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

Innovation, Sciences et

Développement économique Canada

Programme CyberSécuritaire Canada

Sommaire

Juillet 2019

Préparé pour Innovation, Sciences et Développement économique Canada
Nom du fournisseur : Le groupe-conseil Quorus Inc.
Date d'octroi du contrat : Le 5 mars 2019
Numéro de contrat : U1400-198102/001/CY
Valeur du contrat : 129 006,45 $
Date de livraison : Juillet 2019
Numéro ROP : ROP 132-18
Pour de plus amples renseignements, veuillez communiquer avec Innovation, Sciences et Développement économique Canada, à : IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca

This report is also available in English.

Canada

Cette publication est également offerte en ligne : https://www.ic.gc.ca/eic/site/112.nsf/fra/accueil.

Pour obtenir un exemplaire de cette publication ou un format substitut (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication : www.ic.gc.ca/demande-publication ou communiquer avec :

Centre de services Web
Innovation, Sciences et Développement économique Canada
Édifice C.D.-Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5
Canada

Téléphone (sans frais au Canada) : 1-800-328-6189
Téléphone (international) : 613-954-5031
TTY (pour les personnes malentendantes) : 1-866-694-8389
Les heures de bureau sont de 8 h 30 à 17 h (heure de l'Est)
Courriel : ISDE@Canada.ca

Autorisation de reproduction

N° de catalogue lu4-266/2-2019F-PDF

ISBN 978-0-660-32483-8

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

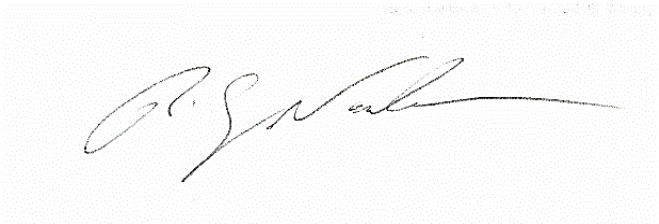
This publication is also available in English, under the title *CyberSecure Canada Program – Final Executive Summary*.

Énoncé sur la neutralité politique

J'atteste, par la présente, à titre d'agent principal du groupe-conseil Quorus Inc., que les produits livrables se conforment entièrement aux exigences en matière de neutralité politique du gouvernement du Canada énoncées dans la Politique sur les communications et l'image de marque et l'Annexe C de la Directive sur la gestion des communications.

Plus précisément, les produits livrables ne contiennent pas d'information sur les intentions de vote électoral, les préférences quant aux partis politiques, les positions des partis ou l'évaluation de la performance d'un parti politique ou de ses dirigeants.

Signé :



Rick Nadeau, président
Le groupe-conseil Quorus Inc.

Table des matières

Sommaire

Contexte et objectifs

Le gouvernement du Canada est déterminé à protéger la sécurité et la prospérité des Canadiens et des Canadiennes à l'heure de l'ère numérique.

Dans cet esprit, Innovation, Sciences et Développement économique Canada (ISDE) et ses partenaires collaborent dans le but de développer et d'établir un programme de cybercertification volontaire et identifiable pour aider les petites et moyennes entreprises (PME) à se protéger contre les cybermenaces et ainsi accroître leur résilience. Le programme vise à permettre aux PME de démontrer à leurs clients d'affaires et aux consommateurs qu'elles ont complété un programme de certification et qu'elles se conforment aux exigences de base en matière de pratiques sécuritaire.

Ce projet de recherche vise à assurer le succès du lancement, de la promotion et de la mobilisation envers le programme de cybercertification dans le but d'inciter les PME à l'adopter. Il se penchera sur les éléments suivants :

- la perception des participants face aux trois concepts créés pour désigner le programme (l'aspect visuel et les messages);
- les éléments préférés de chaque concept;
- la réaction et le niveau de confiance à l'égard d'une « image de marque cybersécuritaire »;
- les attentes qu'une certification sur la cybersécurité engendre;
- les avantages perçus et l'identification d'obstacles à l'adoption; et
- la compréhension générale et la crédibilité des messages présentés (écrits et visuels).

Somme toute, la recherche servira à créer une image de marque reconnaissable et crédible pour la cybersécurité au Canada, en plus d'appuyer le programme pour qu'il soit en mesure d'accroître la résilience de la cyberinfrastructure des PME à l'endroit des cyberattaques et d'augmenter le nombre de PME dotées d'un système cybersécuritaire efficace.

Résultats de la recherche

La confiance des PME en matière de cybersécurité

On a exploré des concepts généraux de cybersécurité avec des consommateurs et des PME dans le but d'acquérir une compréhension initiale du contexte dans lequel s'inscrirait un programme de certification.

La perspective des consommateurs

Lorsqu'on a demandé aux consommateurs de décrire la première chose qui leur vient à l'esprit à la mention de « cybersécurité », la plupart d'entre eux se sont limités aux transactions financières. En d'autres mots, ils se préoccupent principalement de la protection et de l'usage éthique de l'information associée à leurs cartes de débit ou de crédit. Ils s'attendent également à ce que leurs institutions

financières les remboursent si on utilise leurs cartes sans leur consentement. L'expression « cybersécurité » a aussi fait ressortir le sentiment de sécurité lié à l'usage de sites Web de certains commerçants, le vol d'identité en général et les « pirates informatiques » ou les virus retrouvés dans leurs dispositifs personnels.

Les consommateurs perçoivent un risque limité dans le cas où ils auraient fait affaire avec une PME dont la cybersécurité aurait été compromise ou dont les agissements seraient contraires à l'éthique. Bon nombre de consommateurs se disent d'ailleurs rassurés, car ils considèrent que les pirates informatiques accordent généralement peu d'intérêt aux PME.

Certains consommateurs ont mentionné les notions de sécurité suivantes dans le cadre de leurs transactions avec des PME :

- Les sites Web qui affichent « un petit cadenas vert » offrent un environnement sécuritaire pour faire des achats en ligne.
- Ils se sentent plus en sécurité lorsqu'ils font affaire avec des PME et des sites Web de PME appuyés par des fournisseurs tiers ou des institutions comme les banques, PayPal, Visa, Interac et autres fournisseurs de services de points de vente.

À la question sur les mesures que les PME pourraient ou devraient prendre pour accroître leur niveau de cybersécurité, les consommateurs ont offert peu de solutions. Même si les PME communiquaient mieux leur niveau de cybersécurité, ils acceptent qu'en général, il soit impossible d'atteindre un niveau absolu.

La perspective des PME

Les PME se préoccupent davantage de leur propre niveau de cybersécurité. Elles admettent qu'il s'agit d'un défi pour elles de rester au fait de leur système informatique et de la technologie en général. Très peu d'entre elles emploient du personnel dédié à leur système informatique et plusieurs indiquent que la surveillance de ces systèmes ajoutée à la gestion d'une petite entreprise constituait un défi de taille.

Lorsqu'elles réfléchissent au niveau de confiance qu'elles ont de leur propre cybersécurité, la plupart des PME semblent se concentrer principalement, voire exclusivement, sur les renseignements qu'elles obtiennent de leurs clients. Elles se préoccupent moins des données internes à l'entreprise (y compris les renseignements sur leurs employés, les données financières et les données exclusives), et des renseignements liés à leurs fournisseurs.

Les PME parmi les plus confiantes quant à leur niveau de cybersécurité sont surtout les plus « grandes »; elles sont plus susceptibles d'avoir érigé une expertise interne pour traiter des questions de cybersécurité. Trois autres catégories d'entreprises affichent un niveau élevé de confiance : celles qui ont une expertise en cybersécurité ou en informatique, celles qui ne considèrent pas recueillir suffisamment de données pour justifier un investissement important en matière de cybersécurité et celles qui ne font pas la cueillette de renseignements sur leurs clients ou qui n'entreposent pas les données dans leurs ordinateurs.

Peu importe leur positionnement sur le spectre de la « cybersécurité », toutes les PME reconnaissent l'impossibilité d'atteindre un niveau de sécurité absolue. Elles supposent que si les pirates informatiques peuvent s'introduire dans les systèmes de grandes entreprises, elles n'en sont pas à l'abri. À savoir si la cybersécurité constitue un critère important dans le choix d'un fournisseur, les entreprises semblent être partagées sur la question. Toutefois, la plupart disent que lors de l'évaluation de deux fournisseurs pour un service ou un contrat donné, elles favoriseraient le fournisseur qui démontre la présence de mesures en matière de cybersécurité plutôt que celui qui ne le démontre pas.

Les avis sont également partagés sur les occasions d'affaires manquées puisqu'elles ne peuvent « prouver » leur niveau de cybersécurité. Certaines plus petites PME perçoivent qu'elles ratent des occasions d'affaires et croient qu'elles seraient en mesure de soumissionner sur de plus grands projets ou devenir des fournisseurs pour de plus gros clients si elles pouvaient faire la preuve de leur niveau de sécurité. À l'inverse, d'autres entreprises, et particulièrement les entreprises traditionnelles ayant pignon sur rue (p. ex., petits détaillants, personnes de métier) n'y voient aucun problème.

Le rôle du gouvernement en matière d'appui aux PME

La plupart des PME et des consommateurs croient que le gouvernement fédéral a un rôle à jouer pour aider les PME à améliorer leur niveau de cybersécurité. Parmi les suggestions les plus populaires, il y a l'offre de formation, des lignes directrices, des pratiques exemplaires et des listes de contrôle pour que les PME puissent vérifier et améliorer le niveau de cybersécurité. Certains participants ont suggéré que le gouvernement fournisse des logiciels ou des systèmes informatiques abordables ou encore des conseils sur le genre de système ou de logiciel que les entreprises devraient se procurer.

Cependant, l'implication gouvernementale ne bénéficie pas d'un soutien unanime. Certains s'opposaient à une réglementation additionnelle pour les entreprises ou encore au fait qu'on affecte des ressources fédérales à une question qui, pour eux, se gère bien par le secteur privé. On note aussi certaines craintes à l'égard du gouvernement du Canada vu ses propres problèmes liés aux systèmes informatiques, ce qui met en doute la capacité du gouvernement du Canada à devenir un conseiller de confiance en la matière.

L'idée d'exiger un certain niveau en matière de cybersécurité pour exploiter une entreprise au Canada a suscité des réactions mitigées. À la base, la plupart s'entendent sur le fait que les PME doivent offrir un niveau minimum de cybersécurité. Certains se disent préoccupés par une approche universelle puisque certaines entreprises doivent assurer un niveau de sécurité supérieur à d'autres en fonction de la quantité et la nature de la collecte de renseignements d'une entreprise. Dans le même ordre d'idées, certains participants des deux groupes s'inquiètent que des exigences en matière de cybersécurité puissent être injustes envers les petites entreprises qui n'ont pas les ressources ou les moyens de satisfaire aux exigences.

L'évaluation générale des concepts

Les participants aux groupes de discussion ont évalué trois différents concepts visuels. Ils ont commenté l'attrait et la pertinence globale des concepts et ont donné leurs impressions à savoir si ceux-ci se prêtent bien à un programme de certification sur la cybersécurité.

Les commentaires suivants s'appliquent aux trois concepts :

- La feuille d'érable rouge constitue un symbole canadien fort pour chaque concept.
- La feuille d'érable seule ne suffit cependant pas pour indiquer que le gouvernement du Canada endosse le programme ou qu'il s'agit d'un programme du gouvernement du Canada.
- Plusieurs participants trouvent que les concepts paraissent trop simples et que n'importe quelle entreprise pourrait reproduire et afficher le logo sans pour autant détenir la certification. Il faut pouvoir valider l'authenticité du certificat.
- On a bien reçu les concepts bilingues – certains les préféraient aux concepts unilingues.
- Les francophones ont décidément aimé le langage utilisé dans la version anglaise des concepts, mais ont trouvé la version française déficiente. Plus particulièrement, ils ont remis en question l'utilisation du mot « fiable » - certains trouvaient qu'il n'était pas suffisamment robuste ou percutant alors que d'autres ne trouvaient pas qu'il se prêtait bien à la cybersécurité.
- Certains participants aimeraient que le mot « certifié » soit intégré au concept de manière à informer qu'il s'agit d'une certification, et non d'un logo d'entreprise ou de produit.

Les commentaires propres à chaque concept sont résumés ci-dessous :

- Concept A (bouclier) : Plusieurs ont aimé l'image puisqu'elle rend bien l'aspect de sécurité; ils ont aussi aimé la police de caractère utilisée avec le concept. D'autre part, bien qu'elle communique la sécurité, on ne considère pas l'image unique puisque d'autres entreprises du domaine de la sécurité utilisent le bouclier dans leur logo.
- Concept B (cadenas) : Le concept communique clairement l'aspect « sécurité » - presque tous les participants ont tout de suite reconnu le cadenas. Certains ont aimé l'incorporation d'un « C » pour cyber et d'un « S » pour sécurité dans la conception du cadenas. Cependant, certains y ont vu un cadenas ouvert, suggérant un manque de sécurité. Plusieurs auraient préféré deux types de polices (semblable à celles utilisées dans les deux autres concepts).
- Concept C (voûte) : Le seul avantage du concept est que certains l'ont trouvé unique. En revanche, on a souvent rejeté ce concept parce que des participants ne pouvaient pas identifier ce que l'image représentait et qu'il ne transmettait pas l'aspect « sécurité ». On a aussi trouvé la police de caractère inadéquate et « manquant de sérieux ».

Dans l'ensemble, les consommateurs aiment mieux, dans une large mesure, le concept du cadenas alors que le choix des PME se partage entre le concept du bouclier et celui du cadenas. Le concept de la voûte s'est classé bon dernier dans les deux groupes. Un concept plus fort pour bon nombre des participants combine l'image du cadenas et la police de caractère utilisée dans le concept du bouclier.

L’exploration d’un programme composé d'échelons

Les consommateurs et les PME ont tous deux largement rejeté la notion d’un programme composé d'échelons. Ils préfèrent un programme qui précise si une entreprise est cybersécuritaire ou si elle ne l’est pas. Les principales préoccupations des participants face aux échelons sont :

- Les consommateurs ont trouvé qu’il faut déjà suffisamment d’efforts pour remarquer le logo, et plus encore pour les échelons. De plus, même s’ils les remarquent, ils croient qu’il faudrait beaucoup de temps pour se familiariser avec le programme et comprendre la différence entre les échelons.
- Les PME considèrent ne pas vouloir rendre les échelons publics, particulièrement s’ils ne se trouvent pas à l’échelon le plus élevé. Elles s’inquiètent du fait que leurs clients s’interrogeraient sur le niveau de cybersécurité, peu importe la signification des échelons.
- Certaines PME ont carrément indiqué qu'elles ne publiciseront pas leur niveau si elles se trouvent « seulement au premier échelon » – elles considèrent que le message suggère des mesures moindres en matière de cybersécurité, ce qui nuirait à leur entreprise, et de plus, les identifierait comme une cible pour les pirates informatiques.
- En examinant la manière de communiquer les échelons aux clients à l’aide des logos, plusieurs participants s’entendent que l’intégration des échelons aux concepts visuels les encombre.

L’usage de couleurs dans les concepts visuels

Les participants ont souvent réagi immédiatement et de manière décisive face aux couleurs présentées : peu d’entre eux les ont aimées. S’ils étaient contraints de choisir, les participants opteraient soit pour le statu quo (c.-à-d. le concept en noir et blanc) ou ils choisiraient le gris parmi les couleurs proposées.

Quoique la plupart des participants n’aiment tout simplement pas les couleurs présentées, certains trouvent que l’ajout d’une couleur affaiblissait le ton général ou le message véhiculé par le concept visuel. Ils considèrent que le concept de sécurité doit être transmis par une couleur plus sérieuse ou plus « dure » que les couleurs présentées.

L’impact possible sur la concurrence

Les consommateurs s’avèrent peu enclins à modifier leurs habitudes de magasinage selon qu’une entreprise a ou non une cybercertification, surtout parce qu’ils font confiance aux entreprises avec lesquelles ils font affaire en ce moment. Les consommateurs ne cesseront pas de faire affaire avec une PME en l’absence de certification.

Les PME ont une opinion partagée à savoir si le fait de détenir une certification aura un impact positif sur leur entreprise. Les PME qui s’intéressent à la cybercertification supposent qu’elle peut devenir un différentiateur concurrentiel, que les consommateurs la remarqueront, et qu’elle pourrait les aider à devenir une meilleure entreprise en étant plus proactives et plus « sensibilisées » à la cybersécurité. Pour plusieurs PME, l’impact de la certification sur leur entreprise dépend largement de l’intérêt et de la compréhension des consommateurs face au programme, de ce que la certification représente pour le consommateur et de ce que la PME a dû faire pour obtenir sa certification.

- Certaines PME se rendent compte que les consommateurs ne reconnaitront pas le programme du jour au lendemain et que l'impact sur leur entreprise pourrait prendre du temps à se faire sentir, impression partagée par certains consommateurs.

Outre sur la vitrine d'un magasin ou sur un site Web, les participants s'attendent à voir ou à utiliser les logos à différents endroits, par exemple sur l'emballage, à la caisse enregistreuse ou près des dispositifs de points de vente, dans la publicité, sur les cartes professionnelles, les factures et dans les signatures de courriel.

Les attentes face au programme

Les participants, et particulièrement les consommateurs, ont eu peine à décrire ce à quoi le programme devrait ressembler. Les PME et les consommateurs voient du même œil certains des principaux éléments du programme, dont plusieurs portent sur le rôle du gouvernement du Canada, et qui comprennent les points suivants :

- Le gouvernement fédéral offrirait à tous ceux qui détiennent une certification l'accès à de la formation, à des lignes directrices et aux pratiques exemplaires en matière de cybersécurité.
- Il devrait y avoir une forme d'audit de la certification et la plupart des participants présument qu'un expert en informatique qui travaille pour le compte du gouvernement du Canada s'en chargerait (plutôt que de sous-traiter à une tierce partie).
- Il faudrait inclure le renouvellement périodique de la certification.

La perspective des consommateurs

Les consommateurs sont d'avis que le programme devrait comprendre un volet important d'éducation publique. Les consommateurs veulent connaitre certains détails du programme, par exemple, qu'est-ce qu'on certifie, quelle est la pertinence de la certification pour le consommateur et quelles exigences une entreprise doit satisfaire pour obtenir sa certification. Au final, les consommateurs veulent que les détails qui entourent le programme deviennent publics pour comprendre les avantages qu'ils en retireront.

Si le programme voyait le jour, bon nombre de consommateurs se sentiraient plus en sécurité lorsqu'ils font affaire avec les PME en général, même s'ils ne recherchent pas activement des assurances en matière de cybersécurité dans leurs transactions avec les PME.

Quelques consommateurs reconnaissent les avantages que le programme pourrait procurer aux PME canadiennes de manière générale, même s'ils n'y voient aucun impact direct pour eux en tant que consommateurs. Si le programme se veut un effort du gouvernement du Canada pour appuyer les PME dans leur quête pour accroître leur niveau de cybersécurité, en particulier celles qui ne pourraient pas y arriver d'elles-mêmes, ils perçoivent alors le programme comme une mesure favorable aux petites entreprises.

La perspective des PME

Les PME qui ont participé à la recherche ont des attentes plus précises face au programme :

- Elles veulent s'assurer que le programme soit utile et que la certification et son renouvellement n'ajoutent pas de lourdeur administrative aux entreprises.
- L'audit pourrait comprendre une inspection sur les lieux ainsi qu'une vérification externe (p. ex., qu'un auditeur tente de pirater le système de la PME).
- Elles veulent que le programme soit accessible financièrement aux plus récentes et aux plus petites entreprises. La plupart s'attendent à ce que le processus de certification soit gratuit, offert à faible coût ou à un coût proportionnel à la taille de l'entreprise afin de maximiser l'adoption du programme par les entreprises de tous les domaines et de toutes les tailles.

Si le programme voit le jour, il semble que l'accroissement de la confiance des PME envers leur propre niveau de cybersécurité serait minimal. Plusieurs d'entre elles demeurent passablement indifférentes au programme, n'étant pas convaincues qu'elles aient besoin d'obtenir la certification.

En l'absence de renseignements précis sur le programme, comme les coûts et le processus de certification, plusieurs PME hésitaient à prédire toute modification de leur niveau de confiance à la suite de la mise en place du programme voire même l'obtention de leur certification.

Le rôle du gouvernement

Parmi les rôles les plus fréquents, les participants croient que le gouvernement du Canada devrait :

- Faire la promotion du programme au public pour s'assurer que celui-ci comprenne bien ce que la certification signifie.
- Établir les normes liées à la certification.
- Mener les audits, la certification et le renouvellement de la certification, y compris des évaluations spécifiques qui permettent de s'assurer que les entreprises certifiées continuent d'être sécuritaires.
- Offrir les outils et les ressources pour valider l'authenticité du certificat d'un fournisseur.
- Offrir des ressources pour la formation des employés, des listes de vérification, des ressources et des outils éducatifs et des pratiques exemplaires pour appuyer les efforts d'obtention et du maintien de la certification.
- Offrir un certain soutien aux entreprises « piratées » malgré leur certification.
- Poursuivre en justice les pirates informatiques et autres cybercriminels de manière plus proactive.
- Sensibiliser les Canadiens et les Canadiennes à leur propre cybersécurité.

Méthodologie

Pour réaliser cette recherche, on a mené 10 groupes de discussion traditionnels en personne, six groupes de discussion par webconférence (téléweb), et cinq entrevues en profondeur par téléweb. Des

consommateurs âgés de plus de 18 ans de genre, de niveau d'éducation et de revenu différents ont participé à cinq groupes de discussion en personne. On a réalisé toutes les autres séances et les entrevues avec des décideurs de petites ou moyennes entreprises ou des personnes qui jouent un rôle important dans l'exploitation et la gestion de l'entreprise et qui ont également des connaissances sur les systèmes d'informatique et les pratiques de gestion des données de l'entreprise.

Les séances ont eu lieu à travers le pays dans des villes de grande taille et de taille moyenne (Calgary, Alb., Victoria, C.-B., Halifax, N.-É., Kitchener, Ont., et Montréal, Qc), de même que dans des régions rurales et éloignées à travers le Canada. Les groupes de discussion ont eu lieu entre le 18 et le 28 mars 2019 alors que les entrevues par webconférence (téléweb) ont eu lieu entre le 25 mars et le 2 avril 2019. La durée de chaque groupe de discussion était de 90 minutes alors que celle des entrevues était de 45 minutes. Rick Nadeau et Eva Gastelum, chercheurs principaux chez Quorus et tous deux sur la liste de l'offre à commandes du gouvernement du Canada, ont animé tous les groupes de discussion.

Avis de non-responsabilité pour la recherche qualitative

La recherche qualitative vise à obtenir un aperçu et une orientation plutôt que des mesures quantitatives pouvant être extrapolées. Le but n'est pas de générer des statistiques, mais bien de recueillir un éventail complet d'opinions sur un sujet donné, de comprendre le langage utilisé par les participants, d'évaluer leur degré de passion et d'engagement, et de tirer parti du pouvoir du groupe pour faire ressortir des idées. Les participants sont invités à exprimer leurs opinions, peu importe qu'elles soient partagées ou non.

En raison de la taille de l'échantillonnage, des méthodes de recrutement spéciales utilisées et des objectifs de la recherche, il est clairement entendu que les travaux faisant l'objet de la discussion sont de nature exploratoire. Les résultats ne peuvent ni ne doivent être extrapolés à une population plus vaste.

Il serait également inapproprié de suggérer ou d'insinuer que quelques utilisateurs réels (ou bon nombre d'entre eux) se comporteraient d'une certaine façon simplement parce que quelques participants (ou bon nombre d'entre eux) se sont comportés de cette façon durant les séances. Ce type de projection relève strictement de la recherche quantitative.

Fournisseur : Le groupe-conseil Quorus Inc.
Numéro de contrat SPAC : U1400-198102/001/CY
Date d'octroi du contrat : Le 5 mars 2019
Valeur du contrat (TVH incluse) : 129 006,45 $
Pour de plus amples renseignements, veuillez communiquer avec Innovation, Sciences et Développement économique Canada, à : IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca