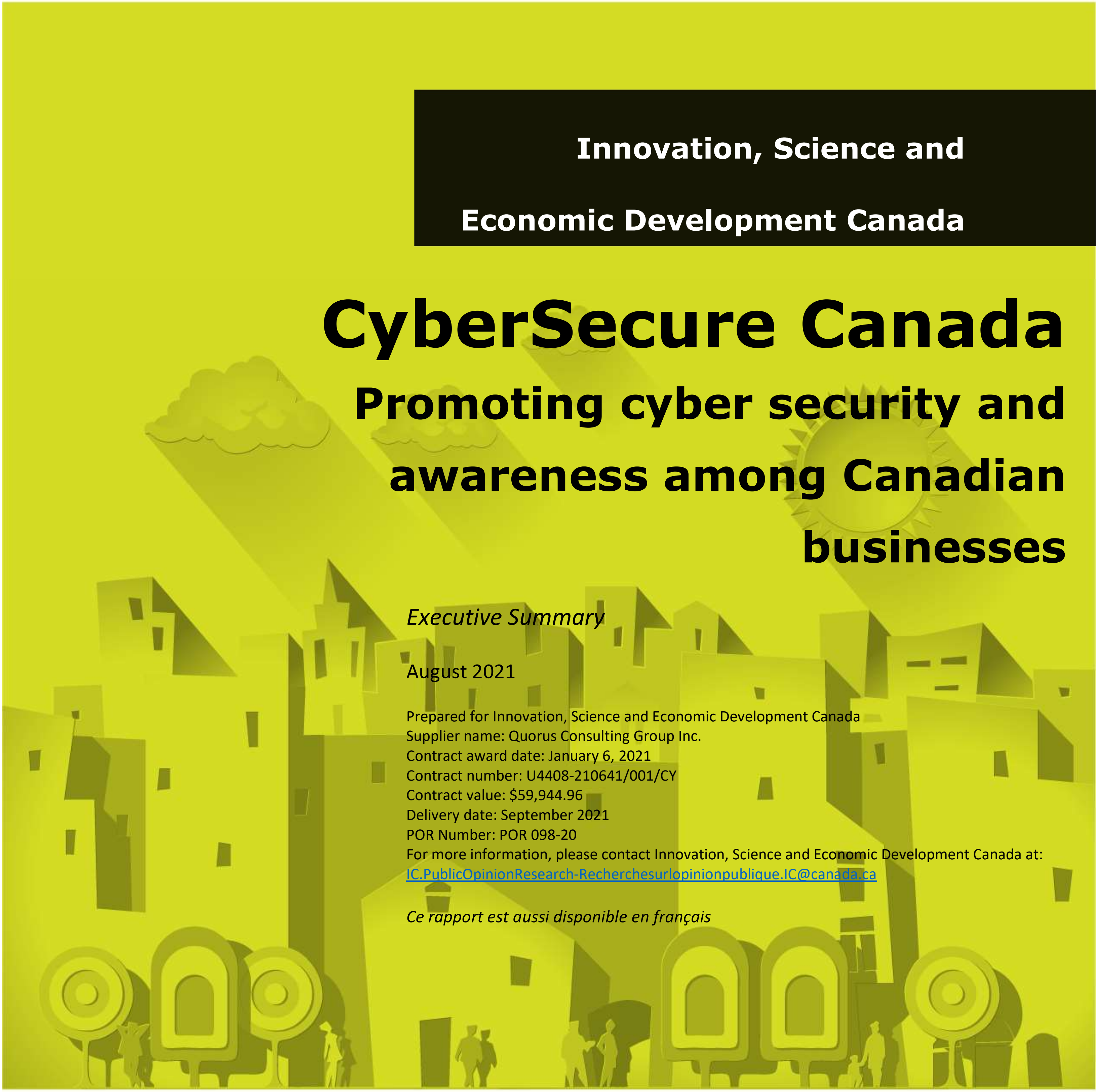
Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada



Innovation, Science and Economic Development Canada

CyberSecure Canada

Promoting cyber security and awareness among Canadian businesses

Executive Summary

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

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.

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