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

Innovation, Science and Economic Development Canada

CyberSecure Canada

Promoting cyber security and awareness among Canadian businesses

Final report

August 2021

Prepared for Innovation, Science and Economic Development Canada
Supplier name: Quorus Consulting Group Inc.
Contract award date: January 6, 2021
Contract number: U4408-210641/001/CY
Contract value: $59,944.96
Delivery date: September 2021
POR Number: POR 098-20
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

Canada

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-isde@ISED-isde.gc.ca

Permission to reproduce

Cat. No. Iu4-407/2021E-PDF

ISBN 978-0-660-40731-9978-0-660-32481-4

Aussi offert en français sous le titre *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

As a response to cyber security threats, budget 2018 announced a cyber certification program for small and medium enterprises (SMEs). In partnership with the Standards Council of Canada and the Communications Security Establishment, ISED have established the Cybersecure Canada program. The goal is to raise the cyber security baseline among SMEs, thereby increasing consumer confidence in the digital economy, promoting international standardization, and better positioning Canadian SMEs to compete globally.

In order to raise awareness, advertising campaigns have been planned. The initial campaign, launched February 2021, is a digital advertising promotion to encourage SMEs to learn about the Cybersecure program and to become certified.

The digital campaign's primary objective is to build brand recognition and awareness of the Cybersecure Canada program and its mark. Its call to action targets small and medium business organizations and drives them to the Cybersecure Canada website at www.Canada.ca/cybersecure.

The primary public opinion research objectives were to test advertising concepts and their underlying messages through the engagement of SMEs in online (virtual) focus groups prior to launch of the campaign. The research also sought the views of small and medium-sized business on both their current understanding of cybersecurity and of the Cybersecure program in particular. The research sought to obtain the following:

a. insights on and reactions towards a set of advertising concepts;
b. preferred elements in the presented creative concepts;
c. whether business participants understand the overall messaging and its credibility (both written and visual);
d. preferred channels of communication for the overall advertising and marketing campaign; and
e. reactions to and interest and level of trust in the Cybersecure program.

The second phase of the research consisted of one-on-one web-assisted depth interviews held with a range of large enterprises and industry groups and associations; the objective of this phase of the research was to further discuss the following:

a) For those representing industry groups or associations, the research sought to discover the importance of cyber security to the industry in general, the impact of the pandemic, the industry's cyber security readiness and what needs to happen for the industry to improve.
b) For those representing private sector businesses with sizable supply chains, the research looked for insights on the organizations' state of cyber security readiness, the impact of the pandemic, and, specifically, views on their approaches to and state of supply chain cyber security management.
c) Awareness of and interest in the Cybersecure program, barriers to use of the program, perceived role of the Government of Canada, and implications for supply chains or for their industry members, as appropriate.

Methodology

The first phase of the research methodology consisted of ten online focus groups, eight groups completed in stage 1 between January 25 and January 28, 2021, and two groups completed in stage 2 on February 16, 2021. Participants were small and medium-sized business owners and representatives from not-for profit organizations from across Canada. Recruitment prioritized representatives of businesses with 40 to 100 employees (i.e., the larger small business segment). Within each organization, the research targeted a decision-maker regarding cyber security or someone who plays an important role in the day-to-day operations and direction of the company.

Each participant received $200 for participating. In total, representatives of 54 businesses participated in the focus groups.

The second phase of the research consisted of six one-on-one web-assisted depth interviews held with a range of large enterprises and industry groups and associations.

The list of organizations invited to this phase of the study was developed by ISED and recruitment was done by Quorus. Each of the interview participants received $250 for their time.

All participants were informed the research was for the Government of Canada.

Research results

Phase 1 focus groups – Initial concept testing

Cyber security

At the beginning of each focus group, a general discussion was held about cyber security. The term was often described by participants with words such as "protection" and "information" and "system safety." While most participants felt that their companies and systems were reasonably secure to quite secure, there was also a general consensus that it is impossible to be fully secure and that there is always room for continuing improvement. Ensuring cyber security was also seen as a necessary cost of doing business.

Virtually all companies had to adapt to a certain degree due to the COVID-19 pandemic. They had become more internet dependent, especially since remote work had to become more prevalent. Working from home was seen as creating liabilities on the cyber security front, and adjustments to practices (for example through employee training) and systems (hardware, software, bandwidth) often had to be made.

A number of participants discussed cyber attacks that had happened since the beginning of the pandemic, and the associated costs.

Reactions to advertising concepts

Three advertising concepts were tested in the initial round of focus groups, as follows:

- Concept A – Easier
- Concept B – First Step
- Concept C – Trust (an original version and a variation, tested in the last four groups, which had a different image)

There were some themes that emerged when discussing all concepts, including that participants often wanted to see a more direct, literal connection to cyber security in the creative approach. Many participants also said that the program seal was a key element of the ad concepts and should get more prominence. This would go a long way in portraying the more literal link sought by participants and focusing the targeted audience, i.e. small and medium businesses, on the main message and purpose of the new program.

On the other hand, there was a sense that the target audience of these ads understood the importance of cybersecurity and that therefore, this would not have to be as much of

a key message as it was in the concepts tested. Rather, they felt that the ads should contain more information about the program itself, as the lack of information about this in the concepts begged many questions and left participants to make assumptions about it, which were not always accurate. As well, participants said that the Government of Canada sponsorship of the program should get more prominence. In the video concepts, showing the government sponsorship should also be done much earlier in the clip to provided reassurance and relevance.

The overall sense was that the ads would do a mediocre job of catching their attention. The call to action to find out more was generally not seen as strong enough to make participants want to investigate more on their own.

Concept A – Easier did not receive high marks and was the least preferred concept. One of the main reasons for this was that it begged questions about the intended audience, which was interpreted at first glance to be consumers, rather than businesses. This was mainly in reaction to the colourful creative execution with the pie, which also fell rather flat because the message it conveyed was often not linked to the idea of cyber security. If anything, it was telling people that cyber security was easy (as pie), which was not necessarily their experience. The content in the text begged questions of participants, rather than informing them of the program. While the call to action to click the link to find out more was clear, most participants said they would not be compelled to do so based on the execution of this concept.

Concept B – First Step received mixed reviews. While it was the preferred choice for some, most participants ranked it second. However, it also received some critical feedback about the execution, the perceived target audience and the message.

While the creative execution was generally seen as eye-catching, some also felt it was too cluttered and not in line with the gravitas that the issue of cyber security had for many. Despite the words on the sneaker, the concept was seen by many participants to be geared towards a younger audience or towards start-up companies. For some, there was no easily recognizable link to cyber security. On the other hand, others appreciated the metaphor of “taking the first step” or “moving towards” something, namely cyber security certification.

The call to action was understood, yet reviews were mixed on whether the ad was compelling enough for people to follow through – some said they would, while others said they would not.

Concept C – Trust was the winner of the three concepts tested, standing out from the other concepts. Participants felt that the idea of trust was the most relevant and direct tie to cyber security and the overall concept was said to be the most targeted to them. This was both because of the creative approach, which received positive reviews, and because of the main message that resonated with them. The idea and images of trust and the links (that we are all in this together, yet links could also easily be broken if there was a weakness) were generally well-liked.

Participants often said that the overall tone of this concept was more serious and more geared towards a business audience.

However, not everyone liked the creative choice of bees; rather, some said they would prefer to have people in the ad.

In the last four groups, participants were also shown a variation of this concept, which had the same text but a different image, which included a person. And while for some, the general idea of depicting a person rather than insects was a positive change, most felt that the execution in this case did not work.

Reactions to the Cybersecure Certificate Program

After seeing the ads, a short discussion was held about the program. While none of the participants had been aware of it, based on the description provided and the concepts they had seen, there was a high level of interest in finding out more. There was some sense, however, that more information that spoke to "what's in it for me" would have to be provided to clarify some details before companies would jump into getting certified.

Phase 1 focus groups – Success check

Two revised concepts were tested in two additional focus groups, namely:

- Concept A – Beavers
- Concept B – Trust Chain

Both concepts received mixed reviews.

Concept A – Beavers was said to have a clear message, but there was some discussion on whether the message about "supply chain" was a key part of the message or would turn off those who felt it was irrelevant to them because they did not have a supply chain. Many participants wanted more information about the program itself instead.

Those who liked it appreciated the ideas of "working together," "interconnectedness" and of "something being built" it conveyed. The idea of trust, the prominence of the logo and the Canadian-ness of the beaver were also pointed to as positive elements of this concept.

Those who did not like it tended to feel that there was a disconnect between beavers and cyber security, and that there was no connection to people or it in the concept. Some also felt it was "too cute" and lacked the serious tone that would be more appropriate for them given the topic.

Concept B – Trust Chain also divided participants. Those who liked it pointed to the picture of diverse people working together, the prominence of the Government of Canada logo and the legitimacy that it lent to the program, and to the focus on trust. As well, there were some who liked the overall execution, saying it would catch their eye.

However, for most participants, the cartoon execution fell flat. Those who did not like it, said it was not fitting as it was seen as not serious enough or representative of cyber security. It was also said that it was not geared towards all audiences or all businesses, but would rather mainly attract younger people or start-ups.

Phase 2 Stakeholder in-depth interviews

Cyber security readiness

As was seen in the focus groups, there was a sense among interview participants that there are always areas for improvement when it comes to cyber security, no matter the level of readiness they currently have.

Key factors for participants in assessing cyber security readiness included:

- The data intensity of their industry: those who are in an industry where data are an important element of their day-to-day operations were more likely to put a higher level of importance and resources into cyber security.
- The size of their business: scale was a key factor, with participants saying that the bigger the business, the more resources they would have, and the more likely they would be to have higher cyber security standards in place. Small businesses or organizations (for example, in the healthcare field) said that cyber security is neither their expertise nor their top priority.
- Budget: cost can be a prohibiting factor that impacts cyber security readiness.

- Knowledge gaps: not all businesses have the expertise needed to improve their level of cyber security.
- Lack of extrinsic expectation or pressure: in certain industries, there is limited to no expectation from customers or regulators to uphold a certain standard when it comes to cyber security.
- The level of competitive differentiation that cyber security can bring for a business or company: this is something that varies greatly from sector to sector.

Supply chain considerations

Interviews with representatives from large organizations in the manufacturing and specialized healthcare fields included a discussion on supply chain management. While the scale of these organizations was large and therefore facilitated having resources and staff dedicated to IT, cyber security and supply chain management, these two types of businesses tended to have different approaches to data management.

While manufacturing companies tended to mainly deal with their own internal data and generally saw this as their priority (rather than data that others, such as customers or suppliers they manage), healthcare organizations often deal with personal data from the general public, which is more complex and needs a more sophisticated approach when it comes to security. Moreover, because of the sensitivity of the data they house and share, there is a higher level of concern about how their suppliers collect and manage data.

While for manufacturers, cyber security is not a procurement consideration in the selection of suppliers nor is it an ongoing concern once a supplier relationship is established, for those in the healthcare field, the level of cyber security of suppliers plays an important role.

Role of Government of Canada in cyber security

Interviewees agreed that there is a role for the Government of Canada in supporting them or those in their industry to become cyber secure. Specifically, the types of supports that were brought up fell into four main categories: to educate and train; to support and incent; to set standards; and to do more to combat cyber criminals.

When it was suggested that the Government of Canada could mandate cyber security levels, there was understanding of why this may happen. While some participants saw advantages, others had concerns. For most, it would have to be seen as a supportive

system, rather than a punitive one. Some also brought up the issue of enforcement, while others wondered whether it would be needed for all types of businesses, or whether this would apply to international suppliers.

Reactions to the Cybersecure Canada program

Participants were given an overview of the program and certification. Awareness was moderate while interest was high, with many commenting on the added value of the program to their industry. Some also indicated they would suggest it to their suppliers or to their broader industry segment. The program was generally seen as appropriate and fairly comprehensive.

At the same time, some concerns were raised. These centered mainly around (the lack of) in-house capacity and expertise, and the cost associated with addressing gaps in cyber security necessary to become certified. Some also felt that it would be difficult to have one standard or certification that would be appropriate for all industries. However, those who already had their own industry standards in place pertaining to cyber security indicated that they would be open to collaborating with the Government of Canada.

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: U4408-210641/001/CY
Contract award date: January 6, 2021
Contract value (including HST): $59,944.96
For more information, please contact Innovation, Science and Economic Development Canada at:
ic.publicopinionresearch-recherchesurlopinionpublique.ic@Canada.ca

Detailed results

Research purpose and objectives

Cyber attacks can have a direct impact on an organization and its customers, including financial losses and reputational damage. By becoming cyber secure, small and medium enterprises (SMEs) can improve their cyber security practices, enabling them to build trust, protect their data and finances, and gain a competitive advantage.

As a response to cyber security threats, budget 2018 announced a cyber certification program for SMEs. In partnership with the Standards Council of Canada and the Communications Security Establishment, ISED established the Cybersecure Canada program. The goal is to raise the cyber security baseline among SMEs, thereby increasing consumer confidence in the digital economy, promoting international standardization, and better positioning Canadian SMEs to compete globally.

The Cybersecure program is a means for SMEs to demonstrate that they are taking appropriate measures to protect their systems, build resiliency against attacks and safeguard their customers' and contractors' information. Once a business obtains the Cybersecure certification, they are certified for two years and have the option of displaying the certification mark on their websites, storefronts, and promotional materials.

The campaign is a digital advertising promotion to encourage SMEs to learn about the Cybersecure program and to become certified. The Cybersecure Canada website (www.canada.ca/cybersecure) provides businesses and consumers with information on the best practices for cyber security, and the safeguarding of customer and business supplier information. The website provides businesses with an in-depth overview of how the Cybersecure Canada certification program works and invites businesses to enroll in the program and begin their journey towards certification.

The digital campaign's primary objective is to build brand recognition and awareness of the Cybersecure Canada program and its mark. The campaign's call to action targets small and medium business organizations and drives them to the Cybersecure Canada website at www.Canada.ca/cybersecure.

This project focuses on the public opinion research required to support the 2020-21 advertising campaign in meeting its objectives and to better understand how businesses are responding to new and substantial cyber security requirements in the context of the

COVID-19 pandemic which has seen businesses pivot to remote work and online operations while dealing with a spike in the number of cyber attacks.

The primary research objectives for the first phase of the study were to test the concepts and underlying messages through the engagement of SMEs in online (virtual) focus groups. The research sought to obtain the following from business participants:

a. insights on and reactions towards a set of advertising concepts promoting Cybersecure certification;
b. preferred elements in the presented creative concepts;
c. whether business participants understand the overall messaging in the proposed ads and its credibility (both written and visual);
d. preferred channels of communication for the overall advertising and the supporting marketing campaign; and
e. reactions to and interest and level of trust in the Cybersecure program.

On project completion, this component of the research was used to select the best concept and messaging (and/or elements) of presented concepts, by audience, and to identify changes that should be made prior to final production and media placement.

Beyond the concepts and messages tested, there was also a need to understand how businesses are responding to cyber security requirements in the context of the global COVID-19 pandemic and their approach to risk mitigation. The pandemic has impacted business views and preparedness for cyber security and their ability to adapt to the new digital environment is dependent on a solid footing with respect to cyber security. ISED's previous research with this group identified large gaps in knowledge, specifically in small-sized businesses, but also in medium businesses, specifically around the issue of supply chain management. To that end, the focus groups tested:

a. awareness of cyber security practices;
b. awareness of impact of cyberattacks on business operations;
c. the expected outcomes of, as well as barriers to, certification; and
d. challenges and barriers around cyber security in the current environment, including the effects of the COVID-19 crisis.

On project completion, this component of the research will be used to improve the effectiveness of ISED's communications, marketing and outreach efforts in supporting its

mandate to help both businesses and consumers through better understanding of the business audience and its perception of the value proposition of the Cybersecure program and certification process.

The second phase of the research focused on large enterprises and industry groups and associations. The objective of this phase of the research was to further discuss the following:

a) For those representing industry groups or associations, the research sought to discover the importance of cyber security to the industry in general, the impact of the pandemic, the industry's cyber security readiness and what needs to happen for the industry to improve.
b) For those representing private sector businesses with sizable supply chains, the research looked for insights on the organizations' state of cyber security readiness, the impact of the pandemic, and, specifically, views on their approaches to and state of supply chain cyber security management.
c) Awareness of and interest in the Cybersecure program, barriers to use of the program, perceived role of the Government of Canada, and implications for supply chains or for their industry members, as appropriate.

Phase 1 focus groups – Initial concept testing

To gain an initial understanding of the backdrop against which a certification program will be introduced, cyber security in general was explored with SMEs. A variety of aspects were examined, ranging from how cyber secure SMEs believe their companies currently are to how they have needed to adapt due to the pandemic. Following that discussion, three advertising concepts were tested.

Cyber security

Confidence in cyber security

Cyber security was generally described in terms like “protecting information going over the internet,” “paying attention to what’s coming and going over our systems and how safe those interactions or communications are,” “protection of all digital assets” and having “controls and processes in place to protect ourselves from potential attacks.”

When asked how “cyber secure” they feel their companies and systems are, most indicated they are feeling fairly secure, or “cautiously positive”, and believe they have the right systems, procedures and technologies in place. There were some, mainly those who had gone through recent security audits or upgrades, who tended to feel quite secure. For those who were feeling less secure, this tended to have less to do with their systems, and more to do with a sense that the threat levels have been higher in the past year or so than they were before the pandemic. These respondents felt more vulnerable in areas where they had lower levels of awareness or understanding, or in areas where they felt relatively protected in the past.

There was a general sense that it is impossible to be 100% secure, but that there is always room for improvement, and even a need to continue to assess and improve based on new risks.

Some businesses, especially smaller ones, were not certain what needs to be in place for them to feel completely cyber secure, or what can be done without the costs being too prohibitive.

Investing in cyber security is for the most part seen as an accepted and necessary cost of doing business, and as something that is not a one-and-done item on their expense list. It is often both something that is looked at on an ongoing or regular basis, and something that gets more attention and investment as the need arises, whether that is related to new circumstances (e.g., more employees working from home) or due to threats or security breaches. Some, especially larger businesses, have internal staff who take care of IT and cyber security, while others rely on external contactors for these functions.

While external cyber attacks were certainly on people's minds, it was often said the extent to which they felt secure was directly related to the behaviours of its own people, and how confident they were that their staff takes security seriously and follows all rules and protocols. While some say that they trust that staff do not "click on every link they get" and report any potential threats or breaches, others say that since hackers are getting more creative and sophisticated, the risks of human behaviour on their company's vulnerability is always something to be worried about.

Changes due to pandemic and ways in which companies adapted

Nearly all participants agreed that they had increased their online presence as a result of the pandemic and that they have become more internet-dependent. The most common forms of adaptation included introducing or increasing remote work and, with that, greater dependence on videoconferencing platforms such as zoom, google meet or Microsoft teams. It was also mentioned that some staff who were previously not typically required to use much or any technology, for example those who would do on-site visits or worked in warehouses or plants, had to adopt to using technology to try to replicate in-person client or supplier interactions, and that on-the-fly training was often required.

Some also saw an increase in e-commerce activities.

The mere fact that people were working from home and using their own internet connections rather than the one in a corporate office, often brought with it the sense that there was automatically less cyber security and less control over what was done online.

Many participants who experienced an increase in remote work reported that their businesses had pre-existing systems and technologies in place. Nearly all businesses with more remote workers explained that they needed to make adjustments to accommodate more remote workers and to try and ensure this was done in a secure manner, including:

- ramping up their hardware (for example ensuring everyone had a laptop or phone, ensuring enough server capacity);
- ramping up their software (for example VPNS, virus protection); and/or,
- increasing bandwidth.

Some mentioned that additional training had been necessary for those newly working from home, including training on how to be cybersecure at home. In general, there was a sense that since the beginning of the pandemic, staff have become more aware of the importance of their own responsibilities and behaviours when it comes to using technology and online resources. However, it was also understood that ongoing training or providing "reminders" was likely necessary.

Most believe they have made the transition to an increased online presence in a relatively secure manner. One of the greatest risks remains users, often their own employees, rather than the technology that they use, prompting many to believe that there is a need for ongoing employee training in this area.

In almost all sessions, there was one business sharing that, since the beginning of the pandemic, their business had been cyber attacked. Most others indicated that they knew of other businesses being cyber attacked. Another aspect that was raised by many was the significant cost implications of these attacks, both in terms of system changes and upgrades needed post-attack but also in terms of hours of production that were lost due to an attack. Others mentioned that their systems were constantly facing threats and attempts, or that they noticed an increase in spam being blocked, but that they had been able to keep it all at bay.

None of the businesses were surprised to hear that the number of cyberattacks had increased since the start of the pandemic.

A few participants said that their customers were asking more questions about the security of their systems, but this was not a general theme. The shift to more e-commerce was again only mentioned by a small number of participants.

Reactions to advertising concepts

Participants were shown three different advertising concepts and were informed upfront that the advertising was to increase awareness among small and medium sized businesses of a cyber security certification program launched by the Government of Canada. Each concept consisted of one print ad, one banner ad (video format) and one short online

video. The presentation and discussion order of the three concepts varied from one session to the next.

There were various overarching themes that emerged when discussing all concepts. These included:

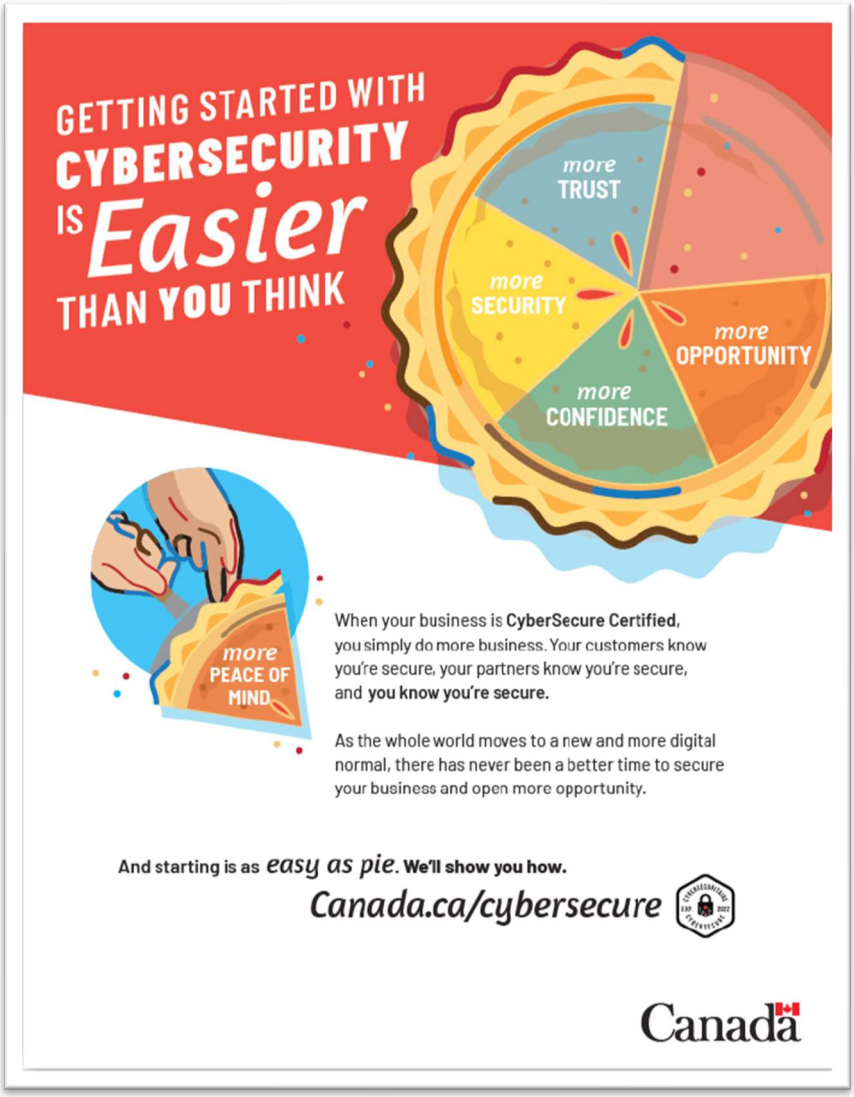
- Participants were often looking for a more direct, literal connection to cyber security in the creative approach. Participants often initially referred to wanting to see computers, shady-looking characters, darker tones, protected vaults, etc., although there was also some sense that these would be cliché and might not get their attention. As some of them explained, they do not have time to decipher metaphors to figure out if something is geared to them or of interest to their business and prefer ads that are straight to the point. In this case, using words like "secure," "IT" or "protection," along with more literal imagery, would go a long way in achieving this. While there was interest in a more serious and direct approach to cyber security, there was some reticence to having ads that are overly fear-based.
- The program seal should be more prominently displayed in the ad concepts and appear early on and larger. Linking back to the idea that many participants wanted the ad to be more literal in its depiction of security, the seal with the lock was often the only image that aligned with this expectation.
- They do not believe the ads need to convey how important an issue cyber security really is as they believe that they and their peers understand that already.
- While most participants agreed that the concepts would catch their attention in some way, this did not necessarily translate into wanting to read the full ad or sit through the entire video. For self-proclaimed "busy people," participants explained that the first impression of an ad goes a long way to determining relevance and ultimately if they will read the full ad or watch the full video. There needs to be a clear hook right at the beginning of the ad, or at the top in bold letters, that grabs their attention with information that compels them to find out more, whether that is by watching or reading the rest of the ad, or by clicking through on the link provided. On the other hand, some did feel that the look of some of the ads was so different from what they typically see, that they would read it out of sheer curiosity.
- The information on the ads begged questions, and often made participants interpret the certification program as being a course they would be able to take.

While it was explained that the idea was for people to get a “teaser” in the ad and that more information would be on the website, the issue often became that there was either no interest in a course, or that the execution of the concepts would not compel them to actually find out more, leaving them with a misconception that would have been corrected by visiting the website.

- Participants would not only prefer a straightforward message, but also a clear identification of the sponsor and of the target audience, and an easy-to-identify call to action. It was suggested that it could be along the lines of “the Government of Canada wants Canadian small businesses to be cybersecure. We have a new certification program that helps you with that. Click here to find out how.”
- The Government of Canada wordmark should appear sooner in the video concepts rather than at just the end. Many believe they will not watch the video until the end since their first impressions would lead them to believe that the ad is for yet another cyber security company selling their software, or as in the case for concepts a (easier) and b (first step) in particular, ads for something unrelated to cyber security altogether. To further increase credibility and trust, participants also suggested that the wordmark be more prominent by making it, for instance, larger or more prevalent.

Following are detailed findings from the discussions of each of the advertising concepts.

Concept A – Easier



Focus groups in Saskatoon/Region, Winnipeg and Calgary/Edmonton and Vancouver were additionally shown a mockup of how this concept would appear in an online newspaper, such as *The Globe and Mail*.

Overall, this concept was not very well-received, and it was the least preferred of the three concepts tested.

Initial reactions often revealed that this concept led to some confusion as to who the actual **target audience** was. For many, it did not feel to be targeted towards a business audience, but rather to consumers. The idea of "getting started" made some comment

that if it were for businesses, it would be for startups or young entrepreneurs just entering into the market – companies that had not yet invested much in cyber security. On the other hand, and seen as contradictory to that idea, the vintage look and feel was said by some to be geared more to an older generation. As well, the repetition of the word “more” in the pie slices suggested to some that it is for companies who are already doing something but want to or need to invest or do “more,” rather than for startups.

The **content,** while somewhat appreciated and sometimes said to be the only thing that mattered, appeared to beg more questions than it provided answers, whether about the purpose of the ad or about the certification program. Even when it was explained that the point of the ad was to draw people in and to have them find out more by going to the website listed, this was not seen as an overly effective ad because most say they would not be compelled to find out more based on their first impression.

Creatively, while it was often felt that the colours were eye catching and that there was perhaps some merit to the idea of the pie with the various sections with security-related text, the concept tended to fall flat. The pie imagery was the main reason participants said it did not appeal to them as business decision-makers. In addition to the overarching idea that the creative appeared to be geared towards consumers, at first glance, some specifically said they would assume it had something to do with selling them pie or baked goods or a recipe, which was not something that would draw them in. Moreover, the quality of the execution was sometimes referred to as amateurish, childish or “clipart” and not as professionally done as one would expect from the Government of Canada. The execution took away from the message that people should trust or feel secure with this certification or this program.

One of the **main messages** gathered from this ad was based on the headline, implying that cyber security was easy (or easy as pie), which was not a premise most agreed with. Others said that the main message was about getting a certification and therefore getting more business. Many felt that the message was lost in the somewhat cluttered execution and that it would require reading the smaller print or intently watching the whole banner sequence or video in order to gather more information. While in general, participants felt that there was useful and interesting information in the smaller print, due to the issues with the execution and the overall sentiment that they would not be compelled to pay it much attention after the headline or the first frame, getting to that main message was unlikely to happen. The reference to “peace of mind” was mentioned as a positive and fitting message.

The Government of Canada logo made virtually all participants **understand that it was a Government of Canada** ad. A few wondered whether there was a third party involved with the certification because it was not necessarily clear to them how it would be rolled out.

The **call to action** was for the most part understood as getting people to find out more by clicking on the link. However, due to the weak execution, most said they would not be compelled to do so.

Concept B – First Step

Focus groups in Saskatoon/Region, Winnipeg and Calgary/Edmonton and Vancouver were additionally shown a mockup of how this concept would appear in an online newspaper, such as *The Globe and Mail*.

This concept received mixed reviews and was usually selected as the second-most preferred option. A small number of participants ranked it as their top choice. However, as was seen with concept a, there was some critical feedback, particularly when it came to the overall execution and to the assumed target audience for this ad. Moreover, the ad was not necessarily immediately recognized to be focused on cyber security certification, but rather at first glance seen as an ad for sneakers or for a job program, community program, fitness program, children's shelter or college program.

Some suggested that they did not feel the ad **targeted** them but that it was rather geared towards a younger audience such as college students. Not only was this derived from the overall sneaker theme and the general creative approach, but also from the message about "the first step." It was said that this felt to be targeted at (smaller) startup companies that had not yet waded into the area of cyber security, rather than their more mature companies that have been dealing with this issue for a long time. Some said that "the first step" was taken decades ago with the introduction of the internet.

However, others understood the **main message** to be encouraging companies to take the first step towards certification (rather than the first step towards addressing cyber security in general). This was seen as a more compelling or fitting message and one that would more likely inspire them to act. The idea of having to take action in order to become cybersecure, that companies would have to "move toward" rather than it being served to them on a silver platter was also appreciated. In general, the text content of the ad was appreciated, especially the layered approach in the banner ad and in the video. However, some again felt that there was key information lacking, which confused them.

The **creative approach** was said to be eye-catching and most said it would grab their attention at least somewhat. The writing on the shoe was hard to read for many and gave the ad a cluttered feel. As the general messages on the shoe were appreciated, there was a call to somehow convey those messages in another way. Some said that the overall approach lacked the seriousness they associate with the issue of corporate cyber security.

The **call to action** to click on the link to find out more was understood. However, not every participant said they would likely follow through on that since they did not necessarily feel that the program or certification was geared to them. On the other hand, some said that the information provided was interesting enough for them to go online

and try to get answers to questions that came up for them when seeing or reading the ad.

The **Government of Canada logo** was noticed and mentioned as giving legitimacy to the ad and to the certification. It made some more receptive to the idea of certification; others said that without the logo, they would assume this was from a private business.

Concept C – Trust

Focus groups in Saskatoon/Region, Winnipeg and Calgary/Edmonton and Vancouver were additionally shown a mockup of how this concept would appear in an online newspaper, such as *The Globe and Mail*.

This concept was by far the most preferred of the three concepts. This did not necessarily mean that it was a perfect ad, but that it stood out among a collection of weak concepts. The main reasons that this concept was almost always selected as the winner, were because it had the most relevance or direct tie to cyber security, and because of the use of the "trust" theme. This concept was the most likely to get participants to click the link and want to find out more about the certification.

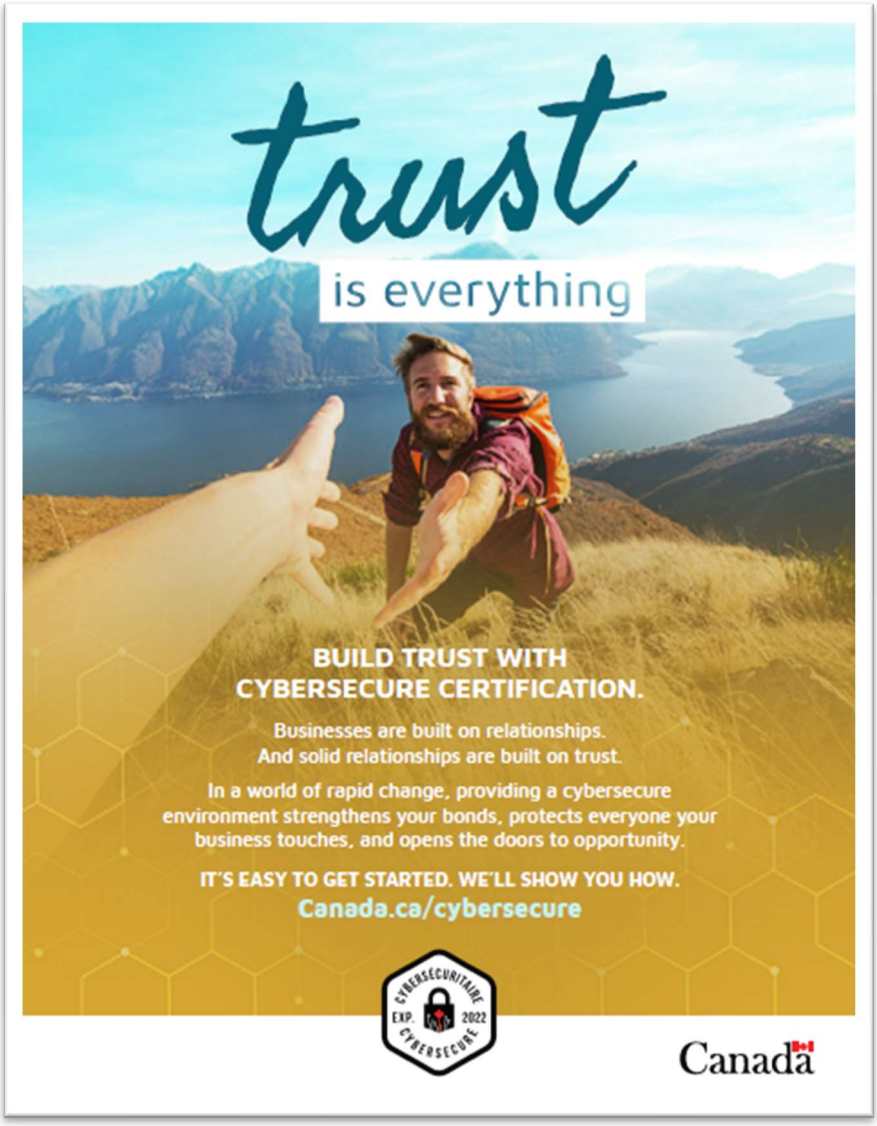
This concept was also more often felt as being **targeted** towards a broader business audience. This was mainly because of the more serious tone overall, compared to that struck by the other two concepts. It was said to "speak my language" and be less "consumerish" than the other two.

The **creative approach** was considered eye-catching and well executed. The theme of the bees, in a chain working together and "all being in it together" was clearly conveyed through the execution, and clearly linked to the main message of the ad. Some also made note of the background imagery of the hives and how it reminded them of "network connections." However, some questioned the link between bees and cyber security, while others who felt a general aversion to insects or bees mentioned that using people in the ad instead would make it more attractive to them.

Some felt that the video was too slow in conveying what the ad was about, and that they likely would not have watched to the end to find out.

The **main message** of trust and of "trust being everything" was easily identified, and generally liked in the context of cyber security. The idea that trust could easily be broken by having one weak link – whether that be a bee or a team member in a company or a weakness in an IT system – also resonated with participants. Cyber security was seen as something requiring a strong network, whether that be internally or externally throughout the supply chain. The idea of building relationships and getting more business if a company was more cybersecure also came through.

The **call to action** to learn more and to go to the Government of Canada website in order to become certified was for the most part easily understood by participants. Due to the use of the logo, the **Government of Canada** was usually easily identified as the sponsor of the ad.



This alternative advertising concept was produced in English only for the last four focus groups held, including the Saskatoon/Regina Region, Winnipeg Region, Calgary/Edmonton Region and Vancouver Region groups.

The revised concept received mixed reactions and was by and large seen as weaker than the execution with the bees.

For some, the general idea of depicting a human rather than insects was a welcome change, and the picture was seen as more relatable and "nicer to look at." The message of trust in the text was once again appreciated, but not everyone saw the stretched-out hand immediately, making them wonder what the link between the image and the trust

message really was. As well, the individual did not necessarily appear to need a helping hand, as he was not seen to be in an overly precarious position. As some participants said - he is not falling off a perilous cliff, he is just having a nice hike in a beautiful setting.

There was some concern that the image reminded them more of an ad for tourism portraying freedom and exploration, rather than for anything related to cyber security or even building trust and relationships. This would compel them less to read on or try to find out more.

Advertising placement

Some of the groups were asked where ISED should place the ads in order for them to be seen by their target audience.

Ideas shared were:

- News websites (such as CTV, CBC, CNN, La Presse, Le Monde, Globe and Mail, Msn.ca)
- Financial or business news websites (such as Forbes, The Economist, Business Insider)
- Technology websites
- Government of Canada pages (such as CRA My Business Account, other business program pages) or provincial government pages
- Chamber of Commerce website
- Professional association websites or online magazines (such as CPA Magazine)
- Trade websites or magazines (such as Investment Executive)
- Social media (such as LinkedIn, Facebook, Twitter, Instagram)

Reactions to the Cybersecure Certification Program

Before discussing the program, participants were asked whether they remembered the name of it from the ads they had been discussing. In each group, one or more participants remembered, while many others were not sure or guessed something that was not entirely correct.

The following description of the program was presented to participants:

> **The Cybersecure Canada certification program is a voluntary cyber security certification program implemented by the Government of Canada.**
>
> **Certified businesses are required to implement 13 security control areas that cover a wide variety of vulnerabilities for small and medium organizations such as employee training, password protection, incident response plans and more.**
>
> **These control areas were developed by the Canadian Centre for Cyber Security, Canada's cyber security experts specifically for small and medium organizations.**

Prior to participating in the focus group, none of the businesses were aware of the new program.

Based on the summary description provided, nearly all participants were interested in finding out more about the program and many believe they would consider or set time aside to get certified.

While most participants believe that the certification would be "good for business" and would not have any draw backs, it was still not always explicitly clear what would be in it for them and how it would help their business. Some wanted to know for example whether they could take the certification to their insurance company and get a break in their liability insurance (as they knew some international certifications that do). Being able to use the seal on advertising collateral was seen as a benefit. Some felt that if all else was equal, companies would be compelled to choose a partner or supplier that had the certification and "showed the logo" over those that don't, and that this would therefore potentially give them a leg up on the competition.

Based on the information shared, it was not always easy for participants to assess how the certification could improve their cyber security. However, there was a hope that it somehow would, or, at a minimum, it would assess how it could be improved or confirm that they were already doing everything "right."

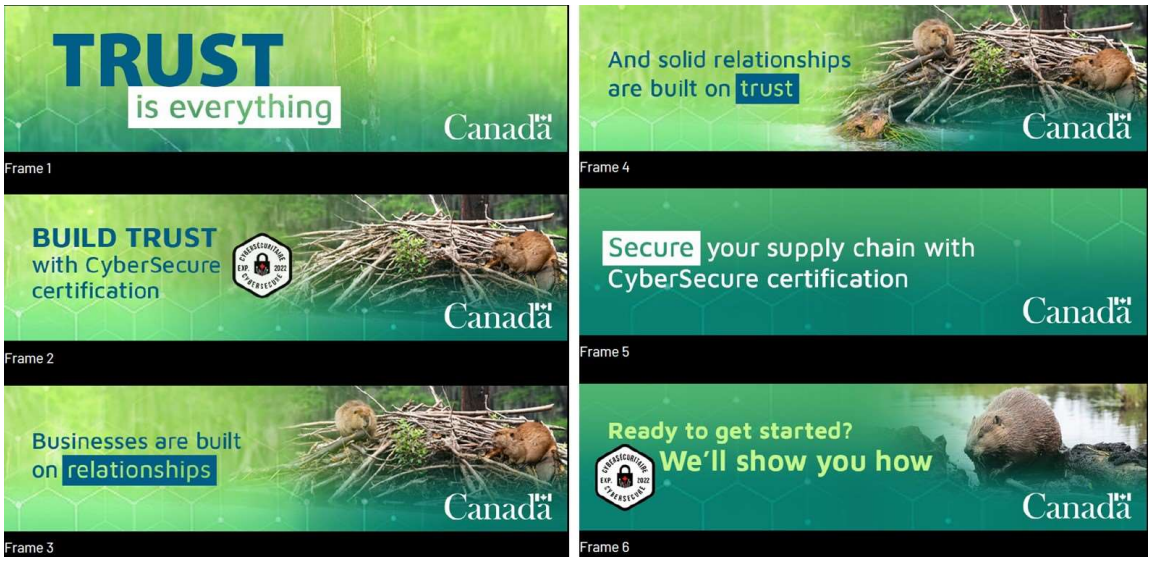
Those interested in the program believed that if the certification process revealed a need to make changes in order to be more secure, they would be prepared to invest in software, hardware, or company training. However, some indicated that there would be a limit to how much they would be willing to spend to get certified if they felt that it would not really make them that much more secure.

The reference to the Canadian Centre for Cyber Security was very reassuring to many, and it was mentioned that this might be something worth including in the advertising to help create legitimacy.

Phase 1 focus groups - Success check

After the first round of focus groups, two additional discussions were held (one in English and one in French) to test two revised advertising concepts that were created based on feedback from the initial round and the overall preference for the "trust" concepts. These were presented to participants as online banner videos. During the discussion, the sequence of frames was kept on the screen to help participants remember the content of each frame in the banner video.

Concept A – Beavers



This concept received mixed reviews.

In general, the overall message was understood, although there were some questions about how to go about getting certified. Some believed it was a course, others were not sure. However, it was clear for most that they could go online to get more information about the program and that questions would likely be answered online.

There was some debate about whether the mention of the supply chain (frame 5) was relevant to everyone, or whether that was really a pertinent part of the information. Some felt that it may turn off those who do not have a supply chain or do not feel that that is important to their business, and that that frame might be better used to explain a bit more about the program itself. For example, it was said that companies can really only secure their own business and can only control their own staff's behaviours, and do not

have an influence on other parts of the supply chain – unless it becomes a mandatory certification. Others said that they had not noticed this reference and that it did not take away from their understanding or the call to action to go find out more.

Those who liked it, pointed to:

- The creative execution using the beavers working together, and the sequencing of adding beavers, going from one to three, which tied into the themes of trust and relationships;
- The visual of something strong being built;
- The honeycomb in the background that signifies inter-relationships, cohesion, and is relatable to (cyber) security;
- The font and use of colours add to the seriousness of the message;
- The prominence of the word "trust," which is key in both relationships and feeling (cyber) secure;
- The logical buildup of the story to "we'll show you how" and the call to action;
- The certification seal showing up early on, (in the second frame) and its position prominently in the middle of the banner; and
- The use of the beaver, which is seen as a true Canadian symbol and related to the Government of Canada.

Those who did not like it as much, offered that:

- They did not connect the beavers with cyber security or with anything that should be considered a threat – instead, they were said to be "cute," which is not very relatable to the serious issue of cyber security in their view;
- There was no connection to people or IT systems in any of the imagery;
- The nature setting was jarring;
- The execution overall did not appear to be geared towards them or to business decision-makers in general and they would not be likely to follow up and look for more information;
- Given the prevalence of ad blocking technology, a few felt an advertising approach that was based on website advertising would not get through to them and that a multi-channel approach is warranted.

Improvements suggested were:

- To add the URL to the last frame so that people could easily click for more information;
- To add the seal to the first frame to draw immediate attention to it;
- To have visuals that are more literal in their connection to cyber security, such as computers "talking" to each other, people working or on social media; and
- To change some of the colours to be more attention-grabbing. The use of red was offered as an example, even if just in the Government of Canada logo / flag.

Concept B – Trust Chain

This concept also received mixed reviews, with the creative execution in particular polarizing participants.

Those who liked it, pointed to:

- Its literal depiction of people working together, of human relationships and of a human "chain";

- The diversity of the people and how they depict different parts of a supply chain or of different businesses or sectors being related and working together;
- The Government of Canada logo adding trust and legitimacy;
- The use of a superhero cartoon execution, which is different from most ads and is attention-grabbing, making them watch for what's next and making them want to find out more information; and
- The focus on the word "trust".

Those who did not like it as much, offered that:

- The cartoon execution and the general tone fell flat and showed disregard for the serious nature of the topic of cyber security, and for some also brought into question the legitimacy of the program altogether;
- It did not have a standard Government of Canada feel that would draw people in or that would give them confidence that this was something they should look into further;
- It was not seen as geared towards all business decision-makers in general, but instead would likely only draw in younger entrepreneurs with startup companies;
- The program's seal showed up late in the sequence; and
- The fact that the people were wearing masks was confusing and not understood, given that this program would continue to exist beyond the current pandemic. Some felt that their attention went to the masks and they were looking for a link between health or protection from COVID-19 and protection from hackers or cyber security overall, which was not there;
- Given the prevalence of ad blocking technology, a few felt an advertising approach that was based on website advertising would not get through to them and that a multi-channel approach is warranted.

Improvements suggested included:

- To depict real people instead of cartoon characters;
- To remove the masks;
- To show the seal earlier on in the ad; and
- To add the URL at the end, both so that people could easily click on it and to add legitimacy and trust that this is actually a Government of Canada ad and certification offered by the Government of Canada.

Phase 2 results – Stakeholder in-depth interviews

For this phase of research, two different types of stakeholders were involved and as such, two different lines of questioning were required. Those representing industry groups or associations were asked about the importance of cyber security to their industry in general, the impact of the pandemic, the industry's readiness and what needs to happen for the industry to improve on this front. Those representing private sector businesses with sizable supply chains were asked about their own organization's state of readiness in terms of cyber security, the impact of the pandemic, and various questions about procurement and how they view supply chain cyber security readiness.

Both types of participants were asked the role they see for the Government of Canada, although industry representatives were asked to focus on their industry vertical in general whereas private sector participants were asked to focus on their supply chain specifically.

Finally, an overview of the Cybersecure Canada program was provided. All participants were asked if they had previously heard of the program and, given the brief overview, what their initial thoughts were on the program. Industry representatives were also asked whether this type of program would be useful to and used by their industry, whether it might have an impact on their industry's overall level of cyber security readiness, what barriers to adoption might hinder enrollment in the program, and what role they see the Government of Canada playing in relation to the program. Private sector participants were presented with fairly similar questions but were asked to focus on their supply chain specifically.

Cyber security readiness

In terms of cyber security readiness, few businesses feel they, or that businesses in their industry, are completely protected. There is a consensus that at least some aspect of their approach or their system can be improved upon. Even the most sophisticated enterprise was reluctant to give themselves a perfect score on this front.

This research suggests that businesses across the various industries span the spectrum of cyber security readiness - some of the industries appear to be performing better than

others. Furthermore, certain businesses are performing better than others within each industry.

This research also points to various factors that contribute to a state of cyber security readiness, in particular the following:

- The data intensity of the industry was a key driver – the more a business or an industry relies on and/or generates data, the more likely they are to believe they are performing relatively well in terms of being cyber secure. The relationship between the importance of data and the relevance of cyber security was evident in industries such as specialized healthcare services and market research. Representatives from these industries explained how cyber security is an ongoing concern, and significant resources are used to maximize their level of security. It is also in these same industries that significant amounts of data, including significant amounts of personal data, are managed. A representative from a different industry explained how cyber security is a growing concern in their industry, mostly because the businesses in that industry are becoming increasingly data intensive.

  The relationship between data intensity and cyber security readiness is not perfect and an interesting paradox exists in some industries. Some businesses do not view the data they own, manage or generate as "sensitive" in nature and as such do not feel cyber security should be the highest priority. As well, one industry representative explained how businesses in their sector (healthcare practitioners) manage significant amounts of personal data however the perceived level of cyber security readiness is relatively low. For this particular industry, owners and operators are not being neglectful or underestimating the importance of the data they manage – in fact they place a premium on privacy. However, other business activities, such as delivering healthcare ("taking care of their patients") take precedence, and other factors, which are described below, limit their ability to fully secure this data.

- Many also agreed that scale was a key factor in how well a business or a vendor performs on cyber security. All participants acknowledged that the larger the business, the more likely they were to be cyber secure given the fact that they had resources dedicated to managing their IT systems, something which typically becomes increasingly scarce as the size of the business decreases. This was also acknowledged by large businesses with sizable supply chains – they either know

or have a strong sense that their larger vendors are better equipped and staffed to manage cyber security. Scale becomes a particular concern for very small and microbusinesses where the business owner/operator is almost entirely focused on revenue generation, which is the case in the healthcare industry where there are thousands of very small offices run by healthcare professionals whose primary focus are their patients. Their area of expertise is healthcare, and their top priority is seeing patients whereas running a business, including the associated IT systems, is quite secondary. This was especially the case during the pandemic.

- Another barrier that impedes businesses from maximizing their cyber security readiness is cost, or at least perceived cost. As busy as some businesses might be, it was said that revenues cannot sustain a dedicated IT resource even though significant amounts of data are being managed. As well, certain business operators would say that they cannot afford more robust or modern IT systems, which, for some, would mean a significant investment in their business.

- Industry representatives explained that even if businesses in their industries wanted to improve their level of cyber security, a variety of knowledge gaps exist:

    - They do not have foundational knowledge of IT – for example, the basic concept of a data back-up is not universally understood,

    - They would not know where to start,

    - They would not know what software or hardware would be needed, and,

    - They would not know what to do to ensure continuous and sustained efficiency in cyber security, including staying on top of new technologies, processes and threats.

- For many businesses in certain industries, there is little to no customer expectation, industry standard or government regulation that requires that a minimum threshold of cyber security is maintained. As such, these businesses essentially self-regulate when it comes to cyber security. Exceptions are in the data intensive industries, such as the market research industry where companies get pressure from both clients and from industry groups and associations.

- Competitive differentiation is a factor but not universally. In certain industries, data management is table stakes, such as in the market research industry. In

other industries, such as in healthcare and vehicle repair and maintenance, clients do not tend to choose a supplier based on their ability to manage their data. Given the growing importance of data in the vehicle repair and maintenance industry, the ***possibility*** that data management could become a competitive differentiator is quite real. On the other hand, representatives from the healthcare industry (notably primary care) explained that any argument that positions cyber security as a competitive differentiator would be in vain since primary care physicians and hospitals are not really operating in a competitive environment. It should be noted that for this research the healthcare industry group was mostly focused on the public healthcare system and not private care providers or allied healthcare providers such as dentistry, physiotherapy, etc.

The pandemic appears to have had a range of impacts on the various industries involved in this phase of the research. In many cases, it has precipitated the use of technology and forced many businesses to use technology in ways they did not before (e.g. Virtual care for healthcare practitioners, telework, new online systems for e-commerce, etc.). Some of these initiatives were done securely while others were patchwork.

The pandemic also forced businesses to focus on staying open and staying healthy, which may have relegated maintaining or upgrading IT systems to the backburner in the short term. That said, the need to roll-out certain new systems, such as those related to e-commerce, has moved the discussion around cyber security to the forefront for others and forced them to achieve in a few months what might otherwise have taken years.

Supply chain considerations

The discussions with large enterprises on supply chains revealed two fairly different approaches to supply chain management when it comes to cyber security. These discussions were not intended to reveal how common each approach is across Canadian enterprises but rather aimed at discovering the range of perspectives and priorities as they relate to supply chain management and cyber security.

The approaches for each type of business are summarized in the following grids:

IT structure and resource allocation

Manufacturing	Specialized healthcare
Have resources and staff dedicated to IT and supply chain management.	Have resources and staff dedicated to IT and supply chain management.

Types of data managed and approach to data management

Manufacturing	Specialized healthcare
Types of data housed: manufacturing processes, operational data, staff-related data, supplier-related data, customer-related data. Views their approach to data management as limited to their own data. Their priority is the data that they house, and they are not concerned with what data their suppliers manage or how that data is managed. They do not consider a vulnerability in their supply chain as a vulnerability in their own level of cyber security. There is no clear sense of how well their supply chain was able to adapt during the pandemic or how resilient it has been. Nor do they have any clear sense of whether the pandemic has exposed or introduced any cyber security vulnerabilities or challenges among their suppliers which have also had an impact on their company.	Types of data housed: operational data, staff-related data, supplier-related data, customer-related data. Considers their data infrastructure as complex requiring sophisticated systems and processes to ensure continuous protection and integrity of this data. They collect and house significant amounts of personal data from the general public and as such they take the necessary steps to maximize the protection of that data from as many perspectives as possible, including how their suppliers collect and manage their data. They view their suppliers are an integral part of their overall data management plan and strategy. Similarly, their overall sense of feeling "completely protected" takes into consideration their supply chain. In fact, for this company, the greatest source of concern is the integrity of their supply chain. They feel fairly confident that they understand the extent to which the pandemic may or may not have had an impact on their supply chain. There is a sense that although their supply chain may not have been impervious to the increases in cyber attacks during the pandemic, it has remained fairly resilient.

Supply chain data management requirements

Manufacturing	Specialized healthcare
Cyber security is not a procurement consideration in the selection of suppliers nor is it an ongoing concern once a supplier relationship is established. Suppliers are not asked to provide any information on the integrity of their IT systems or the processes or safeguards in place to ensure cyber security. Even if they wanted to begin doing this, they would not know what to ask for. Given that many	The level of cyber security of suppliers is embedded into the procurement process and determines in some cases which suppliers are used. Situations surface when a supplier is preferred by project managers irrespective of their level of cyber security which does put some strain on procurement. If a supplier is selected and cyber security levels are not a criteria, post hoc

of their suppliers are international, they are not certain how they would be able to verify or reinforce any cyber security requirements. The discussion around supply chain vulnerabilities did seem to make this participant realize how important it would be to take a closer look at how cyber security vulnerabilities in their supply chain could have an impact on their own operations and that perhaps this needed to be woven into their risk management strategy.	efforts are made to verify and maximize the level of cyber security of these suppliers. This company has developed its own verification/audit process that a supplier must complete. Through this process, specific metrics and reports are obtained to establish the level of cyber security of their suppliers. This audit process ensures some degree of consistency in terms of the types of information they obtain from suppliers. Although this process is rigorous and closely followed, there is no onsite inspection or remote verification of supplier systems. As such, in the absence of standardized and industry-recognized IT reports, they can only trust what their supplier does and tells them about their level of cyber security.

Role of Government of Canada in cyber security

Participants agreed that the Government of Canada, and in some cases also the provincial government, has a role to play when it comes to supporting small and medium-sized businesses to become cyber secure. The following types of roles were specified:

- **Inform, educate and train:** appreciating the significant knowledge gaps that exist among many businesses in their respective industries, it was suggested that the federal government should provide information, education and training on cyber security, including the relevance of cyber security to their business and what steps need to be taken to address, maximize and manage cyber security. Best practices could be provided. Along these same lines, there was interest in having the government provide a list of preferred or recommended suppliers, including hardware and software providers and IT consultants who could advise businesses on cyber security. In the absence of this, perhaps they could provide advice to businesses on what criteria they need to consider when selecting an IT vendor.

- **Support and incent:** it was suggested that the government provide greater financial incentives to small and medium-sized businesses. This was proposed mostly out of a concern that even if businesses are more aware of cyber security, they may still not make the appropriate investments in their systems to effectively improve their level of cyber security.

- **Setting standards:** to ensure a consistent approach across the country, it was proposed that the Government of Canada develop some sort of set of standards to which businesses could refer. Unaware of the Cybersecure Canada program, one participant proposed that the federal government develop some sort of national certification program. It was also mentioned that any effort to create a set of standards should be done in consideration of what is being done in other countries. Insofar as they would want Canada to be at the forefront of this sort of activity, they would want to avoid a situation where the standards hinder global competitiveness of Canadian companies.
- **Greater efforts to combat cyber criminals:** while supporting businesses in their efforts to become more cyber secure was important, it was also suggested that the government do more to combat cybercrime.

None of the participants actively proposed that the Government of Canada make it mandatory for businesses to have in place some level of cyber security protection or proof of diligence. When asked whether this might be a possible approach, participants voiced a range of opinions, including potential advantages but also some concerns.

Appreciating that cyber security is an issue and has become increasingly important during the pandemic, any effort to improve how Canadian small and medium-sized businesses perform on this front is a good idea. The spirit behind the requirement is understandable and is in many respects warranted. Those with sizable supply chains also voiced how this sort of requirement would make it easier for them to assess the level of cyber security of their suppliers and it would make them more confident in their supply chain.

Inasmuch as industry group representatives and enterprises with large supply chains like the idea of making it mandatory for businesses to have in place some level of cyber security protection, all participants also had some concerns with this approach. First, they would want the requirement to be seen as a support rather than a punishment or an additional burden. Participants explained that the government cannot make this a requirement without providing some sort of financial support to help businesses meet the requirement. Specific concern was raised for small businesses, many of which do not have the same types of resources as medium and large companies to oversee their IT systems.

There were also concerns about how this sort of requirement could be enforced, that oversight alone might prove overly cumbersome for the government to take on, and that this requirement may in some respects represent excessive government oversight on the private sector. It was also suggested that this sort of requirement may not be needed for all types of businesses across the country, and that, instead, it should only be required of businesses that collect or manage certain amounts or types of data.

There was also a concern in terms of how this type of requirement might or might not apply to international suppliers. There was some uncertainty over the ability of the Government of Canada to enforce this requirement on businesses located outside of Canada. Furthermore, even if they tried to enforce this requirement internationally, there were notable concerns about how this might make international suppliers more reluctant to do business with Canadian buyers. While these suppliers might be very important to Canadian companies, in the global context Canadian companies may not represent an important proportion of their revenues and as such, they may not think twice about abandoning those relationships if excessive requirements are introduced. Finally, there was a concern that this requirement may make Canadian businesses less competitive on the international stage if it increases their costs of doing business.

Reactions to the Cybersecure Canada program

The following overview of the program was provided to each participant:

The Cybersecure program is a means for SMEs to demonstrate that they are taking appropriate measures to protect their systems, build in resiliency in case of any attacks, as well as safeguard their customers and contractors' information.

To be eligible for certification, the organization must review and implement the 13 security controls established by the Canadian Centre for Cyber Security:

- Develop an incident response plan
- Automatically patch operating systems and applications
- Securely configure devices
- Enable security software
- Use strong user authentication
- Provide employee awareness training
- Back up and encrypt data
- Secure mobility

- Establish basic perimeter defences
- Secure cloud and outsourced IT services
- Secure websites
- Implement access control and authorization secure portable media

A certification body (accredited through the Standards Council of Canada) will evaluate the businesses' implementation of the 13 security controls. The certification body consults directly with each organization to:

- Determine if the organization is ready to be certified;
- Provide a cost estimate for the organization to achieve Cybersecure certification; and,
- Audit the organization's implementation of the security controls.

Once a business obtains the Cybersecure certification, they are certified for two years and have the option of displaying the certification mark on their websites, storefronts, and promotional materials.

Awareness of the program was moderate. One of the industry associations that was familiar with the program had discovered it while developing the accreditation program for their own industry group.

Based on the overview provided, interest in the program was high. Industry representatives felt that this type of certification program would be beneficial to their "members" and to their industry overall. They would see themselves promoting the program to encourage enrollment. The representative from a market research association has been developing their member accreditation program and is keen on finding a way to conduct third party audits of members. Their audit process would be more far-reaching than member's IT systems and their level of cyber security, but if a member were to be certified, it could simplify or streamline the audit process for that member. Furthermore, the program might seem more feasible for many of their members since alternative types of certifications (e.g. Iso) are expensive.

Those with large supply chains also agreed that this type of program would make a difference. While they would not see themselves making the certification a requirement for their suppliers, they would see themselves recommending the program.

Participants felt that the program was fairly comprehensive and appropriate for a cyber security certification. The specialized healthcare business with a large supply chain felt that the certification aligns very well with the types of items they look at when assessing their suppliers' level of cyber security.

There were a few concerns raised about the program that largely mirror the concerns voiced earlier when discussing the challenges businesses currently face when trying to tackle cyber security. In particular, few would have the in-house expertise to take on this type of certification. As well, participants felt that businesses are not sufficiently acquainted with the concepts described in the overview, let alone the technological requirements involved to meet the certification requirements. Finally, even if they were to follow the certification process to understand their most important gaps, they are not convinced that businesses in their industry would be able to afford the infrastructure needed. Some suspect that the gaps may be quite significant for many businesses in their industry and that the recommendation list would be both overwhelming and too costly.

A few of the industry group representatives had programs or audit processes that touched on cyber security. Based on the overview, they felt that the federal program would complement what they already have in place and largely aligns with the types of outcomes they are looking to achieve through their own initiatives. That said, industry groups would welcome the opportunity to collaborate with the federal government to make sure that the certification requirements take into consideration the unique needs of their specific industries. There is some concern that an effort to have an approach that suits everyone ends up not being sufficiently specific to address the needs of anyone.

One participant was concerned that the program's focus on small and medium-sized businesses might suggest that the certification is "light" or simplified to accommodate the smaller tiers of Canadian businesses. They felt that if larger companies were also certified, it would bring a lot of credibility to the program and the resulting certification.

Finally, there was interest in making sure that the certification does not become a "checkbox" activity or a one-off. Rather, ongoing training, engagement and certification renewal needs to be built into the process for the certification to have any meaningful success in the long term.

Detailed methodology

The research methodology consisted of 10 online focus groups and 6 1-on-1 web-assisted depth interviews. The focus groups were conducted with Canadian small to medium enterprises (SMES) with a focus on the larger-small organizations (those with 40+ employees). These sessions spanned the country in large and medium cities, as well as in rural and remote areas. One-on-one web-assisted interviews were held with a range of large enterprises and industry groups and organizations / associations (e.g., professional industry associations, business associations, etc.).

Quorus was responsible for coordinating all aspects of the research project including working with ISED in designing and translating the recruitment screener, email invitation scripts and the moderation guides, coordinating all aspects of participant recruitment, managing the online interviewing platform and related logistics, moderating all sessions and interviews and delivering required reports at the end of data collection. The research approach is outlined in greater detail below.

Target audience and sample frame

The research consisted of two broad segments of the business community:

- **Target population 1 – Canadian small to medium enterprises (SMES):** this group consisted of Canadian SMEs and not-for profit organizations, with a focus on the larger small organizations (those with 40+ employees). Within this group, the research targeted a cross section of business types of interest to ISED, including those part of a supply chain, those in manufacturing and those who have adopted a digital online model during the pandemic. Within each organization, the research targeted a decision-maker regarding cyber security or someone who played an important role in the day-to-day operations and direction of the company.

  Within this segment, the research recruitment considered, on a best-effort basis, the following demographic groups:

  - Women, indigenous, black and disabled people in business ownership or at the director level;
  - Rural and/or remote businesses.

- **Target population 2 – industry groups and organizations and large Canadian enterprises:** these were broadly defined as organizations that either rely on or coordinate supply chains and/or organizations that can in some way influence

SMEs. A range of organization types were identified by ISED that included but were not limited to the following:

- Businesses managing or using supply chains.
- Professional industry associations that can influence SMEs.
- Business associations that can influence SMEs.

In addition to the general participant profiling criteria noted above, additional screening measures to ensure quality respondents include the following:

- 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.).
- In addition, no participant who worked in any such occupation in the past 5 years, as appropriate to the specific research objectives.
- 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.

Target population 2 participants were recruited from a list provided to Quorus by ISED. This list included the name of the organization/company, a contact name, a telephone number and/or an email address. Participants were also obtained through outreach to associations by Quorus consultants. To ensure their eligibility for this phase of the study, all organizations were vetted by ISED before being contacted.

Description of data collection procedures

Data collection consisted exclusively of online focus groups and web-assisted interviews. The duration of the sessions was:

- Phase 1 focus groups – initial concept testing: 90 minutes

- Phase 1 focus groups – success check: 60 minutes
- Phase 2 depth interviews: 45 minutes.

Target population 1 participants were screened by telephone, recruiting 6 participants to achieve 4 to 6 participants per focus group. Participants invited to participate in the focus groups were recruited through a combination of random contacts by telephone and through the use of a proprietary database. These research candidates were screened using a traditional recruitment screener to ensure they met the target audience definitions for this study. Quorus recruited 6 participants for each session, with the goal of having 4 to 6 participants ultimately attend each session.

Recruitment for target population 2 participants was done exclusively from lists provided by ISED. Recruitment was conducted exclusively by Quorus consultants with the support of ISED staff who already had a working relationship with some of the targeted research candidates. These individuals were notified by ISED ahead of the study so that they were aware that they would be contacted by a Quorus consultant to schedule an interview.

The recruitment of focus group and 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 audio/video 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 began their focus group or interview session.

All online focus groups were conducted in the evening after regular business hours, while all online depth interviews were conducted during regular business hours or during evenings (whatever suited the respondent's availability and preferences). The research team used the zoom platform to host and record sessions (through microphones and webcams connected to the moderator and participants electronic devices, i.e. Laptops and tablets) enabling client remote viewing.

The research was structured in two phases, as follows:

Phase 1 – Online focus groups

A total of 10 online focus groups were conducted across two stages:

- **Stage 1 – initial concept testing:** consisted of eight (8) focus groups obtaining initial feedback on concepts across the following regions (all sessions conducted in English except "Montreal and surrounding areas"):
    - Vancouver and surrounding area
    - Calgary/Edmonton and surrounding areas
    - Saskatoon/Regina and surrounding areas
    - Winnipeg and surrounding areas
    - Toronto and surrounding areas
    - Ontario urban centres other than Toronto
    - Montreal and surrounding areas
    - Atlantic Canada (mix of the four provinces)

- **Stage 2 – success check:** consisted of two (2) focus groups obtaining feedback on finalized concepts from businesses located in the following areas:
    - Manitoba, Saskatchewan and Alberta (English)

- Quebec, New Brunswick and Ontario (French)

The details of these groups are outlined in the table below.

Location	Segment	Language	Number of participants	Date and time	Honorarium
Phase 1 – stage 1 (groundwork)					
Toronto area	SMEs	English	5	January 25 @ 5:30 pm	$200
Ontario excluding Toronto	SMEs	English	5	January 25 @ 7:30 pm	$200
Atlantic Canada	SMEs	English	6	January 26 @ 5:30 pm	$200
Montreal area	SMEs	French	6	January 26 @ 7:30 pm	$200
Saskatoon/ Regina	SMEs	English	6	January 27 @ 6:30 pm	$200
Winnipeg area	SMEs	English	6	January 27 @ 8:30 pm	$200
Calgary/ Edmonton	SMEs	English	6	January 28 @ 7:30 pm	$200
Vancouver area	SMEs	English	4	January 28 @ 9:30 pm	$200
Phase 1 – stage 2 (success check)					
Quebec/New Brunswick/Ontario	SMEs	French	5	February 16 @ 5:30 pm	$200
Manitoba/ Saskatchewan/Alberta	SMEs	English	5	February 16 @ 7:00 pm	$200

Phase 2 – Online depth interviews

A total of six (6) 1-on-1 web assisted depth interviews were conducted with participants from target population 2. Participants were able to participate in the official language of their choice.

The scheduling and details of the sessions are outlined in the table below:

Interview	Language	Date and time	Honorarium
Interview #1 – private sector	English	April 22 @ 10:30 am	$250
Interview #2 – professional industry association/organization	English	May 6 @ 10:00 am	$250
Interview #3 – professional industry association/organization	Bilingual	May 10 @ 1 pm	$250
Interview #4 – professional industry association/organization	English	May 11 @ 11 am	$250
Interview #5 – professional industry association/organization	English	May 12 @ 8 am	$250
Interview #6 – private sector	English	May 26 @ 11 am	$250

Appendices

Phase 1 - SME recruitment screener

Online focus groups: (e=English; f=French)	**Details:**
Group 1: Toronto and surrounding areas (e); January 25, 5:30 pm EST	Recruit 6 for 4 to 6 to show
Group 2: Ontario urban centres other than Toronto (e); January 25, 7:30 pm EST	Incentive: $200
Group 3: Atlantic Canada (mix of the four provinces) (e); January 26, 5:30 pm AST	90 Minute sessions
Group 4: Montreal and surrounding areas (f); January 26, 7:30 pm EST	
Group 5: saskatoon/Regina and surrounding areas (e); January 27, 5:30 pm CST	
Group 6: Winnipeg and surrounding areas (e); January 27, 7:30 pm CST	
Group 7: Calgary/Edmonton and surrounding areas (e); January 28, 5:30 pm MST	
Group 8: Vancouver and surrounding area (e); January 28, 6:30 pm PST	
Group 9: Quebec/New Brunswick/Ontario (f); February 16, 5:30 EST	
Group 10: Manitoba/ Saskatchewan/Alberta (e); February 16, 7:00 EST	

Target audience:

Canadian SMEs and not-for profit organizations, with a focus on the larger small organizations (those with 40+ employees). Within this group, the research will target a cross section of business types of interest to ISED, including those part of a supply chain, those in manufacturing and those who have adopted a digital online model during the pandemic. Within each organization, the research will target a decision-maker regarding cyber security or someone who plays an important role in the day-to-day operations and direction of the company.

Within this segment, the research will also consider, on a best-effort basis, the following demographic groups in its recruitment however given the challenging project timelines, their representation cannot be guaranteed:

- Women, indigenous, black and disabled people in business ownership or at the director level;
- Rural and/or remote businesses.

A. 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 and the business community. 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, including the privacy act and the access to information act. We are simply interested in hearing your opinions, no attempt will be made to sell you anything. The format will be an online "round table" discussion lead by a research professional.

Protecting the health and economic well-being of Canadians during the COVID-19 pandemic is a priority for the Government of Canada. The results to surveys such as this one help the Government of Canada continue to deliver on its mandate and to improve its work.

[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**

B. Business and participant profile

1. How would you rate your own level of familiarity with the topic of cyber security, including 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. Including yourself, 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 and a micro business]**
   - 6 to 39 **["medium-small" business]**
   - 40 to 99 **["large-small" business]**
   - 100 to 499 **[medium business]**
   - 500 or more **[thank & terminate]**

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

	Yes	No
a) Are you a person who is blind or has any difficulty seeing even when wearing glasses or contact lenses? [**thank and terminate if "yes"]**	❑	❑
b) 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?	❑	❑
c) Do you have any difficulty learning, remembering or concentrating?	❑	❑
d) Do you have any emotional, psychological or mental health conditions?	❑	❑
e) 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?	❑	❑

*source: 2017 Canadian survey on disability

- *If yes at any of q3a-d – recruit as entrepreneur / business operator / decision-maker with a disability*
- *If yes at q3e – recruit as rural and remote entrepreneur / business operator / decision-maker*

4. Do you identify as any of the following?

    - An indigenous person (first nations, Inuit or Métis); first nations includes status and non–status Indians.
    - A member of an ethnocultural or a visible minority group other than an indigenous person
    - None of the above

- *If yes q4=1: recruit as indigenous entrepreneur / business operator / decision-maker*
- *If yes q4=2: recruit as ethnic community entrepreneur / business operator / decision-maker*

5. **[ask only if q4=2]** what is your ethnic background?

    Record ethnicity: _____

6. 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
   - Not-for-profit / Charity
   - Other (specify)

7. Can you please provide me with your job title? _____

8. Does your company deliver goods or services as part of a supply chain? In other words, one or many companies deliver products and services to your company, and in turn you then provide products and services to one or many other companies?

   - Yes **"supply chain" companies - recruit at least 2 per focus group**
   - No

9. Since the onset of the COVID-19 pandemic, has your company needed to rely more heavily on the internet to continue operations? This would include having staff work remotely more than before, ordering products and services online more than before, selling your company's products and services online more than before, etc.

   - Yes **"pandemic online adapters" - recruit at least 2 per focus group**
   - No

10. 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**

o Very comfortable	**min 5 per group**
o Fairly comfortable	
o Not very comfortable	**terminate**
o Not at all comfortable	**terminate**

11. Again, to make sure we have a good mix of participants at the table, how do you identify yourself? Would you say…

Note 1: ensure a good mix in and across all sessions
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.*

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

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?

o Yes	**maximum 5 per group**
o No	**go to invitation**

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

o Within the last 6 months	**terminate**
o Over 6 months ago	

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

o Fewer than 5	
o 5 or more	**terminate**

C. Online focus group invitation

I would like to invite you to participate in an online 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 $200 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. **You can use a tablet if you so choose however you cannot use a smartphone to participate in this discussion since the screen size is too small.**

If asked: you will be asked to use a webcam to participate so please be sure that the device you use has a properly functioning microphone and webcam.

Over the coming days we will be sending you an email with the web link to connect to the online session as well as the date and time of the session.

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!

Focus group moderation guide for SMEs (Phase 1 – Part 1)

A. Introduction (8 minutes)

- Introduce moderator and that he works with Quorus consulting, and they are conducting this research on behalf of the Government of Canada (the moderator is not a Government of Canada employee)
- Thanks for attending/value you being here
- Explain general purpose of focus group discussions:
    - Gauge *opinions* about issues/ideas/products
    - Not a knowledge test; no right or wrong answers (interested in opinions)
    - Today's session will last approximately 90 minutes.
    - 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
    - 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 are on the web conference as well.
    - All comments will remain confidential and anonymous and the recordings are not shared with anyone. If we wanted to share the recordings or any of your personal information, we would need to obtain your express written consent first.
    - If you have a cell phone, please turn it off.
    - To participate in this session, please make sure your webcam and your microphone are on and that you can hear me clearly. 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!
    - I will be sharing my screen to show you some things.
    - We will be making regular use of the chat function. To access that feature, please scroll over the bottom of your 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.

- I also want to say that if you feel you didn't have a chance to express your opinion on anything during the session, you can feel free to comment in writing in the "chat". For the most part chat with "everyone" unless you feel you need to send me a private message.

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

- What type of business do you own/operate/manage?
- What is your role or your position?
  - Are you responsible for anything to do with IT or cyber security?
- And, in that role, what would you say is your biggest concern these days? What keeps you up at night?
  - What does cyber security mean to you?

B. Business confidence in current level of cyber security (20 minutes)

To start, how many of you have had to increase your online presence as a result of the pandemic or had to quickly adopt new internet-based technologies to continue your operations? **If needed:** …such as social media, ecommerce platforms or other applications?

- Can you give me examples of the ways your company has had to adapt?

Overall, how are you feeling about your level of "cyber security" these days especially given the dramatic shift this pandemic has had on the digital economy? 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.

- To help me understand this, let's use the chat feature and 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 your company's level of cyber security these days? Go ahead and enter your score in the chat window and then we'll discuss. **Moderator collects scores**
- What are your concerns exactly? …is there room for improvement?
- 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?

Working remotely - pivoting to e-commerce

I would like to explore a couple of the ways in which some of you have needed to adapt to the COVID-19 pandemic let's start by looking at having your staff work remotely more than before.

- Through a show of hands, for how many of you does this apply?

- Was your business already working remotely before the pandemic?
  - **If yes:** what infrastructure, systems or procedures did you have in place?
    - **If needed:** were employees working on personal devices?
- What infrastructure, systems or procedures have you had to implement?

Explore as needed:

  - Did you have to create policy for workspaces on personal devices? Or provide work only devices for employees?
  - Has your business accelerated migration to cloud infrastructure and applications?
  - Has your business had to grow its functionality and use of online collaborative tools? …like MS teams, zoom, google meetings, etc.

Now, I'd also like to look **at the pivot to e-commerce**.

- Has your business experienced a rise in e-commerce?
- Through a show of hands, how many does this apply to?
  - How confident are you that you've made this transition securely?

- Has your business adapted to conducting risk assessments and enforcement mechanisms while adopting these new technologies, be it for telework or ecommerce?

- Has your business experienced any cyber-attacks due to increased telework?

- How about those related to increased e-commerce?

- Were you aware of the increase of cyber-attacks since the pandemic started?
  - **If yes:** did you do anything to prepare your business?
  - **If no:** does it surprise you to hear that there has been an increase in cyber-attacks since the pandemic started?

C. General concept evaluation (50 minutes – three concepts a, b, c)

Let's turn our attention to some advertising concepts.

The Government of Canada launched a cyber security certification program for small and medium sized businesses. Those who meet the certification requirements are "certified" and are able to demonstrate this achievement by displaying the Cybersecure Canada certification mark.

We would like to get your feedback on the creative concepts for a national advertising campaign to promote awareness of the importance of cyber security more generally and, more specifically, to promote awareness of the program.

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. The ads will appear in national media business sections/web pages (e.g., in the Globe and Mail on Business; La Presse), on IT industry web sites.

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.

For internal use only:

Concepts (each identifiable by a letter of the alphabet) are presented one at a time by the moderator (concepts to be presented in a different order for each session):

Concept A = Easier

Concept B = First Step

Concept C = Trust

Randomize concepts for each group as follows:

Session 1: A, B, C	**Session 5: B, A, C**
Session 2: B, C, A	**Session 6: C, B, A**
Session 3: C, A, B	**Session 7: A, B, C**
Session 4: A, C, B	**Session 8: B, C, A**

For each concept, I will show you (in this order):

- A print ad,
- An internet banner ad which would appear at the top of webpages you visit,
- A short video ad, also intended for online use (not a TV ad).

Moderator to show each concept and give participants time to consider the following questions for themselves (self-questionnaire)

Please consider the following when I am showing you the ad – you may want to jot down some notes on a piece of paper, but let's reserve discussion while everyone thinks about the following:

Moderator to show on screen after showing each concept:

What is the point of this ad?
How does this ad make you feel?/what comes to mind when you see this ad?
Would you do anything after seeing this ad?

Once everyone is done, start with discussion probes:

- What were your overall reactions to the ad? Help me understand those reactions…
- What were your first impressions: tell me, what did you like about this ad? Now tell me what you did not like.

I want to get your views on the concept. We're going to focus on the 3 key components of any advertising:

1. The **main message**, what they're trying to say to you
2. The **creative idea**, how they're trying to say/present that message to you
3. The **call-to-action**, what they're trying to get you to do or think

Main message verbal probes

- What is the main message in this concept, what were they trying to say to you?
- Is the main message…
  - Clear? Why/why not?
  - New information for you? How so?
  - Helpful or relevant for you? Why / why not?
  - Persuasive? Why / why not?
  - Memorable? Why/why not?

- Was it clear to you that this was a Government of Canada ad?

Creative verbal probes

- What did you think of the creative idea they are planning to use to get this message across to you? **Probe:**
  - Describe it to me in your own words.
    - How would you describe the tone of it? Positive; negative; upbeat; realistic? Is this appropriate given the message?
    - Likes/dislikes
    - Attention grabbing/unique – specific visuals, script, etc.? What was your eye drawn to?

Call to action probes

- What are they trying to get you to do or think? Would you? Why / why not?
- If you were to follow-up, is it clear what the next steps are?
- Do you remember the name of the program? What impression are you left of the program in this concept? Why is that?
- Would you visit the website after seeing this ad? Why / why not?
    - What was the website shown in the ad?
    - Did the concept do enough to persuade you that there is useful information on the site for business owners/operators like yourself? How so?

Probes after all 3 concepts are shown:

- **Moderator to show a screen that features all three concepts with their associated letters:** of the three concepts, which one do you prefer and why? I need everyone to submit an answer on this. **Please use the chat function and indicate a, b, or c.**

- Is there anything that could be done to improve on the way the information is presented on your preferred ad concept? What specifically would you suggest and why is that?

- Where should we place this concept to get your attention? Where do you go for your business news?

D. Exploring expectations set by advertisements (12 minutes)

Let's get your initial reactions to the cyber secure certification program itself. This certification program was developed with the Canadian Centre for Cyber Security.

Moderator to share screen:
The Cybersecure Canada certification program is a voluntary cyber security certification program implemented by the Government of Canada.

Certified businesses are required to implement 13 security control areas that cover a wide variety of vulnerabilities for small and medium organizations such as employee training, password protection, incident response plans and more.

These control areas were developed by the Canadian Centre for Cyber Security, Canada's cyber security experts specifically for small and medium organizations.

- Were you aware of this certification program before today's group discussion?
    - If yes, how did you come across it?

- Do you think you would consider or set time aside to get certified? …help me understand your position on this.

If needed:

- Would you feel more secure?
- Have you considered other certification programs?

- Do you feel having your business associated with the cyber secure Canada brand would benefit your business? How so?
- Some of you are parts of supply chains. If supply chains started to require proof of cyber security from their suppliers would this change your views of cyber certification?
  - To become certified, would your business be willing and able to invest in your cyber security by…
    - Updating software?
    - Updating hardware such as cell phones, computers, etc.?
    - Upgrading IT infrastructure?
    - Investing in a security audit toward cyber secure certification?

E. Thank and close (2 minutes)

[moderator checks with client team regarding any new questions/clarifications needed]

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

Thanks again! The team that invited you to participate in this session will contact you regarding the manner in which you can receive the incentive we promised you.

And have a great evening!

Focus group moderation guide for SMEs (phase 1 – success check)

A. Introduction (10 minutes)

- Introduce moderator and that he works with Quorus consulting, and they are conducting this research on behalf of the Government of Canada (the moderator is not a Government of Canada employee)
- Thanks for attending/value you being here
- Explain general purpose of focus group discussions:
    - Gauge *opinions* about issues/ideas/products
    - Not a knowledge test; no right or wrong answers (interested in opinions)
    - Today's session will last approximately 60 minutes.
    - 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
    - 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 are on the web conference as well.
    - All comments will remain confidential and anonymous and the recordings are not shared with anyone. If we wanted to share the recordings or any of your personal information, we would need to obtain your express written consent first.
    - If you have a cell phone, please turn it off.
    - To participate in this session, please make sure your webcam and your microphone are on and that you can hear me clearly. 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!
    - I will be sharing my screen to show you some things.
    - We will be making regular use of the chat function. To access that feature, please scroll over the bottom of your 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.

- I also want to say that if you feel you didn't have a chance to express your opinion on anything during the session, you can feel free to comment in writing in the "chat". For the most part chat with "everyone" unless you feel you need to send me a private message.

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

- What type of business do you own/operate/manage?
- What is your role or your position?
  - Are you responsible for anything to do with IT or cyber security?
  - What does cyber security mean to you?

B. Business confidence in current level of cyber security (10 minutes)

To start, how many of you have had to increase your online presence as a result of the pandemic or had to quickly adopt new internet-based technologies to continue your operations? **If needed:** …such as social media, ecommerce platforms or other applications?

- Can you give me examples of the ways your company has had to adapt?

Overall, how are you feeling about your level of "cyber security" these days especially given the dramatic shift this pandemic has had on the digital economy? 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.

- To help me understand this, let's use the chat feature and 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 your company's level of cyber security these days? Go ahead and enter your score in the chat window and then we'll discuss. **Moderator collects scores**
- What are your concerns exactly? …is there room for improvement?

- Were you aware of the increase of cyber-attacks since the pandemic started?
  - **If yes:** did you do anything to prepare your business?
  - **If no:** does it surprise you to hear that there has been an increase in cyber-attacks since the pandemic started?

C. General concept evaluation (30 minutes – concepts A and B)

Let's turn our attention to some advertising concepts.

The Government of Canada launched a cyber security certification program for small and medium sized businesses. Those who meet the certification requirements are "certified" and are able to demonstrate this achievement by displaying the cybersecure Canada certification mark.

We would like to get your feedback on the creative concepts for a national advertising campaign to promote awareness of the program.

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. The ads will appear in national media business sections/web pages (e.g., in the Globe and Mail on Business; La Presse), on IT industry web sites.

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.

For internal use only:

Concepts (each identifiable by a letter of the alphabet) are presented one at a time by the moderator (concepts to be presented in a different order for each session):
Concept A = Beavers
Concept B = Trust chain

<u>Randomize concepts for each group as follows:</u>
Session 1: A, B
Session 2: B, A

For each concept, I will show you (in this order):

- An animated internet banner ad which would appear at the top of webpages you visit,
- A version of the same internet ad as it would appear online in publications such as the globe & mail business page or la Presse.

Moderator to show each concept and give participants time to consider the following questions for themselves (self-questionnaire)

Please consider the following when I am showing you the ad – you may want to jot down some notes on a piece of paper, but let's reserve discussion while everyone thinks about the following:

Moderator to show on screen after showing each concept:
What is the point of this ad?
What is the main message?
What comes to mind when you see this ad?
Would you do anything after seeing this ad?

Once everyone is done, start with discussion probes:

- What were your overall reactions to the ad? Help me understand those reactions…
- What were your first impressions: tell me, what did you like about this ad? Now tell me what you did not like.

I want to get your views on the concept. We're going to focus on the 3 key components of any advertising:

1. The **main message**, what they're trying to say to you
2. The **creative idea**, how they're trying to say/present that message to you
3. The **call-to-action**, what they're trying to get you to do or think

Main message verbal probes

- What is the main message in this concept, what were they trying to say to you?
- Is the main message…
  - Clear? Why/why not?
  - New information for you? How so?
  - Helpful or relevant for you? Why / why not?
  - Persuasive? Why / why not?
  - Memorable? Why/why not?

- Was it clear to you that this was a Government of Canada ad?

Creative verbal probes

- What did you think of the creative idea they are planning to use to get this message across to you? **Probe:**
  - Describe it to me in your own words.
    - How would you describe the tone of it? Positive; negative; upbeat; realistic? Is this appropriate given the message?
    - Likes/dislikes
    - Attention grabbing/unique – specific visuals, script, etc.? What was your eye drawn to?

Call to action probes

- What are they trying to get you to do or think? Would you? Why / why not?
- If you were to follow-up, is it clear what the next steps are?
- Do you remember the name of the program? What impression are you left of the program in this concept? Why is that?
- Would you visit the website after seeing this ad? Why / why not?
  - What was the website shown in the ad?
  - Did the concept do enough to persuade you that there is useful information on the site for business owners/operators like yourself? How so?

Probes after both concepts are shown:

- **Moderator to show a screen that features both concepts with their associated letters:** of the two concepts, which one do you prefer and why? I need everyone to submit an answer on this. **Please use the chat function and indicate a or b.**
- Is there anything that could be done to improve on the way the information is presented on your preferred ad concept? What specifically would you suggest and why is that?
- Do you have a supply chain or do you consider your business to be part of a supply chain?
- Where should we place this concept to get your attention? Where do you go for your business news?

F. Thank and close (2 minutes)

[moderator checks with client team regarding any new questions / clarifications needed]

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

Thanks again! The team that invited you to participate in this session will contact you regarding the manner in which you can receive the incentive we promised you.

And have a great evening!

Cybersecure program Phase 2: In-depth interview guide

A. Introduction (7 minutes)

Interviewer introduces him/herself: my name is [insert moderator name] and I work with Quorus consulting, and we are conducting research on behalf of the Government of Canada.

- Thank you for participating in this one-on-one 45 minute depth interview.

Explain general purpose of the in-depth interviews:

- Protecting the health and economic well-being of Canadians during the COVID-19 pandemic is a priority for the Government of Canada. Throughout the pandemic, one issue that has become increasingly important and challenging for businesses is cyber security.

- As part of its ongoing efforts to understand the challenges businesses and organizations of all sizes face in this area, innovation, science and economic development Canada (ISED) has commissioned quorus consulting group to conduct a reseach study with the Canadian business community.

  We will be exploring the theme of cyber security and will be eager to get your reactions to a recently introduced Government of Canada Cyber Certification program. Please keep in mind the following:

  - Looking for candor and honesty; comments treated in confidence; no names of participants or the companies/organizations they represent are included in the analysis or reporting; reporting in aggregate form only; video recording and note-taking for report writing purposes only; observers are on the web conference as well.

  - The report can be accessed through the Library of Parliament or Archives Canada.

With that, if you don't have any further questions, let's get started!

Warm-up

Let's start by finding out a little bit about you and your organization…

- How would you describe your organization – what is its primary focus?
- What is your role or your position?
    - Are you responsible for anything to do with IT, cyber security, supply chain, supply chain security or procurement?
- And, in that role, what would you say is your biggest concern these days? What keeps you up at night?
    - What does cyber security mean to you as a representative of your organization?

B. Procurement, supply chain, vendors and cyber security (15 minutes)

- Overall, how are you feeling about your company's level of "cyber security" these days?
    - Tell me how you are feeling about your company's level of cyber security these days, on a scale from 0 to 10, where 0 means you are feeling extremely vulnerable and 10 means you are feeling completely protected? **Note score**
- To what extent, if at all, do you view your supply chain as a source of concern for your own organization's cyber security? …help me understand this a bit more.
- How resilient/able to adapt would you say your supply chain / vendors have been during the pandemic? How so?
    - Has the pandemic exposed or introduced any cyber security vulnerabilities or challenges among your suppliers which have also had an impact on your company?
    - Did you lose vendors during the pandemic (e.g., businesses forced to close)?
    - How prepared has your supply chain or vendors been in the face of cybersecure challenges?
        - Did you note cyber security increasing in importance amongst your vendors over the course of the past year?
        - What are the characteristics of vendors/businesses within your supply chains that are performing well (**probe**: business size, experience, knowledge)?
    - Are you concerned about cyber security within your supply chain? How are you addressing this?
    - Did you need to change your procurement practices?

- In terms of your risk management, have you ever required a level of cyber security amongst your suppliers?
    - **If yes:** do you require it of all suppliers or just specific ones/types? And if it is for specific types, what criteria do you use to determine which ones require a level of cyber security?
    - **If not:** have you ever *considered* requiring it amongst your suppliers?
- Do you ask suppliers to demonstrate/prove their level of cyber security?
    - …is that easy or difficult for your suppliers to do? Again, are there certain types of businesses that are doing better in this area?
    - …is that easy or difficult for your company to assess, i.e., is there consistency in how this is reported back to your company?
    - How confident are you in what your suppliers are telling you?
    - Do you think the businesses you deal with should be able to "prove" their level of cyber security?

C. Role of government in cyber security (10 minutes)

Your organization uses small and medium businesses as vendors, as part of a supply chain. What role, if any, could or should the Government of Canada be playing when it comes to supporting these small and medium- sized businesses to become cyber secure?

Moderator note: discussion to stay focused on the role of the federal government and not the roles the provincial or municipal governments may also play.

- How might the Government of Canada better support SMEs to improve the level of cyber security in your supply chains?
    - Can they help improve the security of your supply chain / of your suppliers?
- Should the government make it mandatory for businesses to have in place some level of cyber security protection or proof of due diligence?
    - In your view, what impact could this have on your operations?
    - Thinking of supply chain management, would making some level of cyber security mandatory reduce burdens of cyber security or lessen risks on organizations like yours?

- If not mandatory, what are the best approaches to encouraging organizations like yours and businesses in your supply chain to increase or improve their cyber security measures?

- Would having your various suppliers obtain some sort of cyber certification have an impact on any of the following in your opinion:
  - Trust and confidence in your organization?
  - Enhance protection of privacy (customer records, business data)?
  - Protection of your brand?
  - Better risk awareness and risk management?
  - Better (more secure) supply chain management?
  - What other type of impact could the cyber certification of your supply chain have?

D. Cybersecure program evaluation (13 minutes)

I would like to introduce you to the Government of Canada's cybersecure program and get your thoughts and initial reactions and then return to discuss supply chains – in particular the small and medium businesses that support your organization.

Moderator reads:
The cybersecure Canada program aims to promote trust in Canada's digital economy, both domestic and foreign. Its purpose is to raise the cyber security baseline among small and medium enterprises (SMES) in Canada, increase consumer confidence in the digital economy, promote international standardization and better position SMEs to compete globally.

Interviewer to displays the program summary on screen. Provides participant some time to read/review the summary. Leaves the information up on the screen as the interview resumes.

The CyberSecure program is a means for SMEs to demonstrate that they are taking appropriate measures to protect their systems, build in resiliency in case of any attacks, as well as safeguard their customers and contractors' information.

To be eligible for certification, the organization must review and implement the 13 security controls established by the **Canadian Centre for Cyber Security**:

- Develop an incident response plan
- Automatically patch operating systems and applications
- Securely configure devices
- Enable security software
- Use strong user authentication
- Provide employee awareness training
- Back up and encrypt data
- Secure mobility
- Establish basic perimeter defences
- Secure cloud and outsourced IT services
- Secure websites
- Implement access control and authorization secure portable media

A certification body (**accredited through the Standards Council of Canada**) will evaluate the businesses' implementation of the 13 security controls. The certification body consults directly with each organization to:

- Determine if the organization is ready to be certified;
- Provide a cost estimate for the organization to achieve cybersecure certification; and,
- Audit the organization's implementation of the security controls.

Once a business obtains the CyberSecure certification, they are certified for two years and have the option of displaying the certification mark on their websites, storefronts, and promotional materials.

Moderator resumes:

- Have you heard of this certification or any other certifications for cyber security? …what other certifications are you aware of?
- What are your general thoughts on these types of programs?
  - Would you consider having your company require its supply chain/ suppliers to become cyber certified?

- What would be the challenges in making that happen?
- What would be the benefits to your company?

- How would your customers/citizens/stakeholders (as appropriate) feel if your vendors were certified under this program? …would something like this certification make a difference?

- What are your expectations of government involvement in the program?

- If we consider the types of security control areas that companies would need to address, do you feel your supply chain vendors have the right tools and expertise to begin implementing these controls to achieve certification?

  - **If no:** what do you feel is missing or lacking?

    Explore as needed:

    - Cyber security knowledge
    - Dedicated IT staff

- Do you feel your supply chain vendors would need to hire a consultant to help them implement the controls to become certified?
  - If not, do you think the government has a role to provide solutions for these potential gaps?
  - What is your confidence level in the cyber security provided by these third parties?
  - Would you feel more confident in these third parties if they were themselves certified as being cyber secure?

- If your supply chain members were to become certified through this program, what impact would that have on how cybersecure you feel your own company is? 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 would feel extremely vulnerable and 10 means you would feel completely protected. **Moderator notes rating**

Cybersecure Canada website *(time permitting)*

Before we conclude, I would like to take a minute to look at the program's website briefly: Canada.ca/cybersecure **moderator to show on screen**

- Have you visited this website before?
- What are the main messages you take away from the web page?
- Is the main purpose of the program clearly communicated?
- Based on what you've been able to glean from this visit…
    - …does it strike you as a website that is easy to understand?
    - Is the information well organized?
    - Would you explore it or provide it to your vendors?
    - Is there a clear call to action?
- Is there anything you would add/change to make it more relevant to your vendors?
- Is there anything you would add/change to make it more relevant for companies like yours who would have suppliers with this type of certification?

E. Thank and close (2 minutes)

[interviewer checks with client team regarding any new questions / clarifications needed]

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

Thanks again! And have a great *[day/ evening*]!