on a day-to-day basis. No, and that's strictly up to the IT people to bring it (cybersecurity threats and compliance with regulation) to our attention. Like a third party."

Furthermore, another discourse that emerged from our study is the difference in priorities between SMEs and their 3rd party cyber providers. 3rd party cyber providers often introduce cybersecurity for

privacy at a level that is not required for SMEs, because they are primarily motivated by factors other than just the optimal cybersecurity for privacy measure for Canadian SMEs.

Quote from SME educational expert: “When they do introduce cybersecurity into the discussion, it’s often at a level that isn’t appropriate, in my view, for SMEs. Because the discussion takes on a threat-based tenor. And that's not helpful for small and medium businesses. So, you know, and often it'll associated to a vendor, right? It looks like a vendor will do this out of their spirit, you know, because they're being altruistic. Well, no, not really, because it's marketing, right. They’re trying to make money. And I'm not going to take anything away from them.”

Quote from SME: “I'm not even sure how we got hooked up with the last one. They were the worst. We've just switched again. So every time you switch, it's, it's different because the way they approach it is very different to each other, and their recommendations, what they recommend, and the volume of what they recommend, also change depending on who you ask and a lot of it comes down to service in quickness of responding and giving me what I want and nothing more.”

CONTROVERSY #5: Government’s come-to-me model. The government plays a critical role in coordinating and disseminating information for SMEs regarding cybersecurity and privacy threats, vulnerabilities and legislation. Our study finds that SMEs view the government’s current communication measures as ineffective. They view the current model used by the government as a passive come-to-me model, with the government being viewed as unapproachable and with SMEs preferring a proactive here-you-go model whereby the government reaches out actively to the SMEs. A vast majority of SMEs spoken to in the study had little to no idea of PIPEDA guidelines, standards (CyberSecure Canada) and requirements, hindering their ability to effectively protect their systems and data.

Quote for bad communication from SME: “I would say it's (government communication on cybersecurity for privacy) remarkably bad. I think the only people that are treating it with seriousness are those in the tech field and coming from a tech field.”

“Unfortunately, I have not heard of any legislation that applies to the privacy aspect.”

“That's the problem is that both the federal and the provincial models rely on come to me, as opposed to I'm coming to you, I'm bringing this to you. Right?”

Quote for bad communication from cyber provider: “So I feel like the government has resources on the education side, but very few people know about that. Like I'm always providing that as a resource. And people are like, Oh, where do I find that? So I think what they need, like they're building the education or the library or the knowledge base but they're not marketing it very well, like they need to market it so that every SMB knows that this information is out there and they have to use it.”

When SMEs did express a knowledge of PIPEDA, it was not viewed as a serious piece of legislation, with SMEs expressing the view that the government would not take action against them.

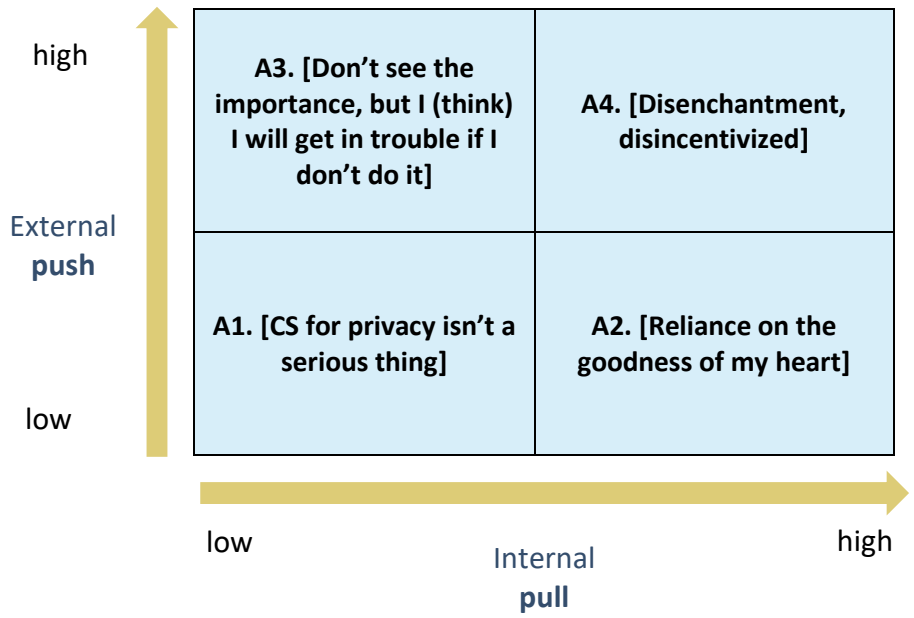
Quote from SME: “There’s no policy. Like even PIPEDA, the privacy thing. No small business knows what it is, nor gives a crap about it. Because the Privacy Commissioner is never going to fine a small business. They’re not going to find a small accountant, or a car dealership, or a dentist. They’re never going to do that. They barely fine large enterprises. So there’s no reason for us to care about that.”

Quote from cyber provider: “The Privacy Commissioner has not charged any small business. There’s no legal precedents, and even the cases they’ve brought to court have been like billion-dollar things, and they’re usually just settled. So the reality is no SME will ever care about that.”

Current state of cybersecurity for privacy in Canadian SMEs

One way of understanding the challenges faced by Canadian SMEs with regard to this topic is to analyze the push and pull forces that affect their cybersecurity and privacy. In this context, the pull forces refer to the internal organizational factors that drive SMEs to invest in cybersecurity measures for privacy, while the push forces refer to the external factors that compel them to do so. By examining these forces, we can gain a better understanding of the factors that influences cybersecurity and privacy decisions in Canadian SMEs, and identify strategies for improving their cybersecurity posture. We find that the Canadian SMEs can be classified and characterized into the following 4 categories as outlined in Table 1.

Table 1: How do Canadian SMEs view cybersecurity for privacy?



A1. *CS FOR PRIVACY ISN’T A SERIOUS ISSUE*

SME’s often underestimate the importance of cybersecurity and privacy measures [43], which results in a lack of cybersecurity and privacy measures. In this particular category, we identify discourses surrounding on how SMEs with a low internal pull to adopt cybersecurity for privacy, when there is low perceived push for adoption from external stakeholders. Our study uncovers several reasons as to why that is. Firstly, we find that Canadian SMEs see cybersecurity for privacy as a cost, with no visible return on investment or incentives. A table of codes of discourses for this category can be found in Table 2.

Quote from SME: “Tie it in with kind of incentive, whether it's through taxes, or it's a credit, or, or just

something within the business, because then say when you're doing taxes at the at the end of the year, and it's like, hey, you know what you're, you're gonna be paying this much, right, you have this much income tax that you got to pay or corporate tax, depending on how, however you're registered. And you can, instead, you can throw some money into here (cybersecurity for privacy), you can bring it into the business, you're not gonna have to pay that tax, and you're gonna be a little bit more protected. Otherwise, it's hard to justify the cost."

Second, we find that SMEs feel like they do not have enough of a voice into cybersecurity for privacy practices and guidelines that affect their business, which causes them to have difficulty buying into the adoption and implementation of cybersecurity for privacy.

Quote from SME: "Do we have enough representation? No, we do not have enough of a voice at this point. Though, there's a lot I mean, you know, I want to be cautious as I say that the Canadian government and the Canadian Privacy Commissioner's Office does put out consultation. So, there are public consultations that are had groups like ours respond to those consultations. And there's an opportunity to but it is not an intent."

Quote from SME: "I feel like the government can do a better job. Having like, more inclusion of us, the people that their policies actually affect, would be so much better, you know? There's a reason why the CyberSecure Certification rate is so low. Because nobody knows about it, we weren't consulted about it, and the implementation is just crazy. It'll never go anywhere. Because it's not required. There's no financial motivation to pay five G's to get certified, because it means nothing."

Third, we find that the perceived lack of consequences and incentives when Canadian SMEs do not have cybersecurity for privacy measures and practices in place adds to the perception of cybersecurity for privacy not being a priority.

Quote from SME: "Well, I think at this point, the state hasn't done enough to support SMBs, right. Why would anyone care about that (CyberSecure Canada)? Like it's just more noise. But if you said this is CyberSecure candidate, if you go through the process, and the training is free by the government, it's going to cost you $5,000, but it will immediately qualify you for cyber insurance and you'll get a $2,500 discount on your first year premium. People will do that."

Quote from SME: "GDPR is fine-ing people left, right and center which has been awesome so that we can actually demonstrate that GDPR works and that they are being fined. But in Canada, no. No consequences. So why would people take it seriously?"

Finally, we find that the understanding and translating of cyber risk to organizational risk is still an ongoing process.

Quote from cybersecurity expert and educator: "And I think there's a misunderstanding of what cybersecurity actually is. And I think that that's a primary example. For example, I teach IT practitioners and providers on cybersecurity. And they go, oh, well, I didn't know it was that. And it's about protecting the business. Oh, well, if it's about protecting the business, that gives them a little different understanding, but talking to them about billions of threats that are potentially pinging on them every day, and they need to do all this stuff, and they need to put up the software and they need to do this

and they should be doing that. And that's the messaging they're hearing from the broader cybersecurity community."

Quote from cybersecurity expert and educator: "Cyber providers still don't entirely understand how the risks associated with technology actually translate into business risks, they think about them as very independent. Like it's a technology issue that haven't connected the dots yet fully to it being a business issue."

Table 2: Coding Table of Discourses - CS for Privacy isn't a serious thing

Cybersecurity doesn't apply to me (low internal pull, low external push)
• As an SME, my need for cybersecurity is not there. other processes take priority. • Comfort in existing practices pre technology • Cybersecurity is a long-term mindset, it's a later problem • I don't see the return on investment in cybersecurity. It's not required, and there are also no incentives • No sense of urgency for cybersecurity • Older generation doesn't see the importance of cybersecurity and privacy • Law not taken seriously because there is no precedent for them to sue SMEs • Government suggests practices, but these practices do not necessarily keep you in compliance with regulation • Government initiatives do not help as many SMEs as they think it does • Government just puts out policies and thinks their job is done, without following through properly with implementation • Cybersecurity is currently a come to me model for help and they (government) are not approachable

A2. *RELIANCE ON THE GOODNESS OF MY HEART*

In this particular category, we identify discourses on how SMEs with a high internal pull to adopt cybersecurity for privacy, when there is a low perceived push for adoption from external stakeholders. A table of codes of discourses in this category can be found in Table 3.

We find that trust and integrity are key factors. SMEs in this category view the trust a consumer has placed in them when giving the SME their data as highly valuable, a serious responsibility, and a reflection of the integrity of the organization and industry.

Quote: “At some point along the way, you’ll realize that this is information that they trusted you to keep confidential, and if there’s that trust (between the customer and SME), then that entails some responsibility, whether you want it or not.”

Quote: “Because we understand that we treat our customers as, you know, not our friends, but people that trust us and keep coming back to us because they respect the fact that we’re giving them the best care for their information. So for me, personally, I kept that in mind and wanted to protect the information that we collect.”

Quote: “It’s important to maintain the integrity of the profession and organization, and keep data safe.”

Table 3: Coding Table of Discourses - Reliance on the goodness of my heart

Reliance on the goodness of my heart (high internal pull, low external push)
• its important to maintain the integrity of the profession and organization, and keep data safe • at some point along the way, you'll realize that this is certain information that you have to actually keep confidential but also, if there's that trust (between the customer and me), then that entails some responsibility, whether you want it or not • Because we understand that we treat our customers as as you know, not our friends, but also people that trust us that that are coming back to us because they they respect the fact that we're giving them the best care but also obviously like you said before, protecting the information that we collect. So for me personally, I kept that in mind.

A3. *DON’T SEE THE IMPORTANCE, BUT I (THINK) I WILL GET IN TROUBLE IF I DON’T DO IT*

In this particular category, we identify discourses on how SMEs with a low internal pull to adopt cybersecurity for privacy, when there is a high perceived push for adoption from external stakeholders. A table of codes of discourses in this category can be found in Table 4.

First, we find that although SMEs in this category does not view data as a serious responsibility entrusted to them by consumers, they view it as a source of competitive advantage.

Quote: “Consumer concerns influence my adoption. Certainty, if they feedbacked to me that they were concerned, I would definitely implement it, right? Because if I don’t, they’ll leave, and I’ll lose money. If I do, and I get ahead of it, I can be ahead of my competitors.”

Second, we find that SMEs in this category don't view cybersecurity for privacy as important, but are wary of the negative consequences that could potentially affect them if they do not implement cybersecurity for privacy measures.

Quote: "The government has in place that you have to keep the info for housing real estate intact. Your clients infer that it's securely kept all their information and protects the business as well because then you're obviously protected from all that. You don't have to go against the government."

Quote: "It's kind of an inferred process from the government to keep data safe in my industry in Ontario from the province because there are ways to complain to them about cybersecurity and privacy of data, but they could come in and say hey you're not doing these things. I don't think anything (of consequence) actually happens though, but we just don't want to be even involved in that."

Table 4: Coding Table of Discourses – I don't really see why it's important, but I (think) I get in trouble if I don't do it, so I do it

I don't really see why it's important, but I (think) I get in trouble if I don't do it, so I do it. Data is not something I intrinsically protect or care about from the goodness of my heart – it is a source of competitive advantage (low internal pull, external push high)
• consumer demand for cybersecurity drives adoption • consumer concerns influence adoption • Some government agencies push for cybersecurity adoption • the government has in place that you have to keep the info for housing real estate intact. Your clients infer that it's securely kept all their information and protects the business as well because then you're obviously protected from all that. You don't have to go against the government. • It's kind of an inferred process from the government to keep data safe in my industry in Ontario from the province because there are ways to complain to them about cybersecurity and privacy of data, but they could come in and say hey you're not doing these things. I don't think anything (of consequence) actually happens though, but we just don't want to be even involved in that.

A4. *DISENCHANTMENT, DISINCENTIVIZED*

In this particular category, we identify discourses on how SMEs with a high internal pull to adopt cybersecurity for privacy, when there is a high perceived push for adoption from external stakeholders. A table of codes of discourses in this category can be found in Table 5.

First, we find that the proactiveness of a SME can conflict with the technology supplied by cybersecurity providers. The goals of cybersecurity providers and SMEs are not aligned (cyber providers aim to sell as many measures as they can so they can profit, and proactive SMEs who proactively seek out cyber measures can inadvertently end up weakening their cyber defenses).

Quote: "I don't mean this in a negative way, but their (goals) are not necessarily to protect consumer privacy as much as me, a business owner."

Quote: "I mean, in some cases, you have people who, like the owner is one of them, he inadvertently put two different protection programs on his computer at home, thinking he was giving himself double the protection and in actual fact, they kind of blocked each other out. So he got hacked, he got broken into."

Second, we find that heightened levels of internal drive by an organization and information on cybersecurity and privacy being much more comprehensive than what most SMEs need can afflict paralysis on SMEs, which could alienate and discourage SMEs from cybersecurity for privacy.

Quote: "I heard about so many threats out there that could affect my organization. There was so many. I'm not able to manage them all! I don't think I'm significant enough for them (hackers) to target me anyway, there are much bigger threats out there. I don't even know if I get the technology if I'm going to 100% be able to defend myself from these breaches. They happen to people with even better defenses and resources than me!"

Table 5: Coding Table of Discourses – Disenchantment and Disincentivized

Disenchantment, disincentivized. A fragile state, teetering on the ledge (high internal pull, external push too high)
• I don't mean in a negative way, but their (cyber providers) goals are not necessarily to protect consumer privacy as much as me, a business owner. • Proactive cyber actions backfired because of conflicting tech given by providers. • I heard about so many threats out there that could affect my organization. There was so many. I'm not able to manage them all! I don't think I'm significant enough for them (hackers) to target me anyway, there are much bigger targets out there. I don't even know if I get the technology if I'm going to 100% be able to defend myself from these breaches. They happen to people with even better defenses and resources than me!

Recommendations by SMEs

As part of our study, we asked Canadian SMEs what they would need (tools, resources, structure) from stakeholders in order to become more cybersecure. Five dominant discourses/recommendations emerged from our study, with coding for these two discourses being coded in Tables 6 and 7 respectively.

RECOMMENDATION #1. INCENTIVES – THE CARROT. A common discourse that emerged throughout the interviews was one of incentives. SMEs currently view security measures as a cost with no visible benefits to their business, and they do not view cyber risks as a key operational risk to their business. SMEs suggested tying in incentives, in various forms (e.g., tax rebates, direct cash, specialized insurance) to cybersecurity measures. A detailed table of codes of discourses for this recommendation can be found in Table 6.

Table 6: Coding Table of Discourses – Incentives

INCENTIVES – THE CARROT
• Incent us, I think if we incent all SMBs through either, like a tax refund some of the district credit program or, you know, just incredibly direct cash 50 bucks, something, make and then the same for small businesses like money works. And, you know, or having some type of insurance available that they can afford. That's another one that we can create, like a computer Health Insurance Program, or that the BDC will make specialized insurance. • I think a good thing would be for if, especially if it's the government wanting people to become more cybersecure for their own protection, as well as kind of state protection, some form of incentive would definitely be beneficial. Think like with electric cars when they like when Tesla first started coming, and you kind of got that like $7,500 kickback or whatever it was to go electric. A lot of people said hey, you know, let's do it. Depending on the cost of the cybersecurity, not 100% Sure what like the write off rules would be with taxes, but if say it's a low percentage like hey, you know, what, you bring the software into the business and we you can get like 80% back on your on your business. So, you get an 80% reduction there. Like I feel like that would be huge. • Yeah, there needs to be some stick or some carrot like right now. It's just like you making a certain certification and saying, this is a me security certification. Okay. Why would

anyone care about that? Like it's just more noise. But if you said this is CyberSecure candidate, if you go through the process, and the training is free by the government, it's going to cost you $5,000, but it will immediately qualify you for cyber insurance and you'll get a $2,500 discount on your first year premium. People will do that. I will do that. That's worthwhile because insurance is hard to get.

RECOMMENDATION #2. A TRUSTED RESOURCE TO TURN TO FOR HELP. A controversy identified earlier in the report indicated how the priorities of the industry and SMEs are not always aligned. With limited resources that SMEs have, and high noise levels surrounding cybersecurity and privacy, SMEs indicated that they need specific, tailored, consistent help and messaging from a centralized location - with SMEs and organizations supporting SMEs expressing a view that traditional avenues are not meeting their needs. A detailed code of discourses for this recommendation can be found in Table 7.

Table 7: Coding Table of Discourses - A trusted resource for help

A TRUSTED RESOURCE FOR HELP
• I think we have to, we have to come up with some kind of plan, or information or resource to us, so we can feel like things are accessible without being overwhelming. Because right now it's overwhelming. So companies that provide this service need to be more, more able to, to provide a better understanding of what is required for cybersecurity, and why certain companies need like hospitals need one level and we need you know, the rest of us little businesses, we need something completely different. • It's almost like it's almost solely pull by the cybersecurity community to get SMEs engaged. And I don't want to take away from any of the efforts that had been utilized by the Chambers of Commerce and Business Federation's and things like this one or associations not going to take away from anything they do, because but they it's not their job to do that they've got a lot of other advocacy things going on. • There's local support networks that have popped up. So there's places that a small medium business can go and get access to

information right now. But it's, it's very foundational, and often expresses the importance but doesn't always give them the resources required to act on it. And it is still left up to the small medium business to really figure out which resources make the most sense for them.

- I would suggest something needs to happen with these types of organizations (3rd party vendors). Perhaps some sort of non-profit organization, right? Where they don't, don't typically sell a lot of product to SMEs. So but anyway, so that's, that's where I think we get could get a lot of the information.
- The other places are, again, trade associations, industry associations, and things like that, which I know have been helpful as well. But a lot of us don't even bother with those things, right? Because, again, they tend to cost money, you need to be a member before you're gonna get any, the tools and stuff they use.
- The Canadian Center for cybersecurity, if you go on their website, they're the technical authority, but everything else, they're not the policy authority, they're not the authority for small medium businesses, they're not the authority for critical infrastructure, we don't know if their practices are a precursor or maintenance to compliance with legislation, they're not the authority for so there is no centralized authority for cybersecurity in Canada, which is a problem, and the same thing ripples down through the provinces.
- Have a centralized source. An organization that isn't trying to sell anything, that works with the government and other stakeholders, and us, to create a platform that aligns with the needs of SMEs. Then at least there's a central repository. There needs to be a repository of knowledge that the entire SME segment in Canada can go to as a starting point.
- I don't think it's.. I don't think it's having any impact. I support them because I know they're, they're trying to make a difference. I don't disagree with their efforts. I'm commenting on the effect. Like no small business owner knows that there's a provincial Privacy Commissioner, nor do they care. So they're talking to the wind and

I commend them for trying but it's not reaching the person that they need to speak to. • And like, there's a lot of policy people talking to each other. There's a lot of security people talking to each other. Okay, but it's no point because we're not talking to the business owner that we need to speak to.

RECOMMENDATION #3. BETTER COMMUNICATION AND MARKETING. A common discourse the study has uncovered is need for better communication and marketing. SMEs and associations helping SMEs express a concern about existing materials from the government and the industry being hard to find, and existing communication occurring in closed loops, without reaching the intended audience (SMEs). A table of codes from discourses can be found in Table 8.

Table 8: Coding Table of Discourses: Better communication and marketing

BETTER COMMUNICATION AND MARKETING
• So, I think the government has found a great way to communicate things in simple terms, in layman terms for SMEs to digest. The problem is that very few people know about this. Like I'm always providing that as a resource to SMEs, and people are like, oh where do I find that? • My LinkedIn feeds are full of people advertising the stats, but you're not reaching the right people. You're reaching like, you know, it's like an echo chamber, like you're yelling at all the other cyber professionals. We already know those stats. So really, I feel like they need a marketing effort that reaches the non-technical people, especially the Dairy Queens and the restaurants that collect your birthday so that they send you a few coupons. All those people need better cyber. • They're (The government) not active. Like there's no public information there. Their Twitter, they barely post anything. Like the American department posts constantly like I get multiple emails from their newsletters per day, with advisories and tips and stuff like that. Canadian resources just not active so no one knows about them. If they're supposed to be working for public safety,

they're just not engaging with the people that they're responsible for, like the business owners definitely don't know they exist, right. • Definitely the easiest thing for the government to do is educate like it's super easy to put out free information, free tips, free guides. So that's super easy to do, because like you need a Twitter account and an intern to just publish stuff and a researcher to make the content super easy to do. That's what the that's what this does in the United States. Like I got a team of, of outreach personnel that is doing constant education. Cool little graphics that they make on Canva. And just like every day, they're saying, hey, remember, reset your passwords, you know, like that kind of stuff. Super easy to do. Cheap, hurts no one. And it helps because when the small business owner sees reset your passwords, they'll say, oh my god, I haven't reset my passwords. In my life.

RECOMMENDATION #4. CLEAR MESSAGING AND MORE CONSULTATION. As earlier outlined in controversy #1, there exists a difference in views as to when approaching cybersecurity and privacy issues, by different stakeholders. For instance, cyber professionals generally apply a threat-based approach and try and capture privacy requirements and threats within the broader cybersecurity approach. SMEs, on the other hand, tend to prioritize privacy requirements over the broader, more obscure cybersecurity requirements. As a result, cybersecurity actions for privacy measures may not always be identified. With that in mind, cybersecurity specifically for privacy measures should certainly be identified and documented to support compliance monitoring and audits. SMEs, and industry experts suggest that more consultation and engagement would help all stakeholders understand what is needed. A table of codes from discourses can be found in Table 9.

Table 9: Coding Table of Discourses - Clear messaging and more consultation

CLEAR MESSAGING AND MORE CONSULTATION
• I rarely get consulted on these types of things. There's lots of opinions around on all this stuff. So there is a consultation process, but it's relatively limited. The interesting thing is that the process is full of experts, but nobody has actually, sort of rounding out of that expertise into what is needed into the public domain.

• And one of the biggest struggles I had was explaining cybersecurity, in practical terms to engineers and cybersecurity specialists, right. And encryption people because they are immersed in their own biz, right. They're immersed in their own thing. So I think there isn't, there aren't really good mechanisms where people can actually manage that discussion. • Do we have enough representation? No, we do not have enough of a voice at this point. Though, there's a lot, I mean, you know, I want to be cautious as I say that the Canadian government and the Canadian Privacy Commissioner's Office does put out consultation. So there are public consultations that are had, and groups like ours respond to those consultations. So there's an opportunity to, but it is not an intent. So part of their process to say, do we have enough representation effectively.

RECOMMENDATION #5. ENFORCEMENT – THE STICK. Finally, SMEs commonly expressed that they are not the focus of privacy legislation. Additionally, SMEs expressed that there were no perceived consequences for not being in compliance with legislation and practices, leading to an aloof and detached demeanour towards legislation. A table of codes from discourses can be found in Table 10.

Table 10: Coding Table of Discourses - Enforcement (The stick)

ENFORCEMENT – THE STICK
• I mean, first of all, privacy laws are playing catch up in Canada. And small medium businesses aren't the biggest focus for them. The biggest focus is actually getting enterprises and public sector where the impact of privacy breaches is much greater. That's I think where a lot of the legislation and policy work is likely being focused now. • No one takes it (legislation) seriously. This is like a parent trying to discipline your kids sooner or later. You got to bring the stick down or else they'll just never believe you will. • There's nothing as far as I know, there's nothing in Canada that forces either with carrot or stick to get into cyber protection of data for a SME. • Canadians, like, many reasonable people, they don't want to lose their money. They don't want to lose their personal information. We all value it. The gap is that

	you and I and regular people say I value my privacy. That's why I use ad blockers and stuff. But then you go to your lawyer, and you assume that the lawyer took the proper precautions to protect your information, but you don't know that CyberSecure tries to do it with a badge. I feel like there's no point because they're not going to volunteer. There's got to be a little bit of stick with this carrot.

Our Recommendations

RECOMMENDATION #1. Certification and evaluation of SMEs cyber hygiene. Our findings suggests that a high external push, in the form of consumer demands and concerns from the Canadian public, can have an effect on cybersecurity adoption by Canadian SMEs. There is evidence to show that Canadians are wary, and prioritize how businesses handle and protect their data when it comes to providing them with their business – otherwise they will go elsewhere. For example: 1) 88% of Canadians said they were at least somewhat concerned about how companies and organizations use their online personal information [44], 2) 71% of Canadians have refused to provide an organization or business with their personal information due to privacy concerns [43], and 3) 40% of Canadians have stopped doing business with a company that experienced a privacy breach [43].

Additionally, the existing literature shows that trust between consumer and business is very important. Evidence in the literature has shown that building the consumer-company relationship should be grounded in trust, with trust being the consumer's belief that a company will act in the best interests of their consumers and keep their promises [45], [46]. This trust significantly contributes to positive outcomes for the business (e.g., consumer retention, overall market performance). Unfortunately, this trust seems to be lacking in the Canadian landscape today. Indeed, results show that a majority of Canadians (55%) do not believe and do not trust that businesses respect their privacy rights [43].

We suggest, that in an effort to build and cultivate trust, and address consumer demands and concerns about privacy from the Canadian public, there should be an initiative that allows for transparency about an organization's cyber hygiene levels. As of present writing, there is no established way for consumers and the Canadian public to know the efficacy of the practices employed by SMEs and organizations to store and secure their personal data. These set of practices that organizations perform regularly to manage the pervasive cybersecurity risks and security of users, devices, networks and data has been defined as cyber hygiene [47].

Studies have shown that a consumers' evaluation on a company's efforts to be transparent and socially responsible will be critical in predicting how trustworthy the company is being perceived [48]. There is a need for more detailed certification and evaluation process to help consumers in this regard. We note that a form of certification already exists for Canadian SMEs, in the form of CyberSecure Canada. However, as reported in the findings and controversies of the report, the stimulus for SMEs to certify themselves with this program is just not there (at the moment).

The importance of certification and evaluation for the consumer has not gone unnoticed by the industry. For example, certification and evaluation processes are even being developed by the industry (e.g., Iceberg Cyber). Iceberg Cyber uses publicly available data on SMEs to evaluate their cyber hygiene, based on select criteria, and ultimately provides a score on their cyber hygiene.

This certification and evaluation initiative has been used successfully in different contexts. For example, the National Environment Agency in Singapore led a certification program for food retail establishments in the services industry to restore public confidence in its facilities and in public sanitation [49]. This certification required food stalls to have a minimum standard of hygiene to operate, based on a framework that was developed through a tri-partite agreement (government, industry, and consumer). Hygiene grades (Image 1) are issued to food stalls, and the grades are required to be displayed on the store front (a visible part of the store facing consumers). Since the introduction of this scheme, this grading system has helped raise the hygiene standards in food retail establishments, with 99% of licensees being graded either 'A' or 'B' in 2017, a 22% increase since 2006 [48].

Figure 1: Hygiene Scale

We believe that an initiative that provides consumers with an evaluation of the efficacy of a businesses' cyber hygiene and practices would impact the consumer trust levels in businesses positively - by providing transparency to the efficacy of business cyber practices and providing organizations with the push that they would need.

RECOMMENDATION #2. Better communication and consultation. The findings from this research study indicate an urgent need for a more pro-active communication strategy from the government, as well as for a greater diversity of stakeholder voices to sit at the table. We echo the calls for improvement from SMEs about the accessibility of resources without being overwhelming. The findings from this report indicate that from a Canadian SME's perspective, it is largely left up to the industry at the present time to dictate and communicate what the needs of SMEs are. We heard clearly that a more centralized approach about what needs to be communicated, and a centralized location where that information can be found, would go a long way to meeting the needs of Canadian SMEs – with current communication about cybersecurity and privacy either being inefficient, or occurring in closed loops. Taking a targeted consultative approach to understand the different and diverse needs of SMEs, and establishing a baseline standard of cybersecurity, and cybersecurity for privacy - which all industries and sectors can build on, would help make Canadian SMEs more cybersecure.

Summary

The findings from the research study highlight how humans have significant impact on cybersecurity: their attitudes, experiences, and the way they view cybersecurity affects their subsequent approach and practices. For example, the findings of the study suggest that cybersecurity, being dominated by the technical community, often neglects the non-technical and human aspects of cybersecurity (the people and processes), which leads to significant confusion around cybersecurity messaging and communications. The results of the study are, therefore, a call to action for policy makers, industry, educators, and SMEs to improve upon how we approach, view, and communicate cybersecurity and privacy. Interviewees consistently called out a lack of clarity, implementation, and enforcement of current approaches that has led to a distinctly aloof and poor understanding of cybersecurity and privacy. This manifests itself in the 5 controversies identified: 1) differences in how CS and privacy are viewed, 2) problematic education levels, 3) CS for privacy viewed as unnecessary costs, 4) misaligned roles, responsibilities and priorities between SMEs and the industry, and 5) the government's come-to-me model. They were equally clear about wanting: 1) more incentives, 2) more enforcement, 3) a trusted resource for help, 4) better communication and marketing, and 5) clear messaging and more consultation.

Works Cited

[1] S. Walton, P. R. Wheeler, Y. Zhang, and X. Zhao, 'An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions', *J. Inf. Syst.*, vol. 35, no. 1, pp. 155–186, 2021.

[2] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, 'Decision support approaches for cyber security investment', *Decis. Support Syst.*, vol. 86, pp. 13–23, 2016.

[3] IBM and Ponemon Institute, 'Cost of a Data Breach Report 2020 Highlights', p. 1, 2020.

[4] J. L. Higgs, R. E. Pinsker, T. J. Smith, and G. R. Young, 'The Relationship between Board-Level Technology Committees and Reported Security Breaches', *J. Inf. Syst.*, vol. 30, no. 3, pp. 79–98, Jan. 2016, doi: 10.2308/isys-51402.

[5] L. Kauspadiene, A. Cenys, N. Goranin, S. Tjoa, and S. Ramanauskaite, 'High-Level Self-Sustaining Information Security Management Framework', *Balt. J. Mod. Comput.*, vol. 5, no. 1, pp. 107–123, 2017, doi: 10.22364/bjmc.2017.5.1.07.

[6] P. Neal and J. Ilsever, 'Protecting information: Active cyber defence for the business entity: A prerequisite corporate policy', *Acad. Strateg. Manag. J.*, vol. 15, no. 2, p. 15, 2016.

[7] M. T. Siponen, 'An analysis of the traditional IS security approaches: implications for research and practice', *Eur. J. Inf. Syst.*, vol. 14, no. 3, pp. 303–315, 2005.

[8] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, 'Correlating human traits and cyber security behavior intentions', *Comput. Secur.*, vol. 73, pp. 345–358, 2018, doi: https://doi.org/10.1016/j.cose.2017.11.015.

[9] N. Manworren, J. Letwat, and O. Daily, 'Why you should care about the Target data breach', *Bus. Horiz.*, vol. 59, no. 3, pp. 257–266, 2016.

[10] A. D'Amico and E. M. Roth, 'Introduction to Special Issue of the Journal of Cognitive Engineering and Decision Making Special Issue Focus: Cybersecurity Decision Making', *J. Cogn. Eng. Decis. Mak.*, vol. 9, no. 2, pp. 115–116, 2015.

[11] B. von Solms and R. von Solms, 'Cybersecurity and information security – what goes where?', *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, Jan. 2018, doi: 10.1108/ICS-04-2017-0025.

[12] A. Klimburg, *National cyber security framework manual*. NATO Cooperative Cyber Defense Center of Excellence, 2012.

[13] International Telecommunication Union, 'Cybersecurity', 2010. Accessed: Sep. 12, 2021. [Online]. Available: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20.pdf

[14] S. A. Adams *et al.*, 'The governance of cybersecurity', 2015.

[15] International Data Corporation Canada, 'National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age', Dec. 21, 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (accessed Sep. 10, 2021).

[16] M. D. Cavelty, 'Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities', *Sci. Eng. Ethics*, vol. 20, no. 3, pp. 701–715, 2014.

[17] V. J. Richardson, R. E. Smith, and M. W. Watson, 'Much ado about nothing: The (lack of) economic impact of data privacy breaches', *J. Inf. Syst.*, vol. 33, no. 3, pp. 227–265, 2019.

[18] T. Caldwell, 'Securing small businesses–the weakest link in a supply chain?', *Comput. Fraud Secur.*, vol. 2015, no. 9, pp. 5–10, 2015.

[19] K. Renaud and G. R. S. Weir, 'Cybersecurity and the Unbearability of Uncertainty', in *2016 Cybersecurity and Cyberforensics Conference (CCC)*, Aug. 2016, pp. 137–143. doi: 10.1109/CCC.2016.29.

[20] Insurance Bureau of Canada, 'Small Businesses in Canada Vulnerable to Cyber Attacks', 2019. [Online]. Available: http://assets.ibc.ca/Documents/Cyber-Security/IBC-Cyber-Security-Poll.pdf

[21] I. Government of Canada, 'Key Small Business Statistics - November 2019 - SME research and statistics', 2019. https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03114.html (accessed Sep. 10, 2021).
[22] R. C. McMurrian and E. Matulich, 'Building customer value and profitability with business ethics', *J. Bus. Econ. Res. JBER*, vol. 14, no. 3, pp. 83–90, 2016.
[23] E. Yaghmaei *et al.*, 'Canvas white paper 1–cybersecurity and ethics', *Available SSRN 3091909*, 2017.
[24] D. E. Palmer, 'Pop-ups, cookies, and spam: toward a deeper analysis of the ethical significance of internet marketing practices', *J. Bus. Ethics*, vol. 58, no. 1, pp. 271–280, 2005.
[25] I. van de Poel, 'Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security', *Ethics Cybersecurity*, p. 45, 2020.
[26] J. Domingo-Ferrer and A. Blanco-Justicia, 'Privacy-Preserving Technologies', in *The Ethics of Cybersecurity*, Springer, Cham, 2020, pp. 279–297.
[27] Federal Trade Commission, '16 CFR Part 314 -- Standards for Safeguarding Customer Information', 2023. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314 (accessed Mar. 14, 2023).
[28] National Institute of Standards and Technology, 'Small Business Cybersecurity Corner', *NIST*, Oct. 2018, Accessed: Mar. 14, 2023. [Online]. Available: https://www.nist.gov/itl/smallbusinesscyber
[29] E. Higgins and A. Perusse, 'Canadian SME Cybersecurity Initiatives and Programs', 2021. [Online]. Available: https://www.wto.org/english/tratop_e/msmes_e/cybersecure_canada_18221.pdf
[30] Rogers Cybersecure Catalyst, '"Simply Secure" A Rogers Cybersecure Catalyst initiative', *Simply Secure*, 2023. https://simply-secure.ca/ (accessed Mar. 14, 2023).
[31] European Union Agency for Cybersecurity, 'Cybersecurity for SMEs - Challenges and Recommendations', *ENISA*. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes (accessed Mar. 14, 2023).
[32] N. Fairclough, 'Peripheral vision: Discourse analysis in organization studies: The case for critical realism', *Organ. Stud.*, vol. 26, no. 6, pp. 915–939, 2005.
[33] P. LeVine and R. Scollon, *Discourse and Technology: Multimodal Discourse Analysis*. Georgetown University Press, 2004.
[34] M. Christen, B. Gordijn, and M. Loi, Eds., *The Ethics of Cybersecurity*, vol. 21. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-29053-5.
[35] A. Fleming, C. Mason, and G. Paxton, 'Discourses of technology, ageing and participation', *Palgrave Commun.*, vol. 4, no. 1, pp. 1–9, 2018.
[36] J. M. Corbin and A. Strauss, 'Grounded theory research: Procedures, canons, and evaluative criteria', *Qual. Sociol.*, vol. 13, no. 1, pp. 3–21, 1990.
[37] Office of the Privacy Commissioner of Canada, 'Privacy and Cyber Security', Feb. 12, 2015. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/#fn17 (accessed Jul. 15, 2022).
[38] O. of the P. C. of Canada, 'Speech: The Interconnected Worlds of Privacy and Cyber-Security - April 20, 2016', Jul. 04, 2016. https://www.priv.gc.ca/en/opc-news/speeches/2016/sp-d_20160420/ (accessed Mar. 11, 2023).
[39] A. Barua, C. H. Kriebel, and T. Mukhopadhyay, 'Information technologies and business value: An analytic and empirical investigation', *Inf. Syst. Res.*, vol. 6, no. 1, pp. 3–23, 1995.
[40] Cybersecurity and Infrastructure Security Agency, 'Be Cyber Smart #CyberMonth', 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Awareness%20Month%202021%20-%20Why%20is%20Cybersecurity%20Important.pdf

[41] KPMG, ‘Cyber security services - KPMG Canada’, *KPMG*, Mar. 09, 2023. https://kpmg.com/ca/en/home/services/advisory/risk-consulting/cyber-security.html (accessed Mar. 14, 2023).
[42] OECD, ‘Digital security in SMEs’, in *The Digital Transformation of SMEs*, OECD, 2021. doi: 10.1787/cb2796c7-en.
[43] A. Alahmari and B. Duncan, ‘Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence’, presented at the 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA), 2020, pp. 1–5.
[44] Office of the Privacy Commissioner of Canada, ‘2020-21 Survey of Canadians on Privacy-Related Issues’, Jun. 15, 2021. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/ (accessed Jul. 10, 2022).
[45] A. Chaudhuri and M. B. Holbrook, ‘The chain of effects from brand trust and brand affect to brand performance: the role of brand loyalty’, *J. Mark.*, vol. 65, no. 2, pp. 81–93, 2001.
[46] T. Erdem and J. Swait, ‘Brand credibility, brand consideration, and choice’, *J. Consum. Res.*, vol. 31, no. 1, pp. 191–198, 2004.
[47] U. S. Government Accountability Office, ‘Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene | U.S. GAO’, Apr. 13, 2020. https://www.gao.gov/products/gao-20-241 (accessed Mar. 13, 2023).
[48] J. Kang and G. Hustvedt, ‘Building Trust Between Consumers and Corporations: The Role of Consumer Perceptions of Transparency and Social Responsibility’, *J. Bus. Ethics*, vol. 125, no. 2, pp. 253–265, Dec. 2014, doi: 10.1007/s10551-013-1916-7.
[49] National Environment Agency, ‘Food Hygiene Grading Scheme’, 2018. https://www.facebook.com/NEASingapore/photos/a.1420977064790303/2094840767403926/ (accessed Mar. 13, 2023).