Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada

Innovation, Science and Economic Development Canada

CyberSecure Canada Program

Final Report

July 2019

Prepared for Innovation, Science and Economic Development Canada
Supplier name: Quorus Consulting Group Inc.
Contract award date: March 5, 2019
Contract number: U1400-198102/001/CY
Contract value: $129,006.45
Delivery date: July 2019
POR Number: POR 132-18
For more information, please contact Innovation, Science and Economic Development Canada at:
IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca

Ce rapport est aussi disponible en français

This publication is available online at https://www.ic.gc.ca/eic/site/112.nsf/eng/home.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact:

Web Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: ISED@canada.ca

Cat. No. Iu4-266/1-2019E-PDF

ISBN 978-0-660-32481-4

Aussi offert en français sous le titre *Programme CyberSécuritaire Canada – Rapport final*.

Political Neutrality Statement

I hereby certify as Senior Officer of Quorus Consulting Group Inc. that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the *Policy on Communications and Federal Identity* and the Directive on the Management of Communications - Appendix C.

Specifically, the deliverables do not include information on electoral voting intentions, political party preferences, standings with the electorate or ratings of the performance of a political party or its leaders.

Signed:

Rick Nadeau, President
Quorus Consulting Group Inc.

Table of Contents

Executive Summary

Background and Objectives

The Government of Canada is committed to protecting the security and prosperity of Canadians in the digital age.

To support this, Innovation, Science and Economic Development Canada (ISED) and its partners are working to develop and establish a voluntary and recognizable cyber certification program to help small and medium-sized businesses (SMEs) protect themselves against cyber threats and increase their cyber resilience. The intent of the program is to enable SMEs to demonstrate to their business and consumer clients that they have completed a certification program and meet a baseline set of security practices.

This research seeks to ensure the successful launch, promotion, engagement and adoption of cybercertification by SMEs by providing:

- Insights on three creative identifier concepts (visuals and messaging);
- Preferred elements in presented creative concepts;
- Reaction and level of trust in the cyber secure "brand";
- Expectations established by cyber certification;
- Perceptions of the benefits and identification of any barriers to adoption; and
- Overall understanding and credibility of the messages presented (both written and visual).

Ultimately, the objective of this research is to establish a recognizable and credible brand for cyber security in Canada, increase resilience of SME cyber infrastructure against cyber-attacks, and increase the number of SMEs with an effective cyber security posture.

Research Results

Confidence in SME Cyber Security

To gain an initial understanding of the backdrop against which a certification program would be introduced, cyber security in general was explored with both consumers and with SMEs.

Consumer Perspective

When asked what comes to mind when considering "cyber security," most consumers limit their interpretation to financial transactions. In other words, they are primarily concerned that their debit or credit card information is protected and used ethically, and that the institutions ensure a refund should their cards be used without their permission. "Cyber security" also reminds some of how safe they feel using certain vendor websites, identity theft in general and "hackers" or viruses on their personal devices.

Consumers see limited risk if in fact they happen to deal with a SME that is compromised or unethical. Many consumers are also in some ways reassured because they believe that SMEs are not typically targeted by hackers.

Some consumers mentioned the following in terms of security when they are dealing with SMEs:

- Websites featuring “a small green lock” are secure when making online purchases.
- They feel more secure when dealing with SMEs and SME websites backed by third-party vendors or institutions like banks, PayPal, Visa, Interac and other similar POS service providers.

When asked what SMEs could or should do to make them feel more cyber secure, consumers did not have much in the way of solutions. Even if SMEs were to better communicate their level of cyber security, consumers generally accept that it is impossible to be completely cyber secure.

SME Perspective

SMEs are more concerned about their own level of cyber security. They explain it is a challenge for them to stay on top of everything related to their IT system and technology in general. Very few participants had staff dedicated to their IT systems and an important struggle for many is fitting the oversight of these systems in with other aspects of running or managing a small business.

When considering how secure they feel about their level of cyber security, most SMEs seemed to focus primarily, if not exclusively on data they may be collecting from their clients and less on any of their own internal corporate data (including data on their staff, financial data and proprietary data), and supplier-related data.

SMEs that are generally the most confident about their level of cyber security tend to be a “larger” company and are more likely to have built up internal expertise to address cyber security. Others with high levels of confidence include businesses with an expertise in cyber security or IT, those that believe they do not capture enough data that would warrant significant investment in cyber security and those that feel they don’t capture any data on their clients, or at least none of it is stored on computers.

Irrespective of where they would position themselves on the “cyber secure” spectrum, all SMEs accept that total security is unrealistic. They figure that if hackers can get into large companies, then they can get into theirs. When asked if cyber security is important in their choice of suppliers, businesses seemed split on the issue, however most agree that if they were evaluating two different suppliers for a given service or contract and that one could demonstrate cyber security and that another could not, that factor would weigh in the balance.

SMEs were also split on whether they are missing out on business opportunities because they cannot “prove” their level of cyber security. Some smaller SMEs felt they were missing business opportunities and some felt they could potentially bid on larger projects or become suppliers to larger clients if they could prove their level of security. Conversely, other businesses, especially traditional brick-and-mortar ones (e.g. small retailers, tradespersons) did not see this as an issue.

Role of Government in Supporting SMEs

Most SMEs and consumers believe there is a role for the federal government to play in terms of supporting SMEs become more cyber secure. The most common suggestion involves providing training, guidelines, best practices or checklists that SMEs could use to verify and improve their level of cyber security. Some suggested providing affordable IT software or systems or advising on the types of systems and software companies should have.

Support for government involvement was not unanimous, however. Some were opposed to any further regulation on businesses or having federal resources dedicated to an issue that, in their opinion, the private sector should be able to manage on its own. There were also concerns about whether the Government of Canada can be counted on given some of the IT-related challenges it has been facing, leading a few to doubt whether the Government of Canada was a trusted advisor in this area.

The idea of making a certain level of cyber security a requirement to be able to operate in Canada was met with mixed reactions. Most would seem to agree that SMEs need to provide a minimum level of cyber security, however, some were concerned about a "one size fits all" approach since some businesses warrant a higher level of cyber security compared to others, largely depending on the quantity and nature of the private information the company collects. Along these same lines, there were concerns among both consumers and SMEs that a cyber security requirement might be unfair to small businesses that may not have the resources or the means to meet the requirements.

General Concept Evaluation

Three different visual concepts were tested with focus group participants to obtain feedback on overall appeal and relevance and whether the concepts were the right fit for a cyber security certification program.

Feedback from participants <u>that apply to all three concepts</u> include the following:

- The red maple leaf was a strong Canadian symbol and a strength across all concepts.
- The maple leaf alone was not enough to indicate that the program is endorsed by the Government of Canada or that it is a Government of Canada program.
- Many were worried that the concepts were too simple and that any business could easily replicate and post the identifier without actually holding the certification. There needs to be a way to verify the authenticity of the certificate.
- The bilingual concepts were well received - some even liked those more than the unilingual concepts.
- Francophones clearly liked the language used in the English concept but felt the one in French lacking. In particular, they questioned the use of the word "fiable" – some felt it was not strong or impactful enough while others did not feel it related well to cyber security.
- Some would like to see the word "certified" integrated into the concept to convey that it is a certification and not a company logo or a product.

Feedback specific to each concept is summarized below:

- Concept A (Shield): The imagery was liked by many, as it communicated security. Many also liked the font that was used. On the other hand, while it conveyed security, it was not considered unique because they had seen shields used by other security-related companies.

- Concept B (Lock): The concept clearly conveyed “security” - nearly everyone saw a lock right away. A few liked that the “C” from cyber and “S” from secure were incorporated into the design of the lock. Some felt the lock looked open which conveyed weak security, and many would have preferred two font styles (similar to the font style used in the other two concepts).

- Concept C (Arch): The concept’s only strength was that a few considered it to be unique. On the other hand, this concept was often dismissed mostly because participants could not figure out what the image was and that it did not convey the notion of “security”. The font was also seen as weak and “not serious”.

Overall, consumers preferred the lock concept by a wide margin whereas SMEs were split between the shield and the lock concepts. The arch concept came in a distant third for both segments. An even stronger concept for many would be a combination of the image in the lock concept with the font style used in the shield concept.

Exploring a Program with Tiers

The tier concept was broadly dismissed by both consumers and SMEs, who far preferred the option whereby a company is either cyber secure or it is not. The main concerns participants had with a tiered approach included the following:

- Consumers felt it would take enough effort to notice the identifier, let alone the tiers. Besides, even if they noticed it, they believed that it would take a long time before they were sufficiently familiar with the program to know the difference between the tiers.
- SMEs felt that the tiers may not be something they will want to make public-facing, especially if they are anything other than Tier 3. They were concerned that their customers would question their level of cyber security irrespective of what the tiers actually mean.
- Some SMEs bluntly stated that if they are “only a Tier 1” then they are not going to advertise it – they believe it shows them as weak in terms of cyber security, which will hurt business, and furthermore it paints a target on their business to attract hackers.

- When considering how the tiers could be communicated to customers through the identifiers, many agreed that integrating the tiers into the visual concepts adds clutter.

Use of Colours in the Visual Concepts

Participants' reactions to the colours proposed were often instant and decisive - few liked any of the proposed colours. If forced to choose, participants would opt for either the status quo (i.e. the black and white concept) or, among the new options proposed, they would select the grey concepts.

While most simply did not like the colours proposed, some felt adding colour weakened the overall tone or message behind the visual concept. They believe that security needs to be conveyed through a serious or "hard" colour, rather than through the proposed colours.

Potential Impact on Competitiveness

Consumers are not likely to dramatically change their current shopping patterns based on whether or not a business has been cyber certified, again mostly because they trust the businesses with whom they currently deal. Consumers will not stop using a SME because they are not certified.

SMEs were split in terms of whether or not having the certification would have a positive impact on their business. SMEs interested in the concept of being cyber certified suspected it might become a competitive differentiator, it would be something that customers would notice, and it would help them become better businesses by being more proactive and by being more cyber "aware." For many SMEs, the impact on their business largely depends on the extent to which their customers will become informed about the program and fully understand what it means for them as consumers and what the SME went through to become certified.

- There is some appreciation that recognition of the program among consumers will not happen overnight and that any impact on their business may take time, a sentiment also echoed by some consumers.

Other than on a storefront or a website, participants would expect to see or use the identifier on places such as packaging, at the cash register/near POS machines, advertising, business cards, invoices and email signatures.

Expectations of the Program

Participants, especially consumers, struggled somewhat when asked what they believed the program should resemble. SMEs and consumers shared a common view on some of the main elements of the program, which would include the following, some of which speak to the role they see the Government of Canada playing in the program:

- The federal government would provide all certification proponents access to training, guidelines and best practices in the area of cyber security;
- There would need to be some sort of certification audit, with most participants assuming this would be done by an IT expert working for the Government of Canada (rather than being outsourced to a third party);
- There would need to be regular recertification.

Consumer Perspective

Consumers feel the program should include a significant effort focused on public education. Consumers would want to know certain details such as, but not limited to, what is being certified, how relevant it is to them as consumers and what the companies had to do in order to become certified. Ultimately, consumers just want the details surrounding the program to be public so that they can understand how the program benefits them.

If the program were to be introduced, many consumers would feel more secure in their dealings with SMEs in general even though many are not actively seeking out cyber security reassurances when they deal with SMEs.

A few consumers appreciated how the program could benefit Canadian SMEs in general even if it may not have a direct impact on them as consumers. If the program is an effort by the Government of Canada to support SMEs become more cyber secure, especially those that otherwise might not be able to do so on their own, then the program was generally seen as "pro-small business."

SME Perspective

SME participants had more specific expectations of the program:

- They wanted to be sure that this was a meaningful program and that certification and recertification did not represent additional administrative burden.
- The audit could include an *in situ* inspection as well as an external verification (e.g., by having auditors trying to hack the applicant's system);
- They would want the program to be financially accessible to newer and smaller companies. Many expected the certification process to be free, very low cost or relative to the size of their business to maximize take-up across companies of all shapes and sizes.

If the program were to be rolled out, the lift in confidence among SMEs when it comes to their own level of cyber security would be minimal, with many remaining fairly indifferent towards the program. Many were not convinced they would need to get the certification at all.

Admittedly, SMEs had no specific information on the program itself and until they see more details around what the program involves, including costs and the certification process, many were reluctant to commit to how their level of confidence could really change if the program were to be rolled out or whether they would get certified at all.

Role of the Government

The most common roles participants expect the government of Canada to play included:

- Promoting the program to the general public to ensure it is well informed about what the certification means;
- Establishing the standards of certifications;

- Conducting the audits, the certifications and the recertifications, including ad hoc testing to make sure that certified companies continue to be secure;
- Providing tools and resources to verify the authenticity of a vendor's certificate;
- Providing staff training resources, checklists, education tools and resources and best practices to support SMEs in their efforts to become and remain certified;
- Offering some sort of support to businesses who "get hacked" even though they are certified;
- Being more proactive in going after hackers and other cyber-criminals;
- Educating all Canadians about how to be more cyber secure.

Methodology

The research methodology consisted of 10 traditional, in-facility focus groups, 6 tele-web focus groups, and, 5 tele-web depth interviews (TDIs). Five in-facility focus groups were conducted with consumers, 18 years of age or older, representing a mix of gender, education and household income. All other sessions and interviews were with small and medium-sized business decision makers who play an important role in the day-to-day operations and direction of the company who would also be familiar with the company's IT systems and data management practices.

These sessions spanned the country in large and medium cities (Calgary, Alta., Victoria, B.C., Halifax, N.S., Kitchener, Ont., and Montreal, Que.), as well as a variety of rural and remote areas across Canada. The focus groups were conducted between March 18 and March 28, 2019 while the tele-depth interviews were conducted between March 25 and April 2, 2019. Each focus group lasted 90 minutes while the interviews lasted 45 minutes. All focus groups were moderated by Rick Nadeau and Eva Gastelum, two of Quorus' senior researchers on the Government of Canada Standing Offer.

Qualitative Research Disclaimer

Qualitative research seeks to develop insight and direction rather than quantitatively projectable measures. The purpose is not to generate "statistics" but to hear the full range of opinions on a topic, understand the language participants use, gauge degrees of passion and engagement and to leverage the power of the group to inspire ideas. Participants are encouraged to voice their opinions, irrespective of whether or not that view is shared by others.

Due to the sample size, the special recruitment methods used, and the study objectives themselves, it is clearly understood that the work under discussion is exploratory in nature. The findings are not, nor were they intended to be, projectable to a larger population.

Specifically, it is inappropriate to suggest or to infer that few (or many) real world users would behave in one way simply because few (or many) participants behaved in this way during the sessions. This kind of projection is strictly the prerogative of quantitative research.

Supplier Name: Quorus Consulting Group Inc.
PSPC Contract Number: U1400-198102/001/CY
Contract Award Date: March 5, 2019
Contract value (including HST): $129,006.45
For more information, please contact the Innovation, Science and Economic Development Canada at:
IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca

Detailed Results

Research Purpose and Objectives

Budget 2018 announced a Cyber Certification Program for small and medium-sized businesses (SMEs) as a response to significant cyber security threats facing the business community and its customers. Along with the Standards Council of Canada and the Communications Security Establishment, Innovation, Science and Economic Development Canada (ISED) has begun development of this certification program with the end goal being to raise the cyber security baseline among SMEs. This will ultimately increase consumer confidence in the digital economy, promoting international standardizations and better position Canadian SMEs to compete globally.

This research seeks to ensure the successful launch, promotion, engagement and adoption of cyber security certification by Canadian SMEs by providing

- Insights on three creative identifier concepts (visuals and messaging);
- Preferred elements in presented creative concepts;
- Reaction and level of trust in the cyber secure "brand";
- Expectations established by cyber certification;
- Perceptions of the benefits and identification of any barriers to adoption; and
- Overall understanding and credibility of the messages presented (both written and visual).

Once complete, the research will be used to

- Select the identifier and key messages used in the cyber security certification program, identifying changes that should be made to the preferred concept in final production;
- Improve the effectiveness of ISED's communications, marketing and outreach efforts in support of its mandate to help businesses and consumers; and,
- Facilitate SME adoption of the program, ensuring messages used to explain the value-proposition of the ISED certification process to both businesses (reassuring consumers of the businesses concern for customer well-being) and to consumers (assisting them in easily identifying cyber certified businesses where they can shop with peace-of-mind regarding their information protection) are well developed and resonate with each audience.

Ultimately, the objective of this research is to establish a recognizable and credible brand for cyber security in Canada, increase resilience of SME cyber infrastructure against cyber-attacks, and increase the number of SMEs with an effective cyber security posture.

Confidence in SME Cyber Security

To gain an initial understanding of the backdrop against which a certification program will be introduced, cyber security in general was explored with both consumers and with SMEs. A variety of aspects were explored, ranging from how cyber secure they are feeling these days to what role they believe the Government of Canada should play when it comes to supporting Canadian SMEs in this area.

Consumer Perspective

When asked what comes to mind when considering "cyber security," most consumers limit their interpretation to financial transactions. In other words, they are primarily concerned that their debit or credit card information is protected and used ethically, and that the institutions insure a refund should their cards be used without their permission.

Some participants also think about how their personal information is stored and used, but this only tends to come up after transactions have been discussed. "Cyber security" also reminds some of how safe they feel using certain vendor websites. A few are also reminded of identity theft in general.

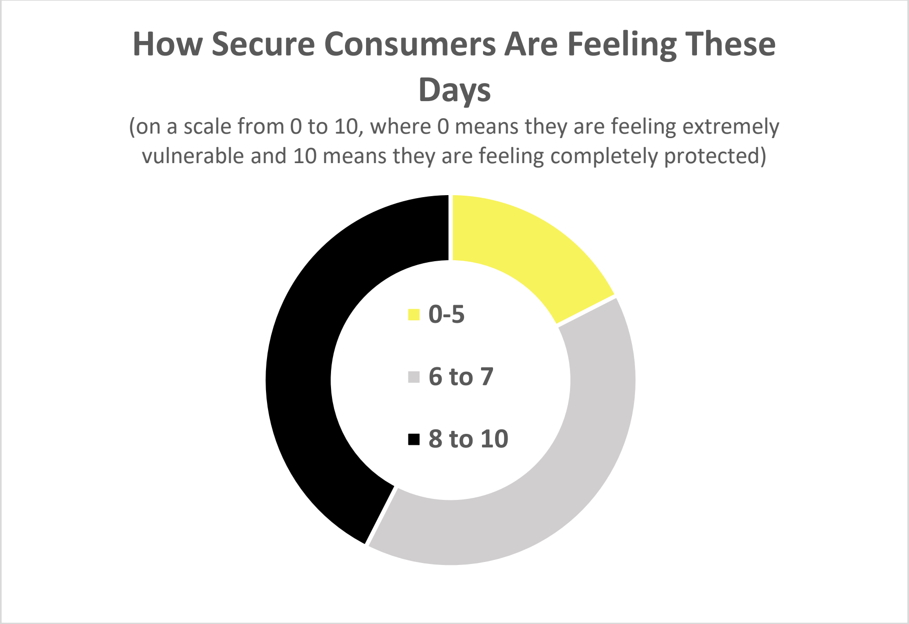
The term cyber security also triggered mentions of "hackers", viruses and firewalls and how their personal and financial information is (or is not) protected against fraudulent or illegal use. In this context, many seemed to focus on unauthorized access to this information through the consumer's technology (e.g. their cell phone, their computer) rather than through the SME's systems.

To make sure all participants were working from the same definitions, the moderator provided a short explanation of what a "SME" is and how "cyber security" should be interpreted for the rest of the session:

- Just so we are all on the same page, Statistics Canada defines a micro business as having 5 or fewer employees, a small business as having roughly 99 or fewer full-time employees and a medium business as having between 100 and roughly 500 employees.
- We are broadly referring to how secure you feel when purchasing something from / dealing with small to medium sized businesses in Canada - this includes how they secure their computers, their Internet and Wi-Fi network, the systems they have in place to store and protect company data, including any information they may be storing about customers, suppliers, staff, etc.

Cyber security is important to consumers and, while not unanimous, most consumers are feeling confident from a cyber security standpoint when dealing with Canadian SMEs. When asked to rate how protected they feel when dealing with SMEs in Canada these days, many would rate themselves at least an 8 out of 10 with a small group rating their confidence 5 or lower (where 10 means they are feeling completely protected).

- Consumers do feel more vulnerable dealing with or purchasing from a SME online than they do in a traditional brick-and-mortar setting.



How Secure Consumers Are Feeling These Days

(on a scale from 0 to 10, where 0 means they are feeling extremely vulnerable and 10 means they are feeling completely protected)

*While based on actual participant responses, this data is not statistically meaningful and should be considered directional in nature.

Those with lower scores have either been directly affected by fraudulent activity in the past, have read of what others have gone through or are generally skeptical of anything connected to the Internet:

> *"There have been problems but the bank was there to help – but because of a problem that's why I did not give a perfect score."*
>
> *"You see on the news sometimes – gas stations taking credit card numbers."*

Consumers explained that their relatively high levels of confidence are related to the fact that they always tend to deal with the same companies and that they have not had any issues in the past. They also explained that they give businesses the benefit of the doubt and they believe SMEs take cyber security seriously because it is in their best interest to do so if they want to stay in business. As one participant summarized: *"it's not only expected but assumed."*

Consumers see limited risk if in fact they happen to deal with a SME that is compromised or unethical since *"all they have is my credit card number."* They further explain that the transactions are typically small and that they have a variety of recourses to get reimbursed (e.g., by calling the card issuer) if they were victims of an unauthorized use of their credit card: *"Any time I've had an issue, I contact the credit card company or PayPal and they fix it."*

Many consumers are also in some ways reassured because they believe that SMEs are not typically targeted by hackers. They believe that hackers are more likely to target larger companies where the payoff is much larger.

Ultimately consumers confide that they do not have many, if any specific way of knowing if the SMEs they deal with are in fact cyber secure. Most admit that they just "trust" that these companies are in fact cyber secure for all the reasons described above.

> *"There is a large range of variables when it comes to cyber security – you could have a company that has invested nothing in security, and a company that invests millions and you don't know who is investing."*

That being said, not all consumers are flying blind when it comes to cyber security:

- Some participants are aware that websites featuring "a small green lock" are secure when making online purchases. Many were also aware of higher security when using https websites.

- Consumers also seek out SMEs and SME websites backed by banks or institutions such as PayPal. They rely a lot on the type of payment system vendors use to signal how secure they should feel. For instance, many explained that if vendors are using systems like PayPal, verified by Visa, Interac, and credit card Point of Sale (POS) machines, their transaction data is considered secure because these large third-party vendors are, themselves, established, secure, and recognized. They also believe that should anything go wrong, these vendors will serve as their safety net and reimburse them.

  It is worth noting that consumers were unaware of any costs passed on to them or to the vendors by the banks or PayPal for POS protection. This makes them more sensitive to any suggestion that a new cyber certification program or requirement might increase costs to SMEs.

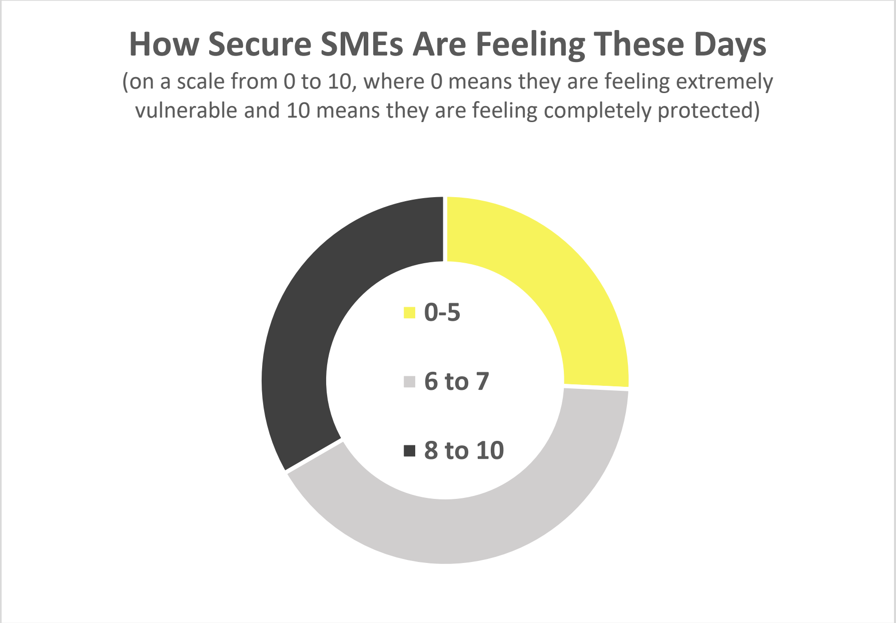
When asked what SMEs could or should do to make them feel more cyber secure, consumers did not have much in the way of solutions. A few did mention having some sort of certification but otherwise participants either did not feel much was needed in the first place (since they are already feeling fairly secure as it is) or they did not know what could be done. Even if SMEs were to better communicate their level of cyber security, consumers generally accept that it is impossible to be completely cyber secure.

SME Perspective

To start the discussion with SMEs, participants were provided the same sort of explanation of cyber security as consumers:

- I am broadly referring to how secure you feel your overall IT system is these days – this includes your computers, your Internet and Wi-Fi network, the systems you have in place to store and protect company data, including any information you may be storing about your customers, your suppliers, your staff, etc.

From their standpoint, SMEs are more concerned about their own level of cyber security. When asked to rate how they feel about their level of cyber security these days, the most common ground is a score of 6 or 7, with nearly as many rating themselves 5 or lower as there are rating themselves at least an 8 out of 10 (where 10 means they are feeling completely protected).



*While based on actual participant responses, this data is not statistically meaningful and should be considered directional in nature.

Businesses explain it is a challenge for them to stay on top of everything related to their IT system and technology in general. Very few participants had staff dedicated to their IT systems and an important struggle for many is fitting the oversight of these systems in with other aspects of running or managing a small business. Other common challenges related to cyber security included:

- Not being able to afford the best software and infrastructure, and even if that were possible, some feel that may not even be enough given how larger companies and even government are getting hacked:

"Our hard drive has died several times and we have lost important information, so we thought of a cloud service, but you hear about a lot of stories with hackers and cloud services – so not sure what to do now."

"Take some precaution, as much as you can, but you are vulnerable. You might just have to accept it. Small businesses don't have the money."

- Not knowing what it means to be completely cyber secure – in other words, many businesses confess to not knowing what they don't know in this area: *"You can feel secure but you'll never know for sure."*

- Remaining informed of the various threats to their system since cyber security seems to be a constantly moving and evolving target: *"You can't be consistently on top of it on a daily basis."*

When considering how secure they feel about their level of cyber security, most SMEs seemed to focus primarily, if not exclusively on data they may be collecting from their clients and less on any of their own internal corporate data (including data on their staff, financial data, and proprietary data), and supplier-related data.

SMEs that are generally <u>the most</u> confident about their level of cyber security (in other words, they are not feeling particularly vulnerable these days) tend to fall into one of four broad categories:

1. Some of the "larger" small companies, and especially medium-sized ones, are more likely to have built up internal expertise, practices, and infrastructure to adequately address cyber security. This would include having staff specifically dedicated to information technology (IT), some of whom actually participated in one of the research sessions. From a process perspective, these businesses would explain that they have formal written procedures pertaining to cyber security, including staff training protocols.

2. Their business has expertise in cyber security or in IT, for instance, they are an IT consulting company, they design websites, etc. These businesses were quite vocal

about how vulnerable other businesses are since they see it every day. As for their own business, they absolutely need to be cyber secure since their entire business model relies on it. That being said, they do not necessarily have anything to prove to clients how cyber secure they are – their reputation is one signal to clients, but many also explain how their clients simply assume that a company operating in the IT space is knowledgeable about cyber security.

3. They believe they do not capture enough data, or the type of data, that would warrant a significant investment in cyber security. For instance, many retail-based businesses will argue that they only collect transaction data and use a large third-party vendor.

4. A few businesses argue that they don't capture any data on their clients or that none of the data is stored on computers. For instance, a few businesses explained that they are "paper only" (or mostly paper) and feel this data cannot be hacked.

Those moderately confident about their level of cyber security explain that they are generally aware of the risks and do basic things like regular backups, they keep an eye out for risky emails, they keep their anti-virus and firewall software updated, they instruct staff to avoid questionable emails, and they use reputable cloud services for file storage and backups (e.g. Dropbox). In spite of these measures, they still believe they could be doing better and that if a professional hacker were to target them, they would probably be in trouble.

Irrespective of where they would position themselves on the "cyber secure" spectrum, all SMEs accept that total security is unrealistic. They figure that if hackers can get into large companies, then they can get into theirs. Furthermore, some argue that once you think you are completely cyber secure, that is when you let your guard down and become vulnerable.

Many SMEs *believe* their customers care about how cyber secure they are but they have never been asked about it. Many SMEs explain that their customers probably just assume they are cyber secure until there is evidence to suggest otherwise:

"It's not a part of the conversation but it would be an issue if something happened."

For some it is part of the conversation and that this largely depends on the nature of the business they are in and the amount and type of data that they have about the customer – there are sometimes requests to see the company privacy policy while others do look for who the payment processors are or for certain reassurances on their website:

"I think most people look for a lock on their browser, and as long as that is there, they feel comfortable."

When asked if cyber security is important in their choice of suppliers, businesses seemed split on the issue. Some argued that their suppliers do not have much information on them, while others explained that they have been doing business with their suppliers for many years and they implicitly trust them. Others felt it might be reassuring knowing that their suppliers are cyber secure. Most agree that if they were evaluating two different suppliers for a given service or contract and that one could demonstrate cyber security and that another could not, that factor would weigh in the balance.

SMEs were also split on whether they are missing out on business opportunities because they cannot "prove" their level of cyber security. On the one hand, some SMEs (especially start-ups, professional services, not-for-profits that rely on funders, and businesses with online features) believe they are missing out on business opportunities. A few also feel they could potentially bid on larger projects or become suppliers to larger clients if they could better demonstrate their level of cyber security. Conversely, other businesses, especially traditional brick-and-mortar ones (e.g. small retailers, tradespersons) did not see this as an issue – they don't believe their customers are focusing on this and if they are not being considered, it is for other reasons.

An important number also could not tell if they are missing out on business opportunities because they cannot "prove" their level of cyber security – again, these SMEs explained that this is not part of the conversation with their customers. In the end though, most would probably agree that if an issue were to surface and that they were to become known as unsecure, it would seriously hurt their business.

Role of Government in Supporting SMEs

Most SMEs and consumers believe there is a role for the federal government to play in terms of supporting SMEs become more cyber secure. The most common suggestions involve providing training, guidelines, best practices or checklists that SMEs could use to verify and improve their level of cyber security. Some suggested providing affordable IT software, systems, or advising on the types of systems and software companies should have.

Other suggestions included:

- Introducing some sort of certification (similar to ISO, LEED, and public health restaurant inspections):

“Comparing it to going to a restaurant, especially a no name one–the first thing I look for is their certification from the health department and that they passed all the requirements by the government so maybe something similar for cyber security.” (SME)

“Businesses have to post their level of security so that consumers know and they can choose.” (Consumer)

- Make sure all Canadians are cyber secure, not just SMEs – for instance, government could better educate Canadians about how to detect secure businesses.

- Further regulate IT backbone service providers like ISPs to make sure those systems are secure.

- Provide credits or additional financial support/incentives for SMEs when they invest in cyber security: *“For very small businesses, some education and funding would be good to help people who are less tech savvy – make their business more competitive and safe for their customers.” (SME)*

Support for government involvement was not unanimous, however. Some were opposed to any further regulation on businesses or having federal resources dedicated to an issue that, in their opinion, the private sector should be able to manage on its own. There were also concerns about whether the Government of Canada can be counted on given some of the IT-related challenges it has been facing, leading a few to doubt whether the Government of Canada was a trusted advisor in this area. A few were also concerned about whether they want a government agency that closely connected to their data and a few others were not certain it was practical or realistic to think the Government could oversee the level of cyber security of every SME in the country: *“How do you enforce this with the amount of small businesses out there?” (Consumer)*

- Opposition to government involvement in this area was especially strong in the focus groups in Calgary and in Halifax.

The idea of making a certain level of cyber security a requirement to be able to operate in Canada was met with mixed reactions. Fundamentally, most would seem to agree that SMEs need to provide a minimum level of cyber security and that if it were to become a requirement, it should also come with some sort of support from the Government.

"Would make me as a business owner and a consumer feel a lot more comfortable but would want to know more about how it would be implemented and regulated." (SME)

However, some were concerned about a "one size fits all" approach since some businesses warrant a higher level of cyber security compared to others, largely depending on the quantity and nature of the private information the company collects. Along these same lines, there were concerns among both consumers and SMEs that a cyber security requirement might be unfair to small businesses that either don't have the resources to meet the requirements or might be forced to adhere to requirements that their business does not warrant.

"I would probably have to shut down if this happened because I wouldn't know what I should be doing." (SME)

Those opposed to this sort of requirement, especially SMEs, either did not see it as practical from an enforcement perspective or did not see it as an issue for government. Notable quotes from SME participants included the following:

"There are so many things going on, that this shouldn't be priority."

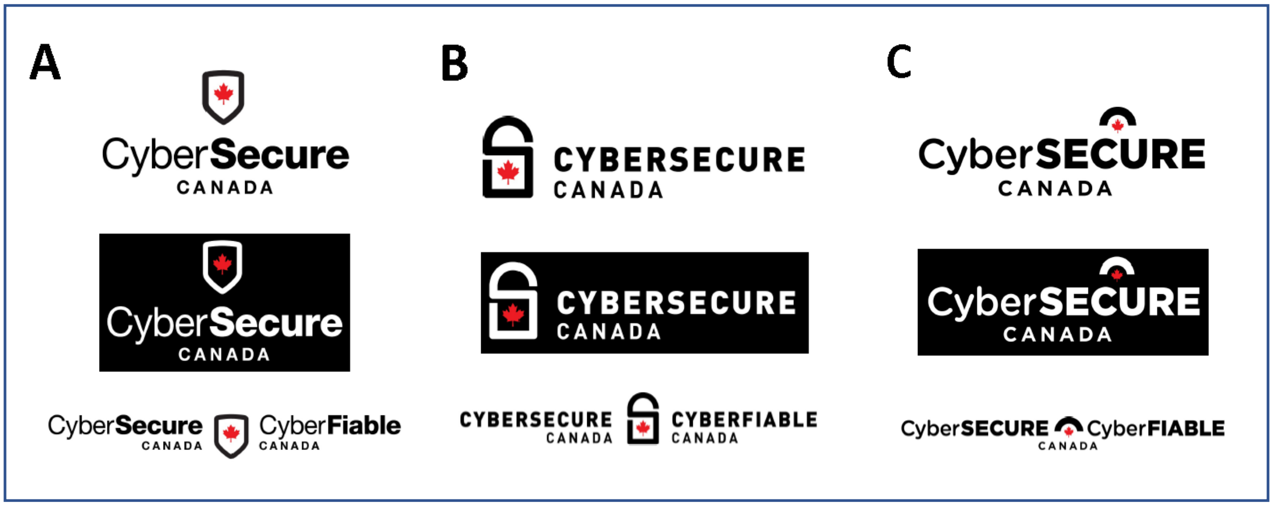
"Should be up to the company – have enough regulations."

"As business owners – we know that there are security levels that we need to have – this is our responsibility not government."

"Make it available but not mandatory."

General Concept Evaluation

The following three concepts were presented to participants one at a time and in a random order from one session to the next to minimize order bias. Concepts were presented in colour on an 8½ by 11 sheet of paper. Before sharing any comments, they were asked to evaluate the concepts on five specific dimensions: unique, memorable, credible, relevant, and, overall appeal (the participant exercise sheet can be found in the appendix). Once all participants had completed their written evaluation of a concept, the concept was discussed and then the process was repeated for the remaining concepts.



Feedback from participants <u>that apply to all three concepts</u> include the following:

- The red maple leaf was a strong Canadian symbol and a strength across all concepts. Any attempts to remove it or change it to a colour other than red were criticized.
- The maple leaf alone was not enough to indicate that the program is endorsed by the Government of Canada or that it is a Government of Canada program. Participants were looking for something more “official” to clearly indicate that this is a Government of Canada initiative (e.g. Federal Identity Program, official wordmark with the maple leaf, or something in words to say the program was backed by the Government of Canada). As it stands, nothing would inform consumers that this is any different from a private sector label:

> *“Would like it to have a Canadian flag rather than just the leaf – then you know it’s Government.” (SME)*

“There needs to be something to make it look like it’s from the Government. It would make it feel more secure.” (SME)

“Normally you can tell when something is Government but this to me does not look like Government. I would be looking for something that is issued by the Government.”

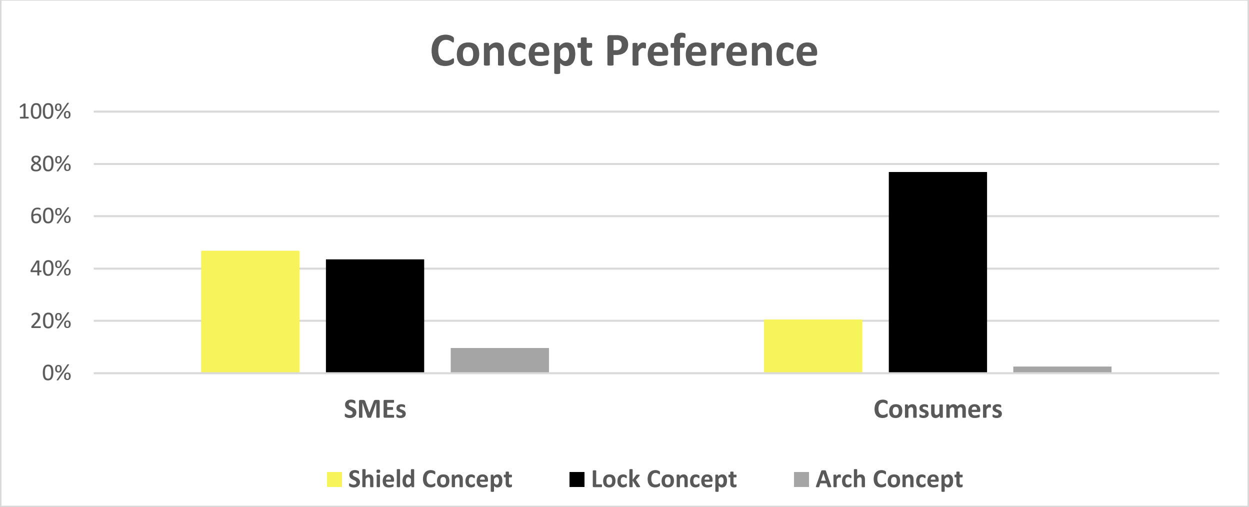
- As much as the concepts were praised for their simplicity, many were worried that the concepts were too simple, even amateurish to some, and that any business could easily replicate and post the identifier without actually holding the certification. Some also felt the concepts looked “cheap.” Along the same lines, participants were looking for some sort of bar code, QR-code, or certificate number that would let the consumer verify the authenticity of the certificate.
- The bilingual concepts were well received – some even liked those more than the unilingual concepts either because they were more visually balanced identifiers or because they were considered more “official” in terms of being a Government of Canada program.
- Francophones clearly liked the language used in the English concept but felt the one in French lacking. In particular, they questioned the use of the word “fiable” – some felt it was not strong or impactful enough while others did not feel it related well to cyber security (“*une personne est fiable, pas un système informatique” (SME))*. Although an appealing alternative was not always found, many did like the use of “sécure” or “sécuritaire” instead of “fiable.” A few also mused that “fiable” is one letter away from reading “faible,” which could be used to ridicule the program if a certified company does not live up to the certification.
- Some would like to see the word “certified” integrated into the concept to convey that it is a certification and not a company logo or a product.

Feedback specific to each concept is summarized in the grid below:

	Strengths	**Weaknesses**
Concept A – Shield	• The imagery was liked by many who felt it effectively communicated “security”, either because they felt it looked like a shield or because it reminded them of what other security-related companies/ products are using. • Many liked the font used.	• While it did convey “security,” it was not considered unique because it is used by other companies, for instance home or private security companies, anti-virus software (McAfee), etc. • For some it reminded them of a badge or a crest that would go on a uniform, which worked for some and less for others.

	Strengths	Weaknesses
	- Some liked that the word Secure was bolded.	- It also reminded some of a car dealership or a vehicle brand, a hockey jersey, or Canadian Tire, which weakened the concept in their eyes since these are not related to security. - From a cohesiveness perspective, the icon seemed detached or disembodied from the text (which is not the case with the other two concepts).
Concept B – Lock	- The concept very clearly conveyed "security" – nearly everyone immediately saw a lock. - A few liked that the "C" from cyber and the "S" from secure were integrated into the design of the lock. - A few knew secure internet sites are https and have a closed lock, therefore they identified the lock as a symbol of cyber security.	- As much as the concept conveyed security, the fact that the lock looked open also suggested "weak security." - Many did not like that only one font style was used for the entire word – they preferred the approach used in the other two concepts.
Concept C – Arch	- The concept's only strength was that a few considered it unique. - Some liked that the word Secure was bolded.	- Most could not figure out the image used – while some liked the concept because it was unique in that way, others did not like it because it did not speak to "security" at all. The image reminded some of the following: an umbrella, a Wi-Fi signal, a rainbow, a bubble, a roof, the sun rising, a "security" blanket, a macaroni, a dome, or an eyebrow/frown, while some could not even think of anything at all. - It also reminded some of the Air Canada logo, the Winnipeg Jets logo, and the logo for the Royal Canadian Air Force. - For a few, especially in Western Canada, it reminded them of a financial services company. - The font was not considered "serious."

Overall, consumers preferred the lock concept by a wide margin whereas SMEs were divided between the shield and the lock concepts. The arch concept came in a distant third for both segments. An even stronger concept for many would be a combination of the image in the lock concept with the font style used in the shield concept.



*While based on actual participant responses, this data is not statistically meaningful and should be considered directional in nature.

Exploring a Program with Tiers

The idea of a tiered system was explored with participants although no details were provided in terms of how it would be structured or how the tiers would be defined. Participant were left to their own interpretation of the tiers.

The tier concept was interpreted two different ways. Some saw the tiers in terms of how cyber secure the SME is – these are seen as **earned tiers**. In this case, a Tier 3 SME is more secure than Tier 2 and Tier 1. Others interpreted the tiers are representing the level of cyber security actually needed by the company based on the quantity and type of data they collect and store – these are seen as **warranted or required tiers**. In this context, a company that only requires basic cyber security (because they don't collect and/or store a lot of data) would be considered a Tier 1 company, whereas a company that stores and collects significant amounts of data or very sensitive data would be Tier 3. Some SMEs even assumed that the higher the tier, the more expensive it would be for them: *"Why are different companies on different levels? Do business owners have to pay to get a higher level?" (SME)*

The tier concept was broadly dismissed by both consumers and SMEs, who far preferred the option whereby a company is either cyber secure or it is not.

The main concerns participants had with a tiered approach included the following:

- Consumers felt it would take enough effort to notice the identifier, let alone the tiers. Besides, even if they noticed it, they believed that it would take a long time before they were sufficiently familiar with the program to know the difference between the tiers. The fact that the entire system can be interpreted in one of two different ways convinced some that there was some risk in using tiers. SMEs also agreed that the tiers will confuse customers.

  "If they are only level one you start wondering – why aren't you level 3?" (Consumer)

  "Would be concerned of what consumers think of less than 3 – as SMEs you research what they mean, consumers won't." (SME)

- SMEs felt that the tiers may not be something they will want to make public-facing, especially if they are anything other than Tier 3. They were concerned that their customers would question their level of cyber security irrespective of what the tiers actually mean. Several said that having anything less than the top level is more likely to create a problem than produce a benefit - rather than proudly promoting that they have achieved a level of cyber security, they expect they would be defending themselves to their customers as to why they are not a Tier 3.
    - That being said, there was some interest in keeping the details of the tiers internal so that managers/owners know where they are and where they need to be in terms of cyber security.

  Some SMEs bluntly stated that if they are "only a Tier 1" then they are not going to advertise it – they believe it shows them as weak in terms of cyber security, which will hurt business, and furthermore it paints a target on their business to attract hackers.

  "If you're a hacker you're going around looking for the place with 1 dot." (SME)

  "I feel as a business owner I would be at a disadvantage if I could only put out a 1." (SME)

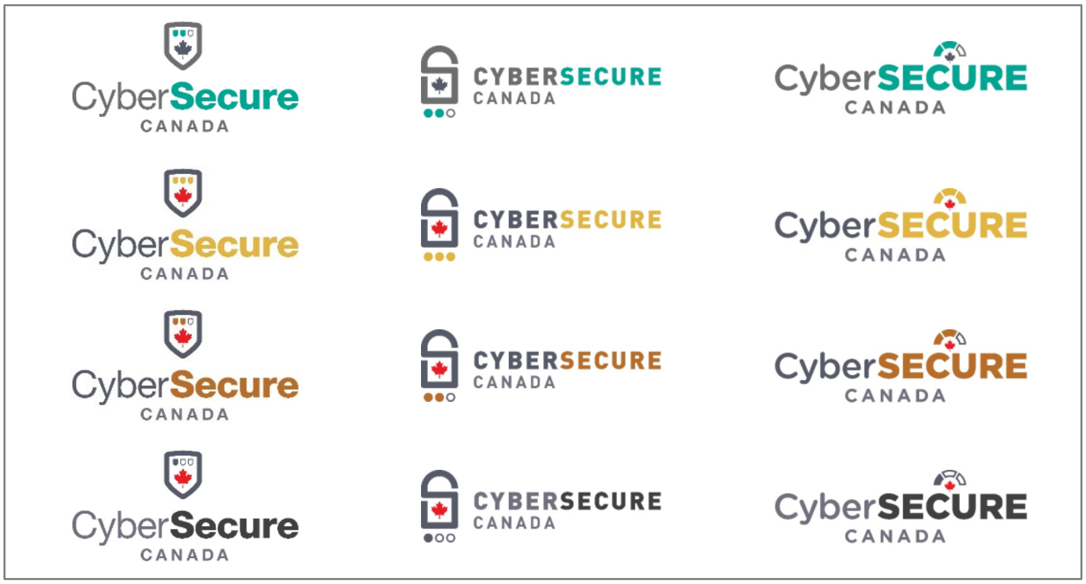
  "Depending on the business you might not need level 3 but now you look bad if you don't get it." (SME)

  "Tier 1 could actually hurt the business rather than help." (SME)

- When considering how the tiers could be communicated to customers through the identifiers, many agreed that integrating the tiers into the visual concepts adds clutter. A few further explained that when these identifiers are in a much smaller format (such as on a business card), the dots will either be hard to notice or weaken the visual appearance of the concept.

Use of Colours in the Visual Concepts

The following colours were explored with participants.



Participants' reactions to the colours proposed were often instant and decisive - few liked any of the proposed colours. If forced to choose, participants would opt for either the status quo (i.e., the black and white concept) or, among the new options proposed, they would select the grey concepts. Other reactions to the colours included:

- "Gold" could work as long as it clearly comes out as gold.

- Some saw the first colour as "green" which has a positive association but then they did not like that the leaf was greyed out.

- The colour red was often spontaneously proposed by participants.

While most simply did not like the colours proposed, some felt adding colour weakened the overall tone or message behind the visual concept. They believe that security needs to be conveyed through a serious or "hard" colour, rather than through the proposed colours, which were seen as either pretty colours or obscure colours. Other than perhaps grey, none of the colours proposed were sufficiently “serious.” Some also felt that adding colour distances the concept in terms of being a Government program. A few also were concerned about how the colours would work with the SMEs branding and colour palette.

“They don’t add anything to the design – maybe the green, but the black and white with the red for the leaf is best.” (SME)

“Black is best because it’s clean and simple.” (SME)

“It’s such a serious thing – don’t add colour, keep it black and white.” (Consumer)

“It takes away from the idea of it being secure – it makes it playful.” (Consumer)

“Don’t like blue/turquoise. Gold and brown are okay but agree to keep it simple with black and white. Makes the leaf stand out more.” (SME)

The only other colour-related feedback pertained to the colour of the maple leaf, which participants all agreed needed to remain red.

Potential Impact on Competitiveness

Consumers are not likely to dramatically change their current shopping patterns based on whether or not a business has been cyber certified, again mostly because they trust the businesses with whom they currently deal. Reactions to more specific scenarios included:

- If given the choice between two vendors who sell the exact same products where one is certified and one that is not (all other things remaining the same including convenience, price, quality, etc.), consumers would lean towards the one that is certified. It is worth noting though that few would be prepared to pay more for that extra peace of mind and a few even noted that they would not drive too much out of their way to go to a certified vendor if an un-certified one is nearby.

- Consumers will not stop using a SME because they are not certified.

SMEs were split in terms of whether or not having the certification would have a positive impact on their business. SMEs interested in the concept of being cyber certified suspected it might become a competitive differentiator; it would be something that customers would notice, and it would help them become better businesses by being more proactive and by being more cyber "aware." Many of these businesses were in some ways struggling to grasp cyber security and appreciated the extent to which cyber security is important to their clients. Those who either believe cyber security is not an issue for their business or is not a factor for their clients were less inclined to believe that being certified would make a difference.

For many SMEs, the impact on their business largely depends on the extent to which their customers will become informed about the program and fully understand what it means for them as consumers and what the SME went through to become certified. Some were also concerned about whether or not consumers would even notice the identifier given that consumers are not looking for that identifier today and given the quantity of other "stickers out there."

- There is some appreciation that recognition of the program among consumers will not happen overnight and that any impact on their business may take time, a sentiment also echoed by some consumers: *"With credit card taps, it used to be something that I didn't trust but now I do. Maybe it'll be something I recognize down the road and realize there isn't one on a store." (Consumer)*

- Those with international sales doubted if the certification would be relevant to their customers located in other countries. There was no awareness of equivalent programs in other countries but there was interest in the idea of having an international standard or program.

- Businesses located in rural and remote areas could see how the program could help given how isolated they are from expertise and resources to help them improve their cyber security. On the other hand, they don't necessarily feel it will make them more competitive since there is very limited competition for similar products and services in rural and remote areas.

<u>Other than on a storefront or a website</u>, participants would expect to see or use the identifier in the following ways:

Consumers would expect to see the identifier…	**SMEs would expect to place the identifier…**
• On packaging • At the cash register/near POS and credit card readers • On "sign-up" forms – for instance, when signing up to a loyalty program • On advertising	• On packaging • On their email signatures • On company letterhead/company stationary • On invoices • In responses to RFPs/on quotes • On business cards

Consumers would expect to see the identifier…	SMEs would expect to place the identifier…
	• At the cash register/near POS and credit card readers • On all marketing material/brochures • On company vehicles • In online advertising • “I would put it everywhere!” • Integrated into online shopping cart – e.g. under the “Add to cart” button • Company Facebook/social media pages

Expectations of the Program

Without much information about what the program will be, participants were asked how they would like the program to work. Participants, especially consumers, struggled somewhat when asked what they believed the program should resemble. SMEs and consumers shared a common view on some of the main elements of the program, which would include the following, some of which speak to the role they see the Government of Canada playing in the program:

- the federal government would provide all certification proponents access to training, guidelines and best practices in the area of cyber security;

- there would need to be some sort of certification audit, with most participants assuming this would be done by an IT expert working for the Government of Canada (rather than being outsourced to a third party); and

- there would need to be regular recertification. While some suggested this recertification could be done every two or three years, most suggested an annual process, especially given the speed at which technology evolves.

There were some expectations specific to consumers and SMEs.

Consumer Perspective

Consumers feel the program should include a significant effort focused on public education. Consumers would want to know certain details such as, but not limited to, what is being certified, how relevant it is to them as consumers, and what the companies had to do in order to become certified. There were some questions about what has led the government to roll out this program – this was especially important to consumers who are already feeling fairly secure in their dealings with SMEs today. For some of these participants, the program was coming across as "a solution looking for a problem." This broader validation of the program would need to be separate from education efforts describing the program itself. Ultimately, consumers just want the details surrounding the program to be public so that they can understand the benefits to them.

> *"What are they trying to accomplish by bringing this in? What are the challenges that the Government is facing that is prompting them to want to roll this out?"*

If the program were to be introduced, many consumers would feel more secure in their dealings with SMEs in general even though many are not actively seeking out cyber security reassurances when they deal with SMEs.

The greatest increase in consumer confidence would come from those who had been through negative experiences in the past or who were most credulous about cyber security in general. Otherwise, consumers appreciate that companies would be going "the extra mile" to keep their customers safe even though they know that, certified or not, there is no expectation that any company can be 100% secure.

Although they may not be more reassured by the program, some consumers could appreciate how the program could benefit Canadian SMEs in general. Throughout the focus groups with consumers, many showed a soft spot for small businesses. If the program is an effort by the Government of Canada to support SMEs become more cyber secure, especially those that otherwise might not be able to do so on their own, then the program was generally seen as "pro-small business."

SME Perspective

SME participants had more specific expectations of the program:

- They wanted to be sure that this was a meaningful program and that certification and recertification did not represent additional paperwork, red tape, or administrative burden.
- The audit could include an *in situ* inspection as well as an external verification (e.g., by having auditors trying to hack the applicant's system).
- They would want the program to be financially accessible to newer and smaller companies. Given this will be a national program, many expected the certification process to be free or very low cost so as to maximize take-up and to make the program

accessible to companies of all shapes and sizes. Many suggested that the cost be revenue and needs-tested so that businesses pay a fee that is relatively affordable to them and calibrated to how important cyber security is to their business.

Some were reluctant to believe that their level of cyber security would increase if they were to become certified, either because they feel it is as good as they can get it or they don't need more. Even if they were to become certified, no one is under the impression that their business will be 100% secure since that is seen as impossible.

If the program were to be rolled out, the lift in confidence among SMEs when it comes to their own level of cyber security would be minimal, with many remaining fairly indifferent towards the program. Many were not convinced they would need to get the certification at all, largely because of the following:

1. Concerns over compliance burden;
2. Unjustified confidence – they believe they are as secure as they need to be, not knowing what they don't know in terms of their own vulnerabilities; and,
3. No appreciation for where they sit in the supply chain.

Admittedly, SMEs had no specific information on the program itself and until they see more details around what the program involves, including costs and the certification process, many were reluctant to commit to how their level of confidence could really change if the program were to be rolled out or whether they would get certified at all.

Many SMEs expected the program to be free, while others expected the cost to be relative to the size of their business. Most who expected a cost associated to the program suggested a low annual fee or the audit to be free but the certification to have a cost. However, most had a hard time suggesting a reasonable fee without more knowledge of the program.

Role of the Government

Participants were asked what role they would expect the Government of Canada to play in relation to the proposed program. The most common roles participants expect the Government of Canada to play included:

- Promoting the program to the general public to ensure they are well informed about what the certification means. Participants would also want to make sure that the burden and cost of promoting the program does not lie on SMEs.
- Establishing the standards of certifications.

- Conducting the audits, the certifications and the recertifications, including ad hoc testing to make sure that certified companies continue to be secure.
- Providing tools and resources for customers to verify the authenticity of a vendor’s certificate.
- Providing staff training resources, checklists, education tools, and resources and best practices to support SMEs in their efforts to become and remain certified.
- Offering some sort of support to businesses who “get hacked” even though they are certified – some felt the Government, as the certifier, would also be a guarantor of sorts if something happens to a certified SME. This, among many other points raised throughout the report, stresses the importance for the Government of Canada to eventually communicate what the program is and what it is not.
- Being more proactive in going after hackers and other cyber-criminals.
- Educating all Canadians about how to become more cyber secure.

Detailed Methodology

The research methodology consisted of 10 traditional, in-facility focus groups, 6 tele-web focus groups, and 5 tele-web depth interviews (TDIs). Most of the research was with small and medium businesses and a sub-set of in-facility focus groups were with consumers. These sessions spanned the country in large and medium cities, as well as in rural and remote areas.

Quorus was responsible for coordinating all aspects of the research project including designing and translating the recruitment screener and the moderation guide, coordinating all aspects of participant recruitment, facilities and related logistics, moderating all sessions and interviews, and delivering required reports at the end of data collection.

The target population for this research consisted of Canadian small and medium-sized enterprises (SME) and consumers. More specifically, the research targeted a mix of the following types of businesses and consumers:

- **Target population 1 – entrepreneurs, business owners, and managers:** This is a group consisting of Canadian entrepreneurs, business owners, and managers of small and medium businesses. Within the SME segment, the research targeted the company's main decision-maker or someone who plays an important role in the day-to-day operations and direction of the company.
- **Target population 2 – consumers:** This is a group consisting of consumers within the general population, 18 years of age and older.

For the purposes of this research, small businesses were defined as those businesses with fewer than 100 employees (including self-employed Canadians), and medium businesses were those with 100 to 499 employees. Within the small business segment, the research also targeted "micro" businesses, which were defined as businesses with five or fewer employees.

Across the small and medium sized business segment, the research also targeted a mix of the following sub-segments:

- **Youth entrepreneurs** are individuals who started and operate their own company and who are 20 to 34 years old.
- **Women entrepreneurs** are women who started and operate their own company.
- **Indigenous entrepreneurs** are individuals who self-identify as a member of a First Nations, Métis, or Inuk (Inuit) community and who started and operate their own company.
- **Entrepreneurs with disabilities** are individuals who self-identify as having a physical or mental disability and who started and operate their own company.

- **Entrepreneurs who have recently immigrated to Canada** are individuals who have immigrated to Canada within the past 10 years and who started and operate their own company in Canada.

There was also a good mix of business lines recruited, including retail, e-commerce businesses, service, IT, manufacturing businesses, businesses serving businesses (B2B), and companies doing business internationally.

Participants invited to participate in the focus groups and depth interviews were recruited through a combination of random contacts by telephone and through the use of a proprietary database. Participants in the "consumers" groups were randomly recruited by telephone from the general public.

In the design of the recruitment screener, specific questions were inserted to clearly identify whether participants qualify for the research program and, where applicable, to ensure a good representation as follows:

- **SME** representatives participating in this research represented a good mix of ages, business stage/experience, as well as a good mix in terms of awareness of the security and privacy issues that digital technologies represent in a business context. All business participants were senior decision-makers in their organization who play an important role in the day-to-day operations and direction of the company who would also be familiar with the company's IT systems and data management practices.
- **Consumers** participating in this research represented a good mix in terms of age, region, gender, education, and household income.

In addition to the general participant profiling criteria noted above, additional screening was done to ensure quality respondents, such as:

- No participant (nor anyone in their immediate family or household) was recruited who worked in related government departments/agencies, nor in advertising, marketing research, public relations, or the media (radio, television, newspaper, film/video production, etc.).
- No participant acquainted with another participant was knowingly recruited for the same study, unless they were recruited into separately scheduled sessions.
- No participant was recruited who had attended a qualitative research session within the past six months.
- No participant was recruited who had attended five or more qualitative research sessions in the past five years.

- No participant was recruited who had attended a qualitative research session on the same general topic as defined by the Researcher/Moderator in the past two years.

Data collection consisted of in person focus groups and tele-web interviews, each lasting 1.5 hours, and tele-web depth interviews (TDIs), each lasting 45 minutes. For each in person focus group, Quorus recruited 10 participants to achieve 8 to 10 participants per focus group. For each tele-web focus group, Quorus recruited 7 participants to achieve 5 to 7 participants per focus group.

The recruitment of focus group and telephone depth interview participants followed the screening, recruiting and privacy considerations as set out in the *Standards for the Conduct of Government of Canada Public Opinion Research–Qualitative Research.* Furthermore, recruitment respected the following requirements:

- All recruitment was conducted in the participant's official language of choice, English and French, as appropriate.

- Upon request, participants were informed on how they can access the research findings.

- Upon request, participants were provided Quorus' privacy policy.

- Recruitment confirmed each participant had the ability to speak, understand, read and write in the language in which the session was to be conducted.

- Participants were informed of their rights under the *Privacy* and *Access to Information Acts* and ensure that those rights were protected throughout the research process. This included: informing participants of the purpose of the research, identifying both the sponsoring department or agency and research supplier, informing participants that the study will be made available to the public in 6 months after field completion through Library and Archives Canada, and informing participants that their participation in the study is voluntary and the information provided will be administered according to the requirements of the *Privacy Act*.

At the recruitment stage and at the beginning of each focus group/depth interview, participants were informed that the research was for the Government of Canada/ISED. Participants were informed of the recording of their session in addition to the presence of ISED observers/ listeners. Quorus ensured that prior consent was obtained at the recruitment stage and before participants entered the focus group room or began their telephone session. Written participants' consent was developed by Quorus and approved by ISED and was obtained from each in-facility focus group participant prior to any recording.

All focus groups were held in the evenings in focus group facilities that allowed the client team to observe the sessions. Recruited participants were offered a different honorarium depending on the segment.

A total of 10 in-person focus groups were conducted across Canada as per the table below.

Location	Segment	Language	Number of participants	Date and Time	Honorarium
Calgary, Alta.	Consumers	English	8	March 18 @ 5:30 pm	$75
Calgary, Alta.	SMEs	English	8	March 18 @ 7:30 pm	$150
Victoria, B.C.	Consumers	English	8	March 19 @ 5:30 pm	$75
Victoria, B.C.	SMEs	English	6	March 19 @ 7:30 pm	$150
Halifax, N.S.	Consumers	English	9	March 21 @ 5:30 pm	$75
Halifax, N.S.	SMEs	English	8	March 21 @ 7:30 pm	$150
Kitchener, Ont.	Consumers	English	6	March 26 @ 5:30 pm	$75
Kitchener, Ont.	SMEs	English	8	March 26 @ 7:30 pm	$150
Montreal, Que.	Consumers	French	9	March 28 @ 5:30 pm	$75
Montreal, Que.	SMEs	French	8	March 28 @ 7:30 pm	$150

A total of six tele-web focus groups were conducted using a tele-web service ("Zoom"), allowing the moderator to share visual concepts with participants and to enable members of the client team to remotely observe the sessions, and to enable a recording of the session. Each session was audio and video recorded (the moderator's screen was recorded – participants did not use their web cameras). All groups consisted of SMEs, as described below.

Segment	Language	Number of participants	Date and Time	Honorarium
Ontario – Rural/Remote	English	3	March 20 @ 5:30 pm EST	$150
Women Entrepreneurs	English	3	March 25 @ 5:30 pm EST	$150
Youth Entrepreneurs	English	2	March 25 @ 7:30 pm EST	$150
Quebec – Rural/Remote	French	7	March 27 @ 6:00 pm EST	$150
Prairies – Rural/Remote	English	5	March 27 @ 8:00 pm EST	$150
Women and Youth Entrepreneurs	English	5	March 28 @ 5:30 pm EST	$150

Finally, a total of five tele-web interviews (four in English and one in French) were conducted with entrepreneurs with disabilities from March 25 to April 2, 2019. All tele-web depth interviews were conducted during regular business hours and during evenings (whatever suited the respondent's availability and preferences) using a tele-web service ("Zoom") allowing the moderator to share visual concepts with participants and to enable members of the client team to listen in. Each session was audio and video recorded (the moderator's screen was recorded – participants did not use their web cameras). All participants were given an honorarium of $150.

Appendices

Recruitment Screener – Consumers (English)

Consumer Recruitment Screener

[NOTE: Recruitment screener for SMB segment is available separately.]

In-Facility Focus Groups:			**Details:**
Calgary: March 18, 2019 - ENGLISH			recruit 10 for 8 to 10 to show 90 minute sessions
Group 1: Consumers	**5:30 pm**	**$ 75**	
Group 2: SMBs	7:30 pm	$ 150	
Victoria: March 19, 2019 - ENGLISH			
Group 3: Consumers	**5:30 pm**	**$ 75**	
Group 4: SMBs	7:30 pm	$ 150	
Halifax: March 21, 2019 - ENGLISH			
Group 5: Consumers	**5:30 pm**	**$ 75**	
Group 6: SMBs	7:30 pm	$ 150	
Kitchener-Waterloo: March 26, 2019 - ENGLISH			
Group 7: Consumers	**5:30 pm**	**$ 75**	
Group 8: SMBs	7:30 pm	$ 150	
Montreal: March 28, 2019 - FRENCH			
Group 9: Consumers	**5:30 pm**	**$ 75**	
Group 10: SMBs	7:30 pm	$ 150	

A. Facility Information

Calgary Facility Address	Victoria Facility Address
Qualitative Coordination Suite 120, 707 10th Avenue SW	RA Malatest 858 Pandora Avenue
Halifax Facility Address	**Kitchener-Waterloo Facility Address**
Corporate Research Assoc. 7071 Bayers Road, Suite 5001 (5th floor)	Metroline Research Group Inc. 301-7 Duke Street West
Montreal Facility Address	
CRC 1610 Saint-Catherine St W., office 411	

Hello/Bonjour, my name is _____. Would you prefer to continue in English or French? / Préférez-vous continuer en anglais ou en français?

[INTERVIEWER NOTE: FOR ENGLISH GROUPS, IF PARTICIPANT WOULD PREFER TO CONTINUE IN FRENCH, PLEASE RESPOND WITH, "Malheureusement, nous recherchons des gens qui parlent anglais pour participer à ces groupes de discussion. Nous vous remercions de votre intérêt." FOR FRENCH GROUP, IF PARTICIPANT WOULD PREFER TO CONTINUE IN ENGLISH, PLEASE RESPOND WITH, "Unfortunately, we are looking for people who speak French to participate in this discussion group. We thank you for your interest."]

I'm calling from Quorus Consulting Group, a national public opinion research firm. We're organizing a series of discussion groups on behalf of the Government of Canada to discuss new programs and initiatives that are being considered.

Participation is voluntary. No attempt will be made to sell you anything or change your point of view. The format is a "round table" discussion lead by a research professional. All opinions expressed will remain anonymous, views will be grouped together to ensure no particular individual can be identified and the research will be conducted in accordance with laws designed to protect your privacy.

[INTERVIEWER NOTE: IF ASKED ABOUT PRIVACY LAWS, SAY: "The information collected through the research is subject to the provisions of the Privacy Act, legislation of the Government of Canada, and to the provisions of relevant provincial privacy legislation."]

About ten people like you will be taking part, all of them randomly recruited just like you. For their time, participants will receive an honorarium of $75.00. But before we invite you to attend, we need to ask you a few questions to ensure that we get a good mix and variety of people. May I ask you a few questions?

Yes	**CONTINUE**
No	**THANK AND TERMINATE**

1. Do you or any member of your household or immediate family, work in any of the following fields? **READ LIST:**

	YES	NO
Market Research or Marketing	1	2
Public Relations or Media (TV, Print)	1	2
Advertising and communications	1	2
A political party	1	2
A federal or provincial government department or agency	1	2

IF "YES" TO ANY OF THE ABOVE, THANK AND TERMINATE

2. Could you please tell me what age category you fall in to? Are you...

Under 18	0	**THANK AND TERMINATE**
18-24 years	1	**ENSURE GOOD MIX PER GROUP**
25-34 years	2	
35-44 years	3	
45-54 years	4	
55-64 years	5	
65-74 years	6	
75 years or older	7	
Refuse	9	**THANK AND TERMINATE**

3. Could you please tell me what is the highest level of education that you have completed?

Some high school	1	**ENSURE GOOD MIX PER GROUP**
Completed high school	2	
Some College/University	3	
Completed College/University	4	
RF/DK	9	

4. What is your current employment status?

Working full-time	1	
Working part-time	2	
Self-employed	3	
Retired	4	
Currently not working	5	**MAX 2 PER GROUP**
Student	6	
Other	7	
DK/RF	9	

5. **[IF EMPLOYED/RETIRED]** What is/was your current/past occupation?

___________________________ **(PLEASE SPECIFY)**

6. Which of the following categories best describes your total household income? That is, the total income of all persons in your household combined, before taxes **[READ LIST]**?

Under $20,000	1	**ENSURE GOOD MIX PER GROUP**
$20,000 to just under $ 40,000	2	
$40,000 to just under $ 60,000	3	
$60,000 to just under $ 80,000	4	
$80,000 to just under $100,000	5	
$100,000 to just under $150,000	6	
$150,000 and above	7	
DK/RF	99	

7. In a typical month, how often do you do any of the following activities: **REPEAT SCALE AS NEEDED**

a) Online shopping from your home computer, tablet or your cell phone
b) Online banking from your home computer, tablet or your cell phone
c) Use social media on your home computer, tablet or your cell phone (**IF NEEDED**: such as Facebook, Instagram, Twitter, Snapchat, or Whatsapp)
d) Use a credit card when making purchases in-person
e) Collect or use loyalty program points when shopping

Often	1	**AIM FOR A MIX OF USERS**
Sometimes	2	
Rarely	3	
Never	4	

8. How do you identify yourself? *DO NOT READ: Gender – Refers to current gender which may be different from sex assigned at birth (male or female) and may be different from what is indicated on legal documents.*

Male gender	1	**AIM FOR A MIX**
Female gender	2	
Gender diverse	3	
Prefer not to answer	4	

9. Are you an Indigenous person, that is, First Nations, Métis or Inuk (Inuit)? First Nations includes Status and Non–Status Indians.

Yes	1
No	2

10. If you won a million dollars what would be the first two things you would do with the money? (**MUST HAVE TWO RESPONSES TO ACCEPT. TERMINATE IF FLIPPANT, COMBATIVE OR EXHIBITS DIFFICULTY IN RESPONDING)**

11. Have you ever attended a group discussion or an interview which was arranged in advance and for which you received a sum of money for your participation?

Yes	1	**MAX. 5 PER GROUP**
No	2	**GO TO INVITATION**

12. How long ago was it? _______________________

TERMINATE IF IN THE PAST 6 MONTHS

13. How many consumer discussion groups have you attended in the past 5 years?

____

Fewer than 5	
5 or more	**TERMINATE**

14. Sometimes participants are also asked to write out their answers on a questionnaire or look at printed material. Is there any reason why you could not participate? If you require reading glasses, please remember to bring them with you, as you may be required to read some materials during the session.

Yes	**TERMINATE**
No	

TERMINATE IF RESPONDENT OFFERS ANY REASON SUCH AS SIGHT OR HEARING PROBLEM, A WRITTEN OR VERBAL LANGUAGE PROBLEM, A CONCERN WITH NOT BEING ABLE TO COMMUNICATE EFFECTIVELY OR IF YOU HAVE ANY OTHER CONCERN.

Invitation

I would like to invite you to participate in the focus group in your city. The discussion will be led by a researcher from a Canadian public opinion research company, Quorus Consulting. The group will take place on **[DAY OF WEEK]**, **[DATE]**, at **[TIME]**. It will last one and a half hours (90 minutes). People who attend will receive $75 to thank them for their time. This will be provided to you at the facility after the session.
Would you be willing to attend?

○ Yes	
○ No	**TERMINATE**

The session will be audio and video recorded for research purposes and representatives of the Government of Canada research team will be observing from an adjoining room. You will be asked to sign a waiver to acknowledge that you will be video recorded during the session. The recordings will be used only by the Quorus Consulting research team and will not be shared with others. As I mentioned, all information collected in the group discussion will remain anonymous and be used for research purposes only in accordance with laws designed to protect your privacy.

The focus group will be at the following location: **REFER TO PAGE 1**

We ask that you arrive fifteen minutes early to be sure you find parking, locate the facility and have time to check-in with the hosts. The hosts may be checking respondent's identification prior to the group, so please be sure to bring some personal identification with a photo with you (i.e. driver's license).

As we are only inviting a small number of people, your participation is very important to us. If for some reason you are unable to attend, please call so that we may get someone to replace you – you cannot send your own replacement if you cannot attend. You can reach us at **1-800-XXX-XXXX** at our office. Please ask for **[recruiter to provide]**. Someone will call you the day before to remind you about the discussion.

So that we can call you to remind you about the focus group or contact you should there be any changes, can you please confirm your name and contact information for me?

First name: ______________________________

Last Name: ______________________________

Daytime phone number: ______________________________

Evening phone number: ______________________________

Thank you very much for your help!

Recruitment Screener – SMEs (English)

SMB Recruitment Screener

[NOTE: Recruitment screener for consumer segment is available separately.]

In-Facility Focus Groups: **Calgary: March 18, 2019 - ENGLISH** Group 1: Consumers 5:30 pm $ 75 **Group 2: SMBs 7:30 pm $ 150** **Victoria: March 19, 2019 - ENGLISH** Group 3: Consumers 5:30 pm $ 75 **Group 4: SMBs 7:30 pm $ 150** **Halifax: March 21, 2019 - ENGLISH** Group 5: Consumers 5:30 pm $ 75 **Group 6: SMBs 7:30 pm $ 150** **Kitchener-Waterloo: March 26, 2019 - ENGLISH** Group 7: Consumers 5:30 pm $ 75 **Group 8: SMBs 7:30 pm $ 150** **Montreal: March 28, 2019 - FRENCH** Group 9: Consumers 5:30 pm $ 75 **Group 10: SMBs 7:30 pm $ 150**	**Details:** recruit 10 for 8 to 10 to show 90 minute sessions
Tele-Web Focus Groups: **Rural and Remote - Ontario: March 20, 2019 - ENGLISH** **Group 11: SMBs 5:30 pm $ 150** **Women Entrepreneurs (Pan-Canada): March 25, 2019 - ENGLISH** **Group 12: SMBs 5:30 pm $ 150** **Young Entrepreneurs (Pan-Canada): March 25, 2019 - ENGLISH** **Group 13: SMBs 7:30 pm $ 150** **Rural and Remote - Quebec: March 27, 2019 - FRENCH** **Group 14: SMBs 6:00 pm $ 150** **Rural and Remote – Prairies/West: March 27, 2019 - ENGLISH** **Group 15: SMBs 8:00 pm $ 150** **Women and Youth Entrepreneurs (Pan-Canada): March 28, 2019 - ENGLISH** **Group 16: SMBs 5:30 pm $ 150**	**Details:** recruit 7 for 5 to 7 to show Incentive: $150 90 minute sessions

Tele-Web Depth Interviews: - **5 entrepreneurs with disabilities (Pan-Canada)**	**Details:** mix of English and French Incentive: $100 45 minute sessions

A. Segment Definitions

Segment	Definition
Micro Business and Small-Size Business	1 to 99 FTE employees
Medium-Size Business	100 to 499 FTE employees
Women Entrepreneurs	Women who started and operate their own company
Youth Entrepreneurs	Individuals who are currently 18 to 34 years old who started and operate their own company
Indigenous Entrepreneurs/ Business operators	Individuals who self-identify as a member of a First Nations, Métis or Inuk (Inuit) community and who started and/or operate their own company. Some of these will be located "North of 60."
Entrepreneurs/Business operators with a disability	Individuals who self-identify as living with a physical or mental disability and who started and/or operate their own company
Rural and Remote Entrepreneurs/Business operators	Entrepreneurs/ business operators whose business is located in a town, village or rural area with a population of less than 10,000 and is at least a two-hour drive from a city of at least 50,000
Entrepreneurs who have recently immigrated to Canada	Entrepreneurs/ business operators who have immigrated to Canada within the past 10 years and who started and operate their own company in Canada.

All SMB groups and interviews will be a mix of Canadian entrepreneurs, business owners and managers of small and medium businesses. The research will target the company's main decision-maker or someone who plays an important role in the day-to-day operations and direction of the company and who is familiar with the company's data security and storage.

Except for Groups 12, 13 and 16 and for the tele-web interviews (which are dedicated to specific sub-groups of SMBs), recruitment efforts will also target representatives from the following segments:

- Women entrepreneurs;
- Young entrepreneurs (under 35 years of age);
- Indigenous entrepreneurs; and
- Underrepresented groups (including, but not limited to those identifying as entrepreneurs living with a disability, and entrepreneurs who have recently immigrated to Canada).

Recruitment efforts across all SMB groups and interviews will also target a mix of business lines, including retail, e-commerce businesses, service, IT, manufacturing businesses, businesses serving businesses (B2B), and companies doing business internationally.

B. Facility Information

Calgary Facility Address	**Victoria Facility Address**
Qualitative Coordination Suite 120, 707 10th Avenue SW	RA Malatest 858 Pandora Avenue
Halifax Facility Address	**Kitchener-Waterloo Facility Address**
Corporate Research Assoc. 7071 Bayers Road, Suite 5001 (5th floor)	Metroline Research Group Inc. 301-7 Duke Street West
Montreal Facility Address	
CRC 1610 Saint-Catherine St W., office 411	

C. Introduction

Hello, my name ________________. I'm calling from Quorus Consulting, a Canadian public opinion research company and we are calling on behalf of the Government of Canada.

Would you prefer to continue in English or French? / Préférez-vous continuer en anglais ou en français?

[INTERVIEWER NOTE: FOR ENGLISH GROUPS/INTERVIEWS, IF PARTICIPANT WOULD PREFER TO CONTINUE IN FRENCH, PLEASE RESPOND WITH, "Malheureusement, nous recherchons des gens qui parlent anglais pour participer à cette recherche. Nous vous remercions de votre intérêt." FOR FRENCH GROUPS/INTERVIEWS, IF PARTICIPANT WOULD PREFER TO CONTINUE IN ENGLISH, PLEASE RESPOND WITH, "Unfortunately, we are looking for people who speak French to participate in this research. We thank you for your interest."]

From time to time, we solicit opinions by sitting down and talking with people. We are preparing to conduct a series of these discussions on behalf of the Government of Canada and I would like to speak to the individual in your organization who plays an important role in the day-to-day operations and direction of the company who would also be familiar with the company's IT systems and data management practices. Is there a person available who fits that description? …this is most likely the owner or President of your company or someone responsible for the company's IT.

ONCE APPROPRIATE CONTACT HAS BEEN REACHED – REPEAT INTRO IF NEEDED AND CONTINUE:

We are reaching out to you today to invite you to a research session to share your feedback on the opportunities and challenges your business faces and the kind of role you expect the Government of Canada to play in relation to these.

Other decision makers from small and medium sized companies located in Canada will be taking part in this research. It is a first-name basis only discussion so nobody, including the Government of Canada, will know the companies being represented. For their time, participants will receive a cash compensation.

Participation is voluntary and all opinions will remain anonymous and will be used for research purposes only in accordance with laws designed to protect your privacy. We are simply interested in hearing your opinions, no attempt will be made to sell you anything. The format may be a "round table" discussion or a telephone interview lead by a research professional.

[INTERVIEWER NOTE: IF ASKED ABOUT PRIVACY LAWS, SAY: "The information collected through the research is subject to the provisions of the *Privacy Act*, legislation of the Government of Canada, and to the provisions of relevant provincial privacy legislation."]

But before we invite you to attend, we need to ask you a few questions to ensure that we get a good mix/variety of businesses. This should only take about 5 minutes. In case you are uncertain, **all my questions pertain to your company's Canadian operations.** May I ask you a few questions?

Yes	1	**CONTINUE**
No	2	**THANK & TERMINATE**

D. Business and Participant Profile

1. How would you rate your own level of familiarity with the security and privacy issues that digital technologies represent in a business context? Would you say you are... **READ OPTIONS - RECRUIT A MIX.**

   IF NEEDED: There are various risks and challenges that any business using digital technologies (this includes any computer connected to the Internet for instance) may face when managing data security and privacy. How familiar would you say you are with these types of risks and challenges?

   ○ Very familiar
   ○ Fairly familiar
   ○ Not very familiar
   ○ Not at all familiar

IF NOT VERY OR NOT AT ALL FAMILIAR, ASK: ***Since this will be one of the themes discussed, is there someone else in your company who would be more familiar with these issues?***

○ **IF YES, ASK TO SPEAK WITH THAT PERSON INSTEAD**
○ **IF NO, CONTINUE**

2. Approximately how many full-time staff (FTE) does your company currently employ in Canada? **(RECORD ACTUAL NUMBER)**
   _______ Full-time equivalent staff

   - 1 to 5 **[SMALL BUSINESS <u>AND</u> A MICRO BUSINESS]**
   - 6 to 99 **[SMALL BUSINESS]**
   - 100 to 499 **[MEDIUM BUSINESS]**
   - More Than 500 **[THANK & TERMINATE]**

3. How do you identify yourself? *(Note 1: Ensure a good mix in and across all sessions/interviews other than Group 12 - "Women Entrepreneurs". Note 2: DO NOT READ: Gender – Refers to current gender which may be different from sex assigned at birth (male or female) and may be different from what is indicated on legal documents.*)

   - Male gender
   - Female gender
   - Gender diverse
   - Prefer not to answer

4. We have been asked to speak to decision-makers from all different ages. May I have your age please? **READ CATEGORIES AS NEEDED** (Note: Ensure a good mix in and across all sessions/interviews other than *Group 13 - "Young Entrepreneurs"*)

   - Under 18 **THANK/TERMINATE**
   - 18 to 24 years
   - 25 to 34 years
   - 35 to 44 years
   - 45 to 54 years
   - 55 to 64 years
   - 65 to 74 years
   - 75 years or older

5. How many years have you owned or managed this company? **Record number** _______ years

   - **[DO NOT READ]** Don't know / Not Sure

6. Are you one of the individuals who founded this company?

   - Yes **[ENTREPRENEURS]**
   - No

- *IF RESPONDENT IS ONE OF THE FOUNDERS AND A WOMAN, FLAG AS "WOMAN ENTREPRENEUR"*
- *IF RESPONDENT IS ONE OF THE FOUNDERS AND BETWEEN 18-34, FLAG AS "YOUNG ENTREPRENEUR"*

7. Please let me know if you fall into any of the following categories:

	Yes	No
a) Are you an Indigenous person, that is, First Nations, Métis or Inuk (Inuit)? First Nations includes Status and Non–Status Indians.	❑	❑
b) Are you a person who is blind or has any difficulty seeing even when wearing glasses or contact lenses? **[THANK AND TERMINATE IF "YES"]**	❑	❑
c) Are you a person who is physically disabled, for instance you have difficulty walking, using stairs, using your hands or fingers or doing other physical activities?	❑	❑
d) Do you have any difficulty learning, remembering or concentrating?	❑	❑
e) Do you have any emotional, psychological or mental health conditions?	❑	❑
f) Is your business located in a town, village or rural area with a population of less than 10,000 and you are at least a two-hour drive from a city of at least 50,000?	❑	❑
g) **[DO NOT ASK IF 7A=YES]** Have you immigrated to Canada within the past 10 years?	❑	❑

*Source: 2017 Canadian Survey on Disability

- *IF YES AT Q7A – RECRUIT AS INDIGENOUS ENTREPRENEUR/BUSINESS OPERATOR*
- *IF YES AT ANY OF Q7B-E – RECRUIT AS ENTREPRENEUR/BUSINESS OPERATOR WITH A DISABILITY*
- *IF YES AT Q7F – RECRUIT AS RURAL AND REMOTE ENTREPRENEUR/BUSINESS OPERATOR*
- *IF YES AT Q7G – RECRUIT AS NEWCOMER ENTREPRENEUR/BUSINESS OPERATOR*

8. Approximately what percentage of your annual revenues come from buyers located outside Canada? _______%

AT LEAST 2 PARTICIPANTS IN EACH IN-FACILITY AND IN EACH TELE-WEB FOCUS GROUP SHOULD HAVE INTERNATIONAL SALES

9. In which industry or sector does your company operate? If you are active in more than one sector, please identify the main sector. **DO NOT READ LIST. ACCEPT ONLY ONE RESPONSE. CONFIRM RESULT WITH RESPONDENT AS NECESSARY. RECRUIT A MIX.**

- Agriculture/Fishing/Hunting/Forestry
- Oil/Gas/Mining
- Utilities
- Construction
- Manufacturing
- Wholesale Trade
- Retail Trade
- Transportation and Warehousing
- Information and Cultural Industries
- Finance and Insurance/Real Estate and Rental
- Professional, Scientific and Technical Services/IT/Computers
- Administrative and Support
- Waste Management
- Remediation Services
- Art/Entertainment/Recreation
- Accommodation/Food Services/Tourism
- Other (specify)

10. Can you please provide me with your job title? _______________________________________

11. Participants in discussion groups or interviews are asked to voice their opinions and thoughts, how comfortable are you in voicing your opinions in front of others? Are you... **READ OPTIONS**

○	Very comfortable	**MIN 5 PER GROUP**
○	Fairly comfortable	
○	Not very comfortable	**TERMINATE**
○	Not at all comfortable	**TERMINATE**

12. Have you ever attended a discussion group or interview on any topic that was arranged in advance and for which you received money for your participation?

○	Yes	**MAXIMUM 5 PER GROUP**
○	No	**GO TO INVITATION**

13. When did you last attend one of these discussion groups or interviews?

○	Within the last 6 months	**TERMINATE**
○	Over 6 months ago	

14. How many discussion groups or interviews have you attended in the past 5 years?

Fewer than 5	
5 or more	**TERMINATE**

E. Focus Group Invitation

I would like to invite you to participate in the focus group in your city. The discussion will be led by a researcher from a Canadian public opinion research company, Quorus Consulting. The group will take place on **[DAY OF WEEK]**, **[DATE]**, at **[TIME]**. It will last one and a half hours (90 minutes). People who attend will receive $150 to thank them for their time. This will be provided to you at the facility after the session. Would you be willing to attend?

○	Yes	
○	No	**TERMINATE**

Sometimes participants are also asked to write out their answers on a questionnaire. Is there any reason why you could not participate?

○	Yes	**TERMINATE**
○	No	

If you require reading glasses, please remember to bring them with you, as you may be required to read some materials during the session.

***TERMINATE IF RESPONDENT OFFERS ANY REASON SUCH AS SIGHT OR HEARING PROBLEM, A CONCERN WITH NOT BEING ABLE TO COMMUNICATE EFFECTIVELY OR IF YOU HAVE ANY OTHER CONCERN*.**

The session will be audio and video recorded for research purposes and representatives of the Government of Canada research team will be observing from an adjoining room. You will be asked to sign a waiver to acknowledge that you will be video recorded during the session. The recordings will be used only by the Quorus Consulting research team and will not be shared with others. As I mentioned, all information collected in the group discussion will remain anonymous and be used for research purposes only in accordance with laws designed to protect your privacy.

The focus group will be at the following location: **REFER TO PAGE 3**

We ask that you arrive fifteen minutes early to be sure you find parking, locate the facility and have time to check-in with the hosts. The hosts may be checking respondent's identification prior to the group, so please be sure to bring some personal identification with a photo with you (i.e. driver's license).

As we are only inviting a small number of people, your participation is very important to us. If for some reason you are unable to attend, please call so that we may get someone to replace you – you cannot send your own replacement if you cannot attend. You can reach us at **1-800-XXX-XXXX** at our office. Please ask for **[recruiter to provide]**. Someone will call you the day before to remind you about the discussion.

So that we can call you to remind you about the focus group or contact you should there be any changes, can you please confirm your name and contact information for me? **COLLECT ON FRONT PAGE**

Thank you very much for your help!

F. Tele-Web Focus Group Invitation

I would like to invite you to participate in a web-assisted telephone focus group discussion with a senior research consultant from a Canadian public opinion research company, Quorus Consulting. The session for businesses in your region is scheduled take place on **[DAY OF WEEK]**, **[DATE]**, at **[TIME]**. It will last one and a half hours (90 minutes). People who attend will receive $150 to thank them for their time. We will get this to you either by email transfer or by mailing you a check at the conclusion of the session. Would you be willing to attend?

○ Yes
○ No **TERMINATE**

The session will be audio recorded for research purposes and representatives of the Government of Canada research team may be on the line as remote observers. You will be asked to acknowledge that you will be audio recorded during the session. The recordings will be used only by the Quorus Consulting research team and will not be shared with others. As I mentioned, all information collected in the group discussion will remain anonymous and be used for research purposes only in accordance with laws designed to protect your privacy.

To conduct the session, we will be using a video conferencing application so that you can see material that the moderator will want to show the group. We will need to send you the instructions to connect by email. The use of a computer is necessary since the moderator will want to show material to participants to get their reactions – that will be an important part of the discussion.

IF ASKED: You will not need to use a webcam to participate – the videoconferencing application is just being used to show you material and although you might be able to see the moderator through their webcam, there is no need for you to use your webcam.

Over the coming days we will be sending you an email with the conference call logistics with the specific telephone number you will need to dial, the participant passcode, a web link to connect to the online session as well as the date and time of the call.

We recommend that you click on the link we will send you a few days prior to your session to make sure you can access the online meeting that has been setup and repeat these steps at least 10 to 15 minutes prior to your session.

As we are only inviting a small number of people, your participation is very important to us. If for some reason you are unable to participate, please call so that we may get someone to replace you – you cannot choose your own replacement if you cannot attend. You can reach us at **1-800-XXX-XXXX** at our office. Please ask for **[recruiter to provide]**. Someone will call you the day before to remind you about the discussion.

So that we can send you the email with the logistics, call you to remind you about the session or contact you should there be any changes, can you please confirm your name and contact information for me? **COLLECT ON FRONT PAGE**

Thank you very much for your help!

G. Tele-Web Interview Invitation

I would like to invite you to participate in a web-assisted telephone interview with a senior research consultant from a Canadian public opinion research company, Quorus Consulting. We would like to schedule the interview with you between **DATE START** and **DATE END** at a time that works best for you. Would you have time on **[INSERT DATE AND TIME OPTIONS]**? It will last roughly 45 minutes, depending on how much feedback you provide. People who participate will receive $100 to thank them for their time – we will get this to you either by email transfer or by mailing you a check at the conclusion of the interview.

SCHEDULE INTERVIEW THAT FITS RESPONDENT AND INTERVIEWER SCHEDULES

The session will be audio recorded for research purposes and representatives of the Government of Canada research team may be on the line as remote observers. You will be asked to acknowledge that you will be audio recorded during the session. The recordings will be used only by the Quorus Consulting research team and will not be shared with others. As I mentioned, all information collected in the interview will remain anonymous and be used for research purposes only in accordance with laws designed to protect your privacy.
To conduct the session, we will be using a video conferencing application so that you can see material that the moderator will want to show you. We will need to send you the instructions to connect by email. The use of a computer is necessary since the moderator will want to show you material to get your reactions – that will be an important part of the discussion.

IF ASKED: You will not need to use a webcam to participate – the videoconferencing application is just being used to show you material and although you might be able to see the moderator through their webcam, there is no need for you to use your webcam.

Over the coming days we will be sending you an email with the conference call logistics with the specific telephone number you will need to dial, the participant passcode, a web link to connect to the online session as well as the date and time of the call. There will also be contact information in the email in case you need to change the date or time of the interview.

We recommend that you click on the link we will send you a few days prior to your session to make sure you can access the online meeting that has been setup and repeat these steps at least 10 to 15 minutes prior to your session.

As we are only inviting a small number of people, your participation is very important to us. If for some reason you are unable to participate, please call so that we may get someone to replace you – you cannot choose your own replacement if you cannot attend. You can reach us at **1-800-XXX-XXXX** at our office. Please ask for **[recruiter to provide]**. Someone will call you the day before to remind you about the discussion.

So that we can send you the email with the call logistics, call you to remind you about the interview or contact you should there be any changes, can you please confirm your name and contact information for me? **COLLECT ON FRONT PAGE**

Thank you very much for your help!

Moderation Guide – Consumers (English)

Focus Group Moderation Guide for Consumers

A. <u>Introduction (8 minutes)</u>

- Introduce moderator
- Thanks for attending/value you being here
- Explain general purpose of focus group discussions:
    - We will be spending an hour and a half discussing various aspects of cyber security when buying products and services from Canadian companies, in particular small and medium sized companies (SME's).
    - Gauge *opinions* about issues/ideas/products.
    - <u>Not</u> a knowledge test; no right or wrong answers (interested in opinions).
    - Okay to disagree; want people to speak up if hold different view.
    - Do not need to direct all comments to me; can exchange ideas with each other.
    - Tonight, we're conducting research on behalf of the Government of Canada but the moderator is not an employee of the Government of Canada.
    - Looking for candor and honesty; comments treated in confidence; reporting in aggregate form only; video recording and note-taking for report writing purposes only; observers behind one-way glass.
    - If you have a cell phone, please turn it off.

So let's go around the table and have everyone introduce themselves. Tell us your name and a little bit about yourself, such as who you live with and what is your favourite hobby.

B. Confidence in Current Level of Cyber Security (25 minutes)

Thank you – today we will be talking about your perceptions and attitudes towards purchasing products and services in Canada from small to medium sized businesses. Just so we are all on the same page, Statistics Canada defines a micro business as having 5 or fewer employees, a small business as having roughly 100 or fewer full-time employees and a medium business as having between 100 and roughly 500 employees.

I'd like to start off with a broad discussion about how you are feeling about your level of "cyber security" these days

- First off, what does cyber security mean to you as a consumer?

AFTER GENERAL DISCUSSION, MODERATOR TO READ: I am broadly referring to how secure you feel when purchasing something from small to medium sized businesses in Canada. This includes how they secure their computers, their Internet and Wi-Fi network, the systems they have in place to store and protect company data, including any information they may be storing about customers, suppliers, staff, etc.

- How important is cyber security to you as a consumer?
- I'm certainly not suggesting you should be worried…but honestly, on a scale from 0 to 10, where 0 means you are feeling extremely vulnerable and 10 means you are feeling completely protected, how protected are you feeling about purchasing items or services from SMEs in Canada these days? **MODERATOR COLLECTS SCORE ON FLIPCHART**
    - **FOR POSITIVE SCORES –** What makes you feel protected? What gives you confidence that your transaction information is protected?
    - **FOR NEGATIVE SCORES –** What are your concerns exactly? …is there room for improvement?

    Probe: Do you feel that SMEs are taking this issue seriously?

- What would a company have to do to make you feel more secure?
- Can you identify the level of cyber security that businesses provide to their customers? If so, how do you identify it?
- Some of you have made purchases online. Does cyber security make a difference if you are shopping in person vs. online?
- Do you think all SMEs should be cyber secure to be allowed to sell products and services in Canada?

- What role, if any, could or should the Government of Canada be playing when it comes to supporting small and medium sized businesses in this area? (Let's try to stay focused on the role of the Federal government and not the roles the provincial or municipal governments play.)
    - Can they better support businesses to improve their level of cyber security?

  Probe if not mentioned by participant: Should the government make it mandatory for businesses to offer some degree of cyber security?

C. General Concept Evaluation (35 minutes)

The Government of Canada will be introducing a cyber security certification program for small and medium sized businesses. Those who meet certain requirements will be "certified" and will be able to demonstrate they have met the requirements through a badge or label that could look like the following.

A few things you need to keep in mind – these are all draft concepts so I'll be eager to get your honest feedback around these ideas.

STEP 1 (20 minutes)

As a first exercise, please rate each proposed badge using the handout I just provided. This is an individual exercise – we'll discuss each one afterwards. **MODERATOR TO HANDOUT "CONCEPT RATING GRID"**

- **PARTICIPANTS USE A RATING GRID TO RATE EACH CONCEPT ON THE FOLLOWING CRITERIA ON A SCALE FROM 0 TO 10:**
    - ✓ Unique [there is nothing else like this in the market]
    - ✓ Memorable
    - ✓ Credible
    - ✓ Relevant [it conveys the notion of cyber security]
    - ✓ Overall appeal

CONCEPTS ARE DISCUSSED BEFORE MOVING ON TO THE NEXT CONCEPT:

- What comes to mind when you see this concept? What does this look like to you?
- What are your quick thoughts on this concept?
- What do you like most about it? What do you like least?
- Does it look like anything else out there? If so, what?

  - If yes, is that a good thing or a bad thing? Does that help or is it confusing in your opinion?
- Do you have any quick reactions to the bilingual concept?
- How well does this concept convey the idea of being cyber secure?
- Would you notice this on a storefront and/or website?

STEP 2 (5 minutes)

ACROSS ALL CONCEPTS:

- Which concept best conveys the idea of being cyber secure?

STEP 3 (5 minutes)

EXPLORE TIER SYSTEM (1 HANDOUT SHOWING ALL CONCEPTS FOR EACH PARTICIPANT TO SEE)

- What are your quick thoughts on the idea of having tiers (i.e. three levels of cyber security)?
  - **SHOW OF HANDS:** Who prefers the idea of having tiers?
- And how do you feel about the way tiering could be conveyed through the visual concept?
- Is one of the concepts more effective or appealing when it comes to showing the tiers?

STEP 4 (5 minutes)

EXPLORE COLOUR CONCEPTS (1 HANDOUT SHOWING ALL CONCEPTS FOR EACH PARTICIPANT TO SEE)

- What are your quick thoughts on the colours considered?
- Across all the options shown on the page, which one do you prefer? Go ahead and circle it.
- If there is going to be a tiering system, should there be a different colour for each tier? If so, what would you propose?

D. Potential Impact on Competitiveness (5 minutes)

- As a consumer, do you think that if this identifier were displayed you would be more likely to choose them over a competitor who lacks this identifier?

    - **ALTERNATIVELY:** Do you think this identifier will convey a sense of trust and/or security when selling products or services? Would you think a business is more cyber secure if they displayed this identifier?
- Would seeing this branding impact your decision when purchasing from a business?
- Other than on a storefront and/or on a website, where else or how else would you want to see this branding?

E. <u>Expectations of the Program (15 minutes)</u>

The program rollout and implementation will be designed and supported by the Government of Canada. This is your opportunity to share what your expectations would be for a program like this. **[IF NEEDED:** You may have many questions for me but I don't have the finer details of the program yet – part of this research involves understanding what you would expect a program like this to look like and achieve.]

- What expectations do you have of the program in terms of how it would work? What would you need to know to be convinced that it is worth considering dealing with businesses that are certified?
- What is your expectation of a company that is certified compared to a company that is not?
- As a consumer, in what way do you feel a certified business will protect you more?
- If a business were to become certified through this program, what would your new level of vulnerability/protection be as a consumer? …let's revisit your rating that you provided at the beginning of the session: on a scale from 0 to 10, where 0 means you are feeling extremely vulnerable and 10 means you are feeling completely protected.
- Does anyone here expect a certification program like this will make a company 100% cyber secure?
    - If it cannot guarantee that, how does that impact your interest in working with a company that has this?
- What are your expectations of government oversight and/or involvement in the program?
- Does anyone here expect the certification process to increase the cost of the product or service purchased?
- Would you be willing to pay more for a product or service from a company that is certified?

F. THAND AND CLOSE (2 minutes)

[BACKROOM CHECK]

In parting, is there anything that you think I should have asked but I didn't?

Please remember to sign out as you leave the focus group room – this is just to confirm you've received the incentive we promised you. [**FOR GROUP 1:** Take care as well not to discuss what has been discussed here as you leave the facility since I have participants from my next session in the lobby/waiting area.]

Thanks again and have a great evening!

Moderation Guide – SMEs (English)

Focus Group Moderation Guide for SMEs

A. <u>Introduction (8 minutes)</u>

- Introduce moderator
- Thanks for attending/value you being here
- Explain general purpose of focus group discussions:
  - We will be spending an hour and a half discussing various aspects of your company's level of cyber security and the challenges you may face achieving the level of security you want.
  - Gauge *opinions* about issues/ideas/products.
  - <u>Not</u> a knowledge test; no right or wrong answers (interested in opinions).
  - Okay to disagree; want people to speak up if hold different view.
  - Do not need to direct all comments to me; can exchange ideas with each other.
  - Tonight, we're conducting research on behalf of the Government of Canada but the moderator is not an employee of the Government of Canada.
  - Looking for candor and honesty; comments treated in confidence; reporting in aggregate form only; video recording and note-taking for report writing purposes only; observers behind one-way glass/are on the web conference as well.
  - If you have a cell phone, please turn it off.

Tele-web: Thank you all for joining the web conference. Even though you can see me, there is no need for you to activate your webcam. As well, in the list of participants, we will make sure only your first name appears (moderator can edit the names of participants as needed to remove last names).

For the most part, you will just be using the audio portion of the tool and the chat feature. In a few moments, I will share my screen with everyone so that you can see some visual concepts we will be discussing.

- **To activate and use the chat function**, scroll over the bottom of their screen until the command bar appears. There you will see a function called “chat”. It will open a chat screen on the far right of your screen. I’d like to ask you to use chat throughout our discussion tonight. Let’s do a quick test right now – please open the chat window and send the group a short message (e.g. *Hello everyone*). If you have an answer to a question and I don’t get to ask you specifically, please type your response in there. We will be reviewing all chat comments at the completion of this project.

- If you are not speaking, I would encourage you to **mute your line** to keep background noise to a minimum…just remember to remove yourself from mute when you want to speak!

So let’s go around the table and have everyone introduce themselves…I’ll be curious to know the following:

- What is your role or your position?
- What type of business do you own/operate/manage?
- And, in that role, what would you say is your biggest concern these days? What keeps you up at night?

B. Business Confidence in Current Level of Cyber Security (20 minutes)

I’d like to start off with a broad discussion about how you are feeling about your level of “cyber security” these days. By this I am broadly referring to how secure you feel your overall IT system is these days – this includes your computers, your Internet and Wi-Fi network, the systems you have in place to store and protect company data, including any information you may be storing about your customers, your suppliers, your staff, etc.

- I’m certainly not suggesting you should be worried…but honestly, on a scale from 0 to 10, where 0 means you are feeling extremely vulnerable and 10 means you are feeling completely protected, how are you feeling about this these days?

  TELE-WEB: MODERATOR COLLECTS SCORE ON FLIPCHART

- What are your concerns exactly? …is there room for improvement?
- And what is getting in your way from achieving complete protection?
  - Is complete protection even achievable? If not, what would you consider realistic in terms of cyber security for your company?

- Does your level of cyber security matter to your customers? If so, do you think your customers notice the level of investment you put into your cyber security? How do you know? How can they tell?
- Do you think you are missing out on potential business by not being able to "prove" your level of cyber security?
- What role, if any, could or should the Government of Canada be playing when it comes to supporting small and medium sized businesses like yours in this area? (Let's try to stay focused on the role of the Federal government and not the roles the provincial or municipal governments play.)
    - Can they better support you to improve your level of cyber security?
    - Should the government make it mandatory for businesses to offer some level of cyber security?
        - What impact would this have on your operations?
    - Can they help you become more competitive because you are more cyber secure?

C. General Concept Evaluation (35 minutes)

The Government of Canada will be introducing a cyber security certification program for small and medium sized businesses. Those who meet certain requirements will be "certified" and will be able to demonstrate they've met the requirements through a badge or label that could look like the following.

A few things you need to keep in mind – these are all draft concepts so I'll be eager to get your honest feedback around these ideas.

TELE-WEB: I am going to be sharing some images with you on the screen. We ask that you do not record or take screen shots or otherwise share this content in any way.

STEP 1 (20 minutes)

As a first exercise, please rate each proposed badge using the handout I just provided. This is an individual exercise – we'll discuss each one afterwards. **MODERATOR TO HANDOUT "CONCEPT RATING GRID"**

CONCEPTS A, B AND C ARE PRESENTED ONE AT A TIME BY THE MODERATOR (CONCEPTS TO BE PRESENTED IN A DIFFERENT ORDER FOR EACH SESSION):

- **IN-FACILITY: PARTICIPANTS USE A RATING GRID TO RATE EACH CONCEPT ON THE FOLLOWING CRITERIA ON A SCALE FROM 0 TO 10:**
- **TELE-WEB: PARTICIPANTS USE THE CHAT FEATURE TO SEND THROUGH THEIR RATINGS**
  - ✓ Unique [there is nothing else like this in the market]
  - ✓ Memorable
  - ✓ Credible
  - ✓ Relevant [it conveys the notion of cyber security]
  - ✓ Overall appeal

CONCEPTS ARE DISCUSSED BEFORE MOVING ON TO THE NEXT CONCEPT:

- What comes to mind when you see this concept? What does this look like to you?
- What are your quick thoughts on this concept?
- What do you like most about it? What do you like least?
- Does it look like anything else out there? If so, what?
  - If yes, is that a good thing or a bad thing? Does that help or is it confusing in your opinion?
- Do you have any quick reactions to the bilingual concept?
- How well does this concept convey the idea of being cyber secure?
- Would you want to display this identifier in your storefront and/or on your website?

STEP 2 (5 minutes)

ACROSS ALL CONCEPTS:

- Which concept best conveys the idea of being cyber secure?
- Which one would you pick to display in your storefront and/or on your website?
  - Help me understand your choices a bit here.

STEP 3 (5 minutes)

EXPLORE TIER SYSTEM (1 HANDOUT SHOWING ALL CONCEPTS FOR EACH PARTICIPANT TO SEE)

- What are your quick thoughts on the idea of having tiers (i.e. three levels of cyber security)?
  - **SHOW OF HANDS / VOTING VIA CHAT FEATURE:** Who prefers the idea of having tiers?

- And how do you feel about the way tiering could be conveyed through the visual concept?
- Is one of the concepts more effective or appealing when it comes to showing the tiers?

STEP 4 (5 minutes)

EXPLORE COLOUR CONCEPTS (1 HANDOUT SHOWING ALL CONCEPTS FOR EACH PARTICIPANT TO SEE)

- What are your quick thoughts on the colours considered?
- Across all the options shown on the page, which one do you prefer? Go ahead and circle it. **(TELEWEB - VOTE VIA CHAT FEATURE)**
- If there is going to be a tiering system, should there be a different colour for each tier? If so, what would you propose?

D. Potential Impact on Competitiveness (10 minutes)

- Do you feel being associated to this brand will benefit your business? Would it genuinely add value to your business?
    - On what would the success of this branding for your company depend? In other words, if this branding is going to benefit your company, what needs to happen?
- As a business owner, do you think that if you display this identifier, consumers would be more likely to choose you over a competitor who lacks this identifier?
    - **ALTERNATIVELY:** Do you think this identifier will convey a sense of trust and/or security to your consumers? Do you think consumers would think your business is more cyber secure if you displayed this identifier?
- Other than on your storefront and/or on your website, where else or how else would you want to display this branding?

E. Expectations of the Program (15 minutes)

The program rollout and implementation will be designed and supported by the Government of Canada. This is your opportunity to share what your expectations would be for a program like this. **[IF NEEDED:** You may have many questions for me but I don't have the finer details of the program yet – part of this research involves understanding what you would expect a program like this to look like and achieve.]

- What expectations do you have of the program in terms of how it would work? What should the process of certification look like for you to be convinced that it is worth your while to go through it?
- What would this program need to look like for you to believe that businesses displaying this branding are in fact more cyber secure?
- If your business were to become certified through this program, what would your new level of vulnerability/protection be? Let’s revisit your rating that you provided at the beginning of the session: on a scale from 0 to 10, where 0 means you are feeling extremely vulnerable and 10 means you are feeling completely protected.
- Does anyone here expect a certification program like this will make your company 100% cyber secure?
    - If it cannot guarantee that, how does that affect your interest in being certified?
- What are your expectations of government oversight and/or involvement in the program?
- Does anyone here expect the certification process to be free?
    - If you need to pay a fee to become certified, how does that affect your interest in being certified?
    - What would you consider a reasonable fee to go through the certification process? Note that I am not referring to any investments you may need to make to meet the program’s requirements – I am just talking about the evaluation or cyber audit your company would need to go through to assess how cyber secure you are.

F. THANK AND CLOSE (2 minutes)

[BACKROOM CHECK]

In parting, is there anything that you think I should have asked but I didn’t?

FOR IN-FACILITY SESSIONS: Please remember to sign out as you leave the focus group room – this is just to confirm you’ve received the incentive we promised you. [**FOR GROUP 1:** Take care as well not to discuss what has been discussed here as you leave the facility since I have participants from my next session in the lobby/waiting area.]

Thanks again and have a great evening!

Participant Activity Sheet (English)

On a scale from 0 to 10, where 0 means “Poor” and 10 means “Excellent”, how would you rate each concept on the following attributes:

Write your rating in the grid for each concept presented	Concept A	Concept B	Concept C
Unique – there is nothing else like this in the market			
Memorable			
Credible			
Relevant – it conveys the notion of cyber security			
Overall appeal			

SCALE TO BE USED:

Poor										Excellent
0	1	2	3	4	5	6	7	8	9	10