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

Innovation, Sciences et Développement économique Canada

CyberSécuritaire Canada : Promouvoir la cybersécurité et la sensibilisation auprès des entreprises canadiennes

Sommaire

Août 2021

Préparé pour Innovation, Sciences et Développement économique Canada
Fournisseur : Le groupe-conseil Quorus Inc.
Date d'octroi du contrat : 6 janvier 2021
Numéro de contrat : U4408-210641/001/CY
Valeur du contrat : 59 944,96 $
Date de livraison : septembre 2021
Numéro de ROP : ROP 098-20
Pour plus d'information, veuillez communiquer avec Innovation, Sciences et Développement économique Canada : IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca

This report is also available in English.

Canada

Cette publication est disponible en ligne à l'adresse suivante : https://www.ic.gc.ca/eic/site/112.nsf/eng/home.

Pour obtenir une copie de la présente publication ou la recevoir sous une autre forme (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande à www.ic.gc.ca/Publication-Request ou communiquer avec :

Centre des 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
ATS (pour les personnes malentendantes) : 1 866 694-8389
Heures d'ouverture : 8 h 30 à 17 h (heure de l'Est)
Courriel : ISED@canada.ca

Numéro de catalogue : Iu4-266/1-2019E-PDF

ISBN 978-0-660-32481-4

Also available in English, entitled *Cyber Secure Canada – Final report*.

Attestation de neutralité politique

J'atteste, par les présentes, à titre de président du groupe-conseil Quorus, que les produits livrables sont entièrement conformes aux exigences en matière de neutralité politique du gouvernement du Canada énoncées dans la *Politique sur les communications et l'image de marque* et la Directive sur la gestion des communications – Annexe C.

Plus précisément, les produits livrables ne comprennent 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.

Sommaire

Contexte et objectifs

En réponse aux menaces à la cybersécurité, le budget de 2018 prévoyait la mise en place d'un programme de certification en cybersécurité pour les petites et moyennes entreprises (PME). En partenariat avec le Conseil canadien des normes et le Centre de la sécurité des communications, ISDE a mis sur pied le programme CyberSécuritaire Canada, dont l'objectif consiste à hausser la base de référence en matière de sécurité pour les PME et par conséquent, à accroître la confiance des consommateurs envers l'économie numérique, à promouvoir la normalisation à l'échelle mondiale et à mieux positionner les PME canadiennes afin qu'elles soient plus concurrentielles à l'international.

Pour mieux sensibiliser le public cible, des campagnes publicitaires ont été organisées. La première, lancée en février 2021, était une publicité numérique visant à encourager les PME à se renseigner sur le programme CyberSécuritaire et à obtenir leur certification.

Le principal objectif de la campagne numérique était de bâtir une image de marque et faire connaître le programme CyberSécuritaire Canada et sa marque. Son appel à l'action visait les petites et moyennes entreprises et les encourageait à visiter le site CyberSécuritaire Canada à https://www.ic.gc.ca/eic/site/137.nsf/fra/accueil.

Les principaux objectifs de la recherche sur l'opinion publique consistaient à tester les concepts publicitaires et leurs messages sous-jacents en faisant participer des PME à des groupes de discussion en ligne (plateforme virtuelle) avant le lancement de la campagne. La recherche avait également pour but de recueillir les opinions des petites et moyennes entreprises sur la cybersécurité en général et le programme CyberSécuritaire en particulier. La recherche visait à recueillir les renseignements suivants :

a. Des points de vue et des réactions envers plusieurs concepts publicitaires
b. Les aspects favoris des concepts publicitaires présentés
c. Si les participants comprenaient les messages (écrits et visuels) et leur crédibilité
d. Les moyens de communication favoris pour l'ensemble de la campagne publicitaire et de marketing
e. Les réactions à l'égard du programme CyberSécuritaire ainsi que le niveau d'intérêt et de confiance envers celui-ci

La deuxième phase de la recherche consistait en des entrevues personnelles en profondeur sur le Web réalisées auprès d'un éventail de grandes entreprises, de groupes et d'associations de l'industrie, et avait pour but d'approfondir la discussion sur les points suivants :

a) Pour les représentants des groupes ou des associations de l'industrie, la recherche visait à découvrir l'importance de la cybersécurité pour l'industrie en général, les effets de la pandémie, l'état de préparation de l'industrie en matière de cybersécurité et ce qui doit se produire pour que l'industrie s'améliore.
b) Pour les représentants des entreprises du secteur privé qui peuvent compter sur une importante chaîne logistique, la recherche avait pour but de recueillir des points de vue sur l'état de préparation des organisations en matière de cybersécurité, les effets de la pandémie et plus particulièrement, les opinions quant à leur façon de gérer la cybersécurité des chaînes logistiques et l'état actuel de cette gestion.
c) La connaissance du programme CyberSécuritaire et l'intérêt envers celui-ci, les obstacles à son utilisation, les perceptions quant au rôle du gouvernement du Canada et les implications pour les chaînes logistiques ou les membres de leur industrie, le cas échéant.

Méthodologie

La première phase de recherche consistait en dix groupes de discussion en ligne; huit groupes ont participé à l'étape 1 du 25 au 28 janvier 2021, et les deux autres, l'étape 2 le 16 février 2021. Les participants étaient des propriétaires de petites et moyennes entreprises, de même que des représentants d'organismes sans but lucratif de partout au Canada. Lors du recrutement, nous avons priorisé les entreprises comptant de 40 à 100 employés (soit le plus grand segment des petites entreprises). Dans chaque organisation, la recherche visait un responsable des décisions en matière de cybersécurité ou une personne qui joue un rôle de premier plan dans les opérations quotidiennes et la direction de l'entreprise.

Chaque participant a reçu 200 $ pour sa contribution. Au total, des représentants de 54 entreprises ont participé aux groupes de discussion.

La deuxième phase de la recherche consistait en six entrevues individuelles en profondeur sur le Web réalisées avec un éventail de grandes entreprises et de groupes et d'associations de l'industrie.

La liste des organisations invitées à participer à cette phase de l'étude a été préparée par ISDE et le recrutement a été mené par Quorus. Chaque participant a reçu 250 $.

Tous les participants ont été informés que la recherche avait été commandée par le gouvernement du Canada.

Résultats de la recherche

Phase 1 – Groupes de discussion : premier test de concepts

Cybersécurité

Chaque séance a débuté par une discussion générale sur la cybersécurité. Les participants ont souvent utilisé les mots « protection », « information » et « sécurité des systèmes » pour la décrire. Bien que la plupart avaient l'impression que leurs entreprises et leurs systèmes étaient de raisonnablement sécuritaires à assez sécuritaires, les participants s'accordaient tous pour dire qu'il était impossible qu'il soit complètement sécuritaire et qu'il y avait toujours place à amélioration. Assurer la cybersécurité a également été perçu comme une dépense de fonctionnement nécessaire pour les entreprises.

Pratiquement toutes les entreprises ont dû s'adapter jusqu'à un certain point en raison de la pandémie de COVID-19. Elles sont devenues de plus en plus dépendantes à l'Internet, notamment en raison du télétravail qui est à la hausse. Le travail à domicile a apporté son lot de défis sur le plan de la cybersécurité et il a fallu modifier les pratiques (p. ex., en offrant une formation au personnel) et les systèmes (matériel informatique, logiciels, largeur de bande).

Un certain nombre de participants ont discuté des cyberattaques qui se sont produites depuis le début de la pandémie et des coûts associés.

Réactions aux concepts publicitaires

Durant la première ronde de groupes de discussion, trois concepts ont été testés :

- Concept A – Plus facile
- Concept B – Un premier pas
- Concept C – La confiance (une version originale et une variante, testée avec les quatre derniers groupes, avec une image différente)

Certains thèmes sont ressortis durant les discussions sur tous les concepts, y compris le désir des participants de voir un lien plus direct et littéral à la cybersécurité dans l'approche créative. Bon nombre d'entre eux ont également mentionné que le sceau du programme était un élément clé des concepts publicitaires et qu'il devrait être mis de l'avant. Cela aiderait grandement à illustrer le lien plus littéral que les participants recherchent et à atteindre l'auditoire cible (c'est-à-dire les petites et moyennes entreprises) pour transmettre le message principal et le but du nouveau programme.

En revanche, plusieurs étaient d'avis que l'auditoire cible avait déjà saisi l'importance de la cybersécurité et, par conséquent, qu'il n'était pas nécessaire d'en faire le message clé comme c'était le cas dans les concepts testés. Ils ont plutôt suggéré d'ajouter de l'information sur le programme lui-même. Dans les concepts testés, le manque de renseignements à ce sujet a soulevé de nombreuses questions et a amené les participants à faire des suppositions qui n'étaient pas toujours les bonnes. Ceux-ci auraient souhaité qu'on indique clairement que ce programme est commandité par le gouvernement du Canada. Dans les concepts vidéo, ils auraient voulu voir une mention de la commandite beaucoup plus rapidement pour se sentir rassurés quant à la pertinence du message.

La majorité des participants se sont entendus pour dire que les publicités ne réussiraient pas à attirer leur attention. L'appel à l'action pour obtenir plus d'information n'était pas suffisamment fort pour les convaincre de faire leurs propres recherches.

Le *concept A – Plus facile* a obtenu de faibles notes et s'est retrouvé au dernier rang. Cela s'explique entre autres par l'incertitude quant à l'auditoire cible, que les participants croyaient être les consommateurs et non les entreprises. Cette impression était attribuable principalement aux couleurs vives et à l'image de la tarte, éléments qui ont raté la cible puisque le message véhiculé n'a pas été associé à la cybersécurité. En fait, on semblait dire aux gens que la cybersécurité, c'était simple (de la tarte), ce qui ne reflétait pas nécessairement leur expérience. Le texte a soulevé des questions parmi les participants au lieu de les informer sur le programme. Même si l'appel à l'action qui les invitait à cliquer sur le lien pour en apprendre davantage était clair, la plupart des participants ont affirmé que ce concept ne les inciterait pas à agir.

Le *concept B – Un premier pas* a suscité des réactions partagées. Bien que certains participants en aient fait leur premier choix, la plupart l'ont relégué au deuxième rang. Il a cependant fait l'objet de critiques pour son exécution, la perception quant à l'auditoire cible et son message.

Bien que dans l'ensemble, le concept ait été qualifié d'accrocheur, certains l'ont trouvé surchargé et sans rapport avec le caractère sérieux qu'ils associent à la cybersécurité. Malgré les mots inscrits sur l'espadrille, de nombreux participants avaient l'impression que le concept s'adressait aux jeunes ou aux entreprises en démarrage. Certains n'ont vu aucun lien avec la cybersécurité. Par ailleurs, d'autres ont aimé la métaphore qui consiste à « faites un premier pas » ou à « se diriger vers quelque chose », c'est-à-dire la certification en cybersécurité.

Les participants ont saisi l'appel à l'action, mais les réactions étaient partagées à savoir si la publicité était suffisamment convaincante pour inciter les gens à poser le geste qu'on leur demandait – certains ont dit qu'ils le feraient et d'autres non.

Le *concept C – La confiance* s'est distingué et a été le favori des trois concepts présentés. Les participants s'entendaient pour dire que l'idée de la confiance établissait le lien le plus pertinent

et le plus direct avec la cybersécurité et que l'ensemble du concept les ciblait mieux que les deux autres. Cela s'explique par l'approche créative, qui a suscité des réactions favorables, et le message principal qui les a interpellés. L'idée et les images de confiance et les liens (que nous sommes tous dans le même bateau, mais que les liens pourraient facilement être rompus s'il y a un maillon faible) ont plu à la majorité.

Les participants ont souvent mentionné que le ton de ce concept était plus sérieux et plus axé vers les entreprises.

Toutefois, le choix des abeilles a déplu à certains qui auraient préféré voir de vraies personnes dans la publicité.

Dans les quatre derniers groupes, nous avons également présenté aux participants une variante de ce concept : le texte était le même, mais l'image était différente et incluait une personne. Bien que certains s'entendaient pour dire que l'idée d'utiliser une personne plutôt que des insectes était un changement positif, la plupart étaient d'avis que l'exécution dans ce cas ne fonctionnait pas.

Réactions au programme de certification CyberSécuritaire

La présentation des publicités a été suivie d'une brève discussion sur le programme. Même si aucun des participants n'en avait entendu parler, selon la description fournie et les concepts qu'ils venaient de voir, la majorité a dit vouloir en apprendre davantage. Les participants ont cependant fait valoir qu'il faudrait leur fournir plus d'information sur les avantages qu'ils pourraient en tirer et préciser certains détails avant que les entreprises décident d'obtenir leur certification.

Phase 1 – Groupes de discussion : vérification du succès

Deux concepts révisés ont été testés dans deux autres groupes. Il s'agit de ceux-ci :

- Concept A – Les castors
- Concept B – La chaîne de confiance

Les deux concepts ont suscité des avis partagés.

D'après les participants, le *concept A – Les castors* avait un message clair, mais plusieurs se sont demandé si la partie concernant la « chaîne logistique » était un élément important du message ou si elle rebuterait ceux qui n'y voient aucune pertinence pour eux parce qu'ils n'ont pas de chaîne logistique. De nombreux participants auraient aimé voir plus d'information sur le programme lui-même.

Ceux qui ont été attirés vers ce concept ont aimé la façon dont il communique les notions de « travail d'équipe », d'« interconnexion » et de « quelque chose que l'on construit ». L'idée de confiance, la visibilité du logo et la nature canadienne du castor ont également été mentionnées comme étant des éléments positifs du concept.

Ceux qui n'ont pas aimé le concept ont invoqué l'absence de lien entre le castor et la cybersécurité, avec les gens ou les TI. D'autres l'ont qualifié de « mignon » alors qu'un ton sérieux aurait été plus approprié, compte tenu du sujet.

Le *concept B – La chaîne de confiance* a également divisé les participants. Ceux en faveur ont mentionné l'image montrant plusieurs personnes qui travaillent ensemble, la visibilité du logo du gouvernement du Canada et la légitimité qu'il confère au programme, et l'accent sur la confiance. L'exécution globale a plu à certains participants qui seraient attirés par ce concept.

Cependant, pour la majorité des participants, le style dessin animé n'a pas atteint sa cible. Ceux qui ne l'ont pas aimé ont expliqué qu'il ne convenait pas, qu'il manquait de sérieux ou qu'il n'était pas représentatif de la cybersécurité. Certains participants étaient également d'avis que ce concept ne s'adressait pas à tous les auditoires cibles ni à toutes les entreprises, mais qu'il plairait surtout aux jeunes ou aux entreprises en démarrage.

Phase 2 – Entrevues en profondeur avec les intervenants

Préparation à la cybersécurité

Comme nous l'avons constaté dans les groupes de discussion, selon les participants, on peut toujours faire mieux sur le plan de la cybersécurité, peu importe le niveau de préparation.

Les principaux facteurs d'évaluation de la préparation en cybersécurité mentionnés par les participants étaient les suivants :

- Le volume de données de l'industrie : les participants œuvrant dans une industrie où les données sont un élément essentiel des opérations quotidiennes étaient plus enclins à accorder plus d'importance et à affecter plus de ressources à la cybersécurité.
- La taille de l'entreprise : il s'agit d'un facteur clé et les participants ont affirmé que plus l'entreprise est grande, plus ses ressources sont nombreuses et plus élevée est la probabilité qu'elle ait mis en place des normes élevées en matière de cybersécurité. Les petites entreprises ou organisations (comme celles du secteur des soins de santé) ont affirmé que la cybersécurité n'était ni leur champ d'expertise ni leur priorité.
- Le budget : les coûts peuvent représenter un obstacle qui nuit à la préparation en cybersécurité.

- Le manque de connaissances : ce ne sont pas toutes les entreprises qui ont l'expertise nécessaire pour améliorer leur niveau de cybersécurité.
- L'absence d'attentes ou de pressions extrinsèques : dans certaines industries, les attentes des clients ou des organismes de réglementation pour le maintien de certaines normes relativement à la cybersécurité sont faibles ou inexistantes.
- Le niveau de différenciation concurrentielle que la cybersécurité peut apporter à une entreprise : cela varie grandement d'un secteur à l'autre.

Considérations relatives à la chaîne logistique

Durant les entrevues avec les représentants de grandes entreprises du secteur manufacturier et des soins de santé spécialisés, les participants ont discuté de la gestion de la chaîne logistique. Malgré la grande taille de ces entreprises qui leur permettait de disposer des ressources et du personnel nécessaires pour assurer la gestion des TI, de la cybersécurité et de la chaîne logistique, ces deux types d'organisations avaient des approches différentes pour gérer les données.

Alors que les entreprises du secteur de la fabrication ont tendance à gérer elles-mêmes leurs données internes et à en faire une priorité (comparativement aux données provenant de tiers, comme des clients ou des fournisseurs), les organisations du secteur des soins de santé doivent souvent composer avec des données personnelles provenant du grand public, ce qui rend le tout plus complexe et qui requiert une approche plus sophistiquée en matière de sécurité. De plus, en raison de la sensibilité des données qu'elles hébergent et partagent, le niveau d'inquiétude quant à la façon dont les fournisseurs recueillent et gèrent les données est plus élevé.

Alors que pour les entreprises manufacturières, la cybersécurité ne représente pas une considération logistique dans le choix des fournisseurs ni une source de préoccupation constante une fois que la relation avec un fournisseur est établie, pour les entreprises du secteur des soins de santé, le niveau de cybersécurité des fournisseurs est extrêmement important.

Rôle du gouvernement du Canada en matière de cybersécurité

Les participants s'entendaient pour dire que le gouvernement du Canada a un rôle à jouer pour soutenir les entreprises afin qu'elles atteignent un niveau de cybersécurité acceptable. Les types de soutien mentionnés pourraient être classés en quatre grandes catégories : éducation et formation, soutien et incitatif, établissement de normes, et mesures additionnelles pour lutter contre les cybercriminels.

Lorsque nous leur avons mentionné que le gouvernement du Canada pourrait exiger des niveaux de cybersécurité, les participants ont bien compris pourquoi. Certains y ont vu des avantages et

d'autres, des inquiétudes. La plupart étaient d'avis qu'il faudrait considérer cela comme un système de soutien et non un système punitif. Des participants ont également parlé de la mise en application, alors que d'autres se sont demandé si on imposerait cette exigence à tous les types d'entreprises ou uniquement aux fournisseurs internationaux.

Réactions au programme CyberSécuritaire Canada

Nous avons présenté aux participants un aperçu du programme et de la certification. Les connaissances étaient modérées, mais l'intérêt était grand. Plusieurs ont parlé de la valeur ajoutée du programme pour leur industrie. Certains ont indiqué qu'ils le suggéreraient à leurs fournisseurs ou au reste de leur industrie. Le programme a généralement été perçu comme étant approprié et assez exhaustif.

Parallèlement, certains participants ont exprimé des inquiétudes. Celles-ci concernaient principalement (le manque de) capacités et d'expertise à l'interne, et les coûts pour combler les lacunes en cybersécurité et obtenir la certification. Certains avaient l'impression qu'il serait difficile d'avoir une norme ou une certification qui serait appropriée pour toutes les industries. Cependant, ceux qui avaient déjà des normes de cybersécurité propres à leur industrie ont mentionné qu'ils seraient disposés à collaborer avec le gouvernement du Canada.

Mise en garde concernant la recherche qualitative

La recherche qualitative vise à obtenir des points de vue et à trouver une orientation plutôt que des mesures qualitatives qu'on peut extrapoler. Le but n'est pas de générer des statistiques, mais d'obtenir l'éventail complet des opinions sur un sujet, comprendre le langage utilisé par les participants, d'évaluer les niveaux de passion et d'engagement, et d'exploiter le pouvoir du groupe pour stimuler les réflexions. Les participants sont encouragés à exprimer leurs opinions, peu importe si ces opinions sont partagées par d'autres.

En raison de la taille de l'échantillon, des méthodes particulières de recrutement utilisées et des objectifs de l'étude eux-mêmes, il est clair que la tâche en question est de nature exploratoire. Les résultats ne peuvent être extrapolés à une plus vaste population, pas plus qu'ils ne visaient à l'être.

Plus particulièrement, il n'est pas approprié de suggérer ni de conclure que quelques (ou de nombreux) utilisateurs du monde réel agiraient d'une façon uniquement parce que quelques (ou de nombreux) participants ont agi de cette façon au cours des séances. Ce genre de projection est strictement l'apanage de la recherche quantitative.

Fournisseur : Le groupe-conseil Quorus Inc.
Numéro de contrat de SPAC : U4408-210641/001/CY
Date d'octroi du contrat : 6 janvier 2021
Valeur du contrat (TVH incluse) : 59 944,96 $
Pour plus d'information, contacter Innovation, Sciences et Développement économique Canada à :
IC.PublicOpinionResearch-Recherchesurlopinionpublique.IC@canada.ca