



**Innovation, Science and
Economic Development Canada**

CyberSecure Canada Program

Executive Summary

July 2019

Prepared for Innovation, Science and Economic Development Canada

Supplier name: Quorus Consulting Group Inc.

Contract award date: March 5, 2019

Contract number: U1400-198102/001/CY

Contract value: \$129,006.45

Delivery date: July 2019

POR Number: POR 132-18

For more information, please contact Innovation, Science and Economic Development Canada at:

IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca

Ce rapport est aussi disponible en français

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

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

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

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

Permission to Reproduce

Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from the Department of Industry, provided that due diligence is exercised in ensuring the accuracy of the information reproduced; that the Department of Industry is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced or as having been made in affiliation with, or with the endorsement of, the Department of Industry.

For permission to reproduce the information in this publication for commercial purposes, please fill out the Application for Crown Copyright Clearance at www.ic.gc.ca/copyright-request or contact the Web Services Centre mentioned above.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Industry, (2019).

Cat. No. Iu4-266/2-2019E-PDF

ISBN 978-0-660-32484-5


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

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:

A handwritten signature in black ink, appearing to read 'Rick Nadeau', is written over a light gray, textured rectangular background.

Rick Nadeau, President
Quorus Consulting Group Inc.

Table of Contents

Executive Summary.....	5
Background and Objectives	6
Research Results	6
Confidence in SME Cyber Security	6
Role of Government in Supporting SMEs	8
General Concept Evaluation	8
Exploring a Program with Tiers	9
Use of Colours in the Visual Concepts	10
Potential Impact on Competitiveness.....	10
Expectations of the Program	10
Role of the Government	11
Methodology.....	12

Executive Summary

Background and Objectives

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

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

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

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

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

Research Results

Confidence in SME Cyber Security

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

Consumer Perspective

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

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

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

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

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

SME Perspective

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

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

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

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

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

Role of Government in Supporting SMEs

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

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

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

General Concept Evaluation

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

Feedback from participants that apply to all three concepts include the following:

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

Feedback specific to each concept is summarized below:

- Concept A (Shield): The imagery was liked by many, as it communicated security. Many also liked the font that was used. On the other hand, while it conveyed security, it was not considered unique because they had seen shields used by other security-related companies.
- Concept B (Lock): The concept clearly conveyed “security” - nearly everyone saw a lock right away. A few liked that the “C” from cyber and “S” from secure were incorporated into the design of the lock. Some felt the lock looked open which conveyed weak security, and many would have preferred two font styles (similar to the font style used in the other two concepts).
- Concept C (Arch): The concept’s only strength was that a few considered it to be unique. On the other hand, this concept was often dismissed mostly because participants could not figure out what the image was and that it did not convey the notion of “security”. The font was also seen as weak and “not serious”.

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

Exploring a Program with Tiers

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

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

Use of Colours in the Visual Concepts

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

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

Potential Impact on Competitiveness

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

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

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

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

Expectations of the Program

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

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

Consumer Perspective

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

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

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

SME Perspective

SME participants had more specific expectations of the program:

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

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

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

Role of the Government

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

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

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

Methodology

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

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

Qualitative Research Disclaimer

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

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

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

Supplier Name: Quorus Consulting Group Inc.

PSPC Contract Number: U1400-198102/001/CY

Contract Award Date: March 5, 2019

Contract value (including HST): \$129,006.45

For more information, please contact the Innovation, Science and Economic Development Canada at:

IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca