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

*Rapport final*

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

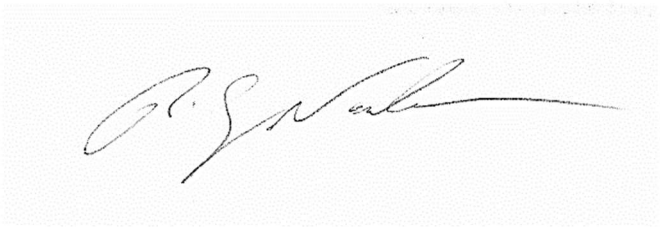
Also available in English, entitled *Cyber Secure Canada – Final report*.

## 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.

# Table des matières

**Sommaire** ..... **5**
Contexte et objectifs ..... 5
Méthodologie ..... 6
Résultats de la recherche ..... 7
**Résultats détaillés** ..... **14**
**But et objectifs de la recherche** ..... **15**
**Phase 1 – Groupes de discussion : test de concept initial** ..... **18**
Cybersécurité ..... 18
Réactions aux concepts publicitaires ..... 20
Réactions au programme de certification CyberSécuritaire ..... 31
**Phase 1 – Groupes de discussion : vérification du succès** ..... **33**
**Phase 2 – Résultats : entrevues en profondeur avec les parties intéressées** ..... **38**
Préparation en matière de cybersécurité ..... 38
Considérations relatives à la chaîne logistique ..... 41
Rôle du gouvernement du Canada en matière de cybersécurité ..... 43
Réactions au programme CyberSécuritaire Canada ..... 45
**Méthodologie détaillée** ..... **48**
Groupes cibles et échantillon ..... 49
Description des procédures de collecte des données ..... 50
**Annexes** ..... **54**
Questionnaire de recrutement – Groupes de discussion ..... 55
Guide de l'animateur – Groupes de discussion ..... 62
Guide de l'animateur – Entrevues avec les parties intéressées (phase 2) ..... 74

# 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**

# Résultats détaillés

# But et objectifs de la recherche

Les cyberattaques peuvent avoir des répercussions directes sur une organisation et ses clients, y compris des pertes financières et une atteinte à la réputation. En devenant cybersécuritaires, les petites et moyennes entreprises (PME) peuvent améliorer leurs pratiques de cybersécurité et ainsi gagner la confiance des clients, protéger leurs données et leurs finances, et renforcer leur avantage concurrentiel.

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.

Le programme CyberSécuritaire permet aux PME de démontrer qu'elles prennent les mesures appropriées pour défendre leurs systèmes, renforcer leur résilience contre les cyberattaques et protéger les renseignements des clients et des fournisseurs. La certification CyberSécuritaire est renouvelable tous les deux ans. Les entreprises certifiées peuvent afficher la marque de certification sur leurs sites Web, la devanture de leur commerce et leur matériel promotionnel.

La campagne est une promotion publicitaire numérique qui vise à encourager les PME à se renseigner sur le programme CyberSécuritaire et à obtenir leur certification. Le site Web CyberSécuritaire Canada (https://www.ic.gc.ca/eic/site/137.nsf/fra/accueil) fournit aux entreprises et aux consommateurs de l'information sur les pratiques exemplaires en matière de cybersécurité et de protection des renseignements des clients et des fournisseurs. Il offre également aux entreprises une vue d'ensemble complète du programme de certification CyberSécuritaire et son fonctionnement, et les invite à s'inscrire au programme en vue d'obtenir leur certification.

Le principal objectif de la campagne numérique est d'accroître la notoriété de la marque et promouvoir le programme CyberSécuritaire Canada et sa marque. L'appel à l'action de la campagne vise les petites et moyennes entreprises et les invite à se rendre sur le site Web (https://www.ic.gc.ca/eic/site/137.nsf/fra/accueil).

Ce projet met l'accent sur la recherche sur l'opinion publique requise pour appuyer la campagne publicitaire de 2020-21 en vue d'atteindre ses objectifs et mieux comprendre comment les

entreprises réagissent aux nouvelles exigences en matière de cybersécurité dans le contexte de la pandémie de COVID-19, laquelle a forcé les entreprises à se tourner vers le télétravail et les activités en ligne, en plus de composer avec une augmentation du nombre de cyberattaques.

La première phase de l'étude avait comme principal objectif de tester les concepts et les messages sous-jacents avec des groupes de discussion composés de représentants de PME sur une plateforme en ligne (virtuelle). La recherche avait pour but de recueillir les renseignements suivants :

a. les points de vue et les réactions à l'égard d'une série de concepts publicitaires destinés à promouvoir la certification en cybersécurité;
b. les éléments des concepts publicitaires qui ont particulièrement plu aux participants;
c. la compréhension des participants à l'égard du message (écrit et visuel) véhiculé dans les publicités proposées et de sa crédibilité;
d. les moyens de communication préférés pour la publicité et la campagne de marketing; et
e. les réactions, l'intérêt et la confiance envers le programme CyberSécuritaire.

Au terme du projet, nous avons utilisé ces renseignements pour sélectionner le meilleur concept, les messages et autres éléments à privilégier pour chaque auditoire cible, et déterminer quels étaient les changements à apporter avant la production finale et le placement média.

Au-delà des concepts et des messages testés, nous voulions observer la réaction des entreprises aux exigences en matière de cybersécurité dans le contexte de la pandémie mondiale de COVID-19, de même que l'approche qu'elles privilégient pour atténuer les risques. La pandémie a modifié leurs perceptions et leur état de préparation à la cybersécurité; elles ont besoin de bases solides en cybersécurité pour s'adapter au nouvel environnement numérique. Une recherche antérieure menée pour ISDE avait permis de détecter d'importantes lacunes au niveau des connaissances, des petites entreprises en particulier, mais également des moyennes entreprises, notamment en ce qui concerne la gestion de la chaîne logistique. Nous avons donc testé ce qui suit :

a. la connaissance des pratiques en matière de cybersécurité;
b. la connaissance des répercussions des cyberattaques sur les activités commerciales;
c. les résultats attendus, de même que les obstacles liés à la certification; et
d. les défis et les obstacles liés à la cybersécurité dans l'environnement actuel, y compris les répercussions de la crise engendrée par la COVID-19.

Au terme du projet, ces renseignements permettront d'améliorer les communications, les campagnes de marketing et les efforts de sensibilisation d'ISDE pour appuyer son mandat qui consiste à aider les entreprises et les consommateurs et cela, grâce à une meilleure compréhension des entreprises et de leurs perceptions de la proposition de valeur du programme CyberSécuritaire et du processus de certification.

La deuxième phase de la recherche était axée sur les grandes entreprises, les groupes et les associations de l'industrie. Son objectif consistait à approfondir la discussion sur les thèmes 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.

# Phase 1 – Groupes de discussion : test de concept initial

Pour nous aider à acquérir une compréhension initiale du contexte dans lequel un programme de certification pourrait être lancé, le thème général de la cybersécurité a été abordé avec les participants. Plusieurs aspects ont été examinés, de la perception des PME quant au niveau de cybersécurité qu'elles ont atteint, à la façon dont elles ont dû s'adapter en raison de la pandémie. Après la discussion, nous avons testé trois concepts publicitaires.

## Cybersécurité

**Confiance à l'égard de la cybersécurité**

De façon générale, les participants ont décrit la cybersécurité comme étant la « protection de l'information sur Internet », « l'attention portée à ce qui circule dans nos systèmes et à la sécurité de ces interactions ou des communications », « la protection de toutes les ressources numériques » et « la mise en place de mesures de contrôle et de processus pour se défendre contre les attaques potentielles ».

Lorsque nous leur avons demandé jusqu'à quel point leurs entreprises et leurs systèmes étaient « cybersécuritaires », la plupart des participants ont répondu qu'ils se sentaient plutôt bien protégés ou « raisonnablement positifs », et croyaient avoir les bons systèmes, les bonnes procédures et les bonnes technologies en place. Certains participants, principalement ceux qui avaient récemment fait l'objet d'un audit de sécurité ou qui avaient fait des mises à niveau, se sentaient bien protégés. Pour ceux qui se sentaient moins bien protégés, ce sentiment avait moins à voir avec leurs systèmes, et davantage avec l'impression que les niveaux de menaces avaient atteint un sommet dans la dernière année, comparativement à la période prépandémique. Ces participants se sentaient plus vulnérables dans des secteurs qui leur étaient moins familiers ou dans d'autres où ils se sentaient relativement bien protégés dans le passé.

Les participants s'entendaient pour dire qu'il était impossible d'être entièrement protégés et qu'on pouvait toujours faire mieux, et un besoin de continuer à évaluer le niveau de protection et de l'améliorer en tenant compte des nouveaux risques.

Quelques entreprises, surtout celles de petite taille, n'étaient pas certaines de ce qui devrait être mis en place pour assurer leur pleine cybersécurité, ou de ce qui pourrait être fait sans que les coûts soient trop exorbitants.

L'investissement dans la cybersécurité est en grande partie considéré comme un prix à payer qui est acceptable et nécessaire pour faire des affaires, et qui doit constamment figurer dans la colonne des dépenses d'une entreprise. C'est un élément qui est examiné sur une base constante ou régulière, qui attire plus d'attention et d'investissements au fur et à mesure des besoins, que ce soit en raison de nouvelles circonstances (p. ex., le nombre accru d'employés en télétravail), de menaces ou d'atteintes à la sécurité. Certaines grandes entreprises peuvent compter sur du personnel à l'interne pour s'occuper des TI et de la cybersécurité, alors que d'autres font appel à des fournisseurs externes pour remplir ces tâches.

Bien que les cyberattaques provenant de l'extérieur aient pu inquiéter les participants, ceux-ci ont souvent mentionné que leur sentiment de sécurité était directement lié aux comportements de leurs employés, et la confiance qu'ils avaient en ces derniers pour prendre la sécurité au sérieux et respecter toutes les règles et tous les protocoles. Même si certains étaient convaincus que leurs employés ne « cliquaient pas sur tous les liens qu'ils reçoivent » et qu'ils signalaient toutes les menaces ou les atteintes potentielles, d'autres ont indiqué qu'avec les pirates informatiques qui deviennent de plus en plus créatifs et sophistiqués, les risques liés aux comportements humains susceptibles de rendre leur entreprise vulnérable demeurent un sujet d'inquiétude.

**Changements attribuables à la pandémie et façons pour les entreprises de s'adapter**

Presque tous les participants s'entendaient pour dire que la pandémie avait fait en sorte qu'ils avaient accru leur présence en ligne et dépendaient de plus en plus de l'Internet. La majorité des entreprises se sont adaptées en introduisant ou en augmentant le télétravail, et dépendaient de plus en plus des plateformes de vidéoconférence comme Zoom, Google Meet ou Microsoft Teams. Des participants ont également mentionné que certains employés qui, auparavant, n'avaient jamais été tenus d'utiliser la technologie à ce point, voire pas du tout, comme ceux qui visitaient les lieux de travail ou qui travaillaient dans des entrepôts ou des usines, avaient dû s'adapter à la technologie ou tenter de reproduire des interactions en personne avec des clients ou des fournisseurs, et qu'une formation à la volée était souvent requise.

Certains participants avaient aussi constaté une hausse des activités liées au commerce électronique.

Le simple fait que les gens travaillaient de la maison et utilisaient leur propre connexion Internet plutôt que celle du bureau donnait souvent l'impression d'une cybersécurité et d'un contrôle moindre sur les activités en ligne.

Bon nombre de participants dont les entreprises avaient connu une hausse du télétravail ont indiqué qu'ils avaient déjà mis en place des systèmes et des technologies. Presque tous ceux qui

employaient un grand nombre de télétravailleurs ont expliqué qu'ils avaient dû apporter des ajustements afin d'accommoder ces travailleurs, et le faire de façon sécuritaire, notamment :

- en augmentant le matériel informatique (en s'assurant que chaque travailleur avait un ordinateur portable ou un téléphone, et une capacité de serveur suffisante);
- en augmentant les logiciels (comme le VPN, la protection antivirus); et/ou
- en augmentant la largeur de bande.

Certains ont mentionné qu'ils avaient dû offrir une formation additionnelle aux employés en situation de télétravail pour la première fois, dont une formation sur la façon d'assurer sa cybersécurité à la maison. Dans l'ensemble, les participants avaient le sentiment que depuis le début de la pandémie, les employés avaient pris davantage conscience de leurs responsabilités et leurs comportements lorsqu'il s'agit d'utiliser la technologie et les ressources en ligne. Ils ont toutefois admis qu'une formation continue ou des rappels étaient nécessaires.

La majorité des participants croyaient qu'ils avaient fait la transition vers une présence accrue en ligne de façon relativement sécuritaire. Un des plus grands risques demeurait les utilisateurs, souvent leurs propres employés, plutôt que la technologie utilisée, ce qui a mené plusieurs à dire qu'il était important d'offrir au personnel une formation continue dans ce domaine.

Dans presque toutes les séances, un participant a mentionné que depuis le début de la pandémie, son entreprise avait été victime d'une cyberattaque. La plupart des autres ont dit connaître d'autres entreprises qui avaient subi le même sort. Plusieurs ont souligné les coûts importants liés à ces attaques, que ce soit pour effectuer des changements aux systèmes et des mises à niveau après l'incident, ou du nombre d'heures de production perdues en raison de l'attaque. D'autres ont expliqué que leurs systèmes étaient constamment menacés, ou qu'ils avaient constaté une hausse du nombre de pourriels bloqués, mais qu'ils avaient été en mesure de les contenir.

Aucun des participants n'a été étonné d'apprendre que le nombre de cyberattaques avait augmenté depuis le début de la pandémie.

Quelques participants ont expliqué que les clients posaient davantage de questions au sujet de la sécurité des systèmes, mais qu'il ne s'agissait pas d'un sujet récurrent. Encore une fois, seul un petit nombre de participants a mentionné une augmentation du commerce électronique.

## Réactions aux concepts publicitaires

Nous avons présenté aux participants trois concepts publicitaires et les avons informés que ceux-ci avaient pour but de promouvoir un programme de certification en cybersécurité destiné aux petites et moyennes entreprises lancé par le gouvernement du Canada. Chaque concept comportait une publicité imprimée, une bannière (en format vidéo) et une courte vidéo en ligne.

L'ordre de présentation des trois concepts et la discussion qui a suivi variaient d'une séance à l'autre.

Plusieurs thèmes principaux sont ressortis de toutes les discussions :

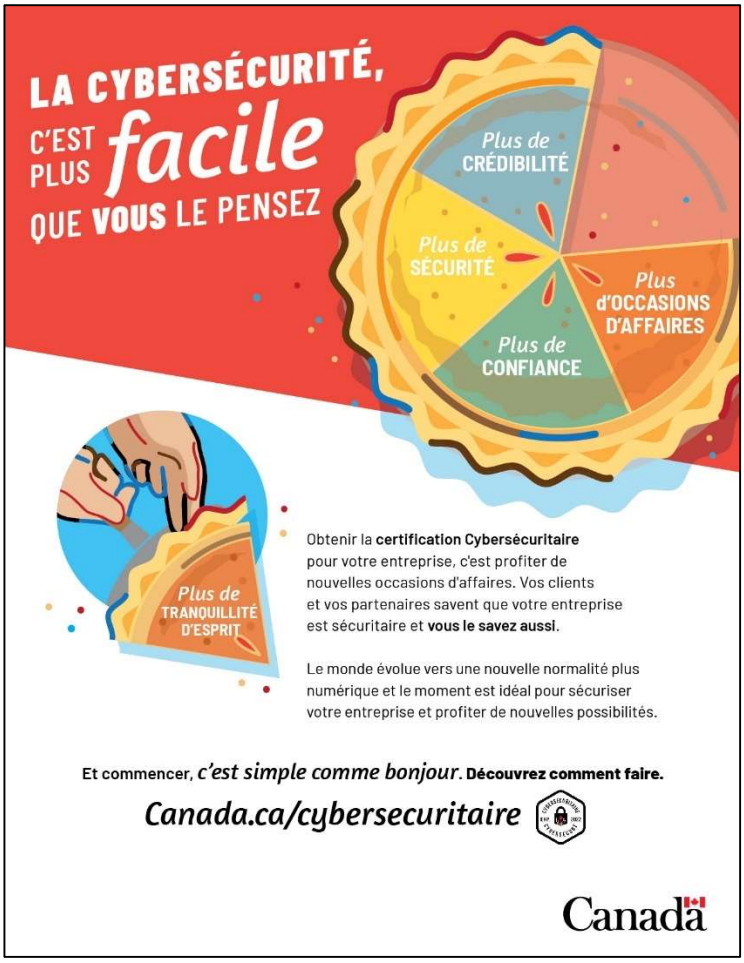
- Les participants cherchaient souvent un lien plus direct et littéral avec la cybersécurité dans l'approche créative. Initialement, ils ont souvent mentionné qu'ils voulaient voir des ordinateurs, des personnages louches, des tons plus sombres, des chambres fortes et ainsi de suite, même si certains croyaient que ces images feraient clichés et n'attireraient peut-être pas leur attention. Comme certains l'ont expliqué, ils n'ont pas le temps de déchiffrer des métaphores pour découvrir si un message s'adresse à eux ou s'il est susceptible d'intéresser leur entreprise, et préfèrent des publicités qui vont droit au but. Dans ce cas, les mots comme « sécuritaire », « TI » ou « protection », combinés à des images plus littérales contribueraient grandement à atteindre cet objectif. Bien que les participants aient manifesté de l'intérêt pour une approche plus sérieuse et plus directe en matière de cybersécurité, certains étaient réticents à ce qu'on utilise des publicités qui inspirent un peu trop la peur.
- Le sceau du programme devrait être plus visible dans les concepts publicitaires, c'est-à-dire plus gros et présenté plus tôt. Puisque de nombreux participants souhaitaient voir une publicité plus littérale dans sa représentation de la sécurité, le sceau avec le cadenas était souvent la seule image qui répondait à ces attentes.
- Les participants étaient d'avis qu'il n'était pas nécessaire de mettre l'accent sur l'importance de la cybersécurité puisqu'eux-mêmes et leurs pairs le comprennent déjà très bien.
- Même si la plupart des participants s'entendaient pour dire que les concepts attireraient leur attention, cela ne signifiait pas nécessairement qu'ils liraient tout le texte ou regarderaient la vidéo au complet. Ceux qui ont affirmé être « très occupés » ont expliqué que la première impression d'une publicité contribue grandement à déterminer sa pertinence et s'ils auront envie de lire tout le texte ou de regarder la vidéo au complet. Pour attirer l'attention, la publicité doit comporter un élément accrocheur dès le départ ou dans le haut de l'image, en caractères gras, et fournir de l'information qui les incite à vouloir en apprendre davantage, que ce soit en regardant ou en lisant le reste de la publicité, ou en cliquant sur le lien fourni. Par ailleurs, certains ont mentionné que l'aspect de certaines de ces publicités était tellement différent de ce qu'ils voient habituellement qu'ils auraient envie de les lire juste pour satisfaire leur curiosité.
- L'information présentée dans les publicités a soulevé des questions et plusieurs participants ont cru que le programme de certification était un cours qu'ils pouvaient suivre. Même si nous leur avons expliqué que le but de la publicité était de « titiller » les

auditeurs qui pourraient trouver de l'information supplémentaire sur le site Web, plusieurs participants ont mentionné que le manque d'intérêt à suivre un cours ou l'exécution des concepts ne les inciteraient pas à vouloir en apprendre davantage, les laissant avec une fausse conception qui aurait pu être évitée en visitant le site Web.

- Les participants préféreraient non seulement un message direct, mais également une identification claire du commanditaire et du public cible, ainsi qu'un appel à l'action évident. Ils ont suggéré d'insérer un texte similaire à celui-ci : « Le gouvernement du Canada souhaite assurer la cybersécurité des petites entreprises canadiennes. Pour ce faire, nous vous offrons un nouveau programme de certification. Cliquez ici pour en savoir davantage. »
- Le mot-symbole du gouvernement du Canada devrait apparaître au début de chaque vidéo et non seulement à la fin. De nombreux participants ont avoué qu'ils ne regarderaient pas les vidéos au complet puisque leurs premières impressions les amèneraient à croire que ces publicités proviennent d'une autre entreprise de cybersécurité qui souhaite vendre un logiciel ou, comme pour les concepts A (Plus facile) et B (Un premier pas) plus particulièrement, des publicités pour un produit qui n'a rien à voir avec la cybersécurité. Pour rendre la publicité plus crédible et digne de confiance, les participants ont suggéré de rendre le mot-symbole plus visible en le grossissant par exemple.

Les résultats détaillés pour chacun des concepts publicitaires sont présentés ci-dessous.

**Concept A – Plus facile**




Dans l'ensemble, ce concept n'a pas été très bien accueilli et s'est classé au dernier rang des trois concepts testés.

Les premières réactions ont souvent révélé que ce concept créait une certaine confusion quant au **public cible**. Pour de nombreux participants, la publicité ne semblait pas s'adresser aux entreprises, mais plutôt aux consommateurs. L'idée de « commencer » a suscité des réactions chez certains qui ont commenté que si ce concept s'adressait aux entreprises, ce serait pour des entreprises en démarrage ou de jeunes entrepreneurs nouvellement arrivés sur le marché – des entreprises qui n'ont pas encore investi dans la cybersécurité. D'autre part, le sentiment contradictoire était que le look rétro semblait viser davantage une génération plus âgée. Pour certains, la répétition du mot « plus » dans les pointes de tarte donnait l'impression que la publicité était destinée aux entreprises qui ont déjà des mesures en place, mais qui souhaitent ou doivent investir ou en faire « plus » plutôt qu'aux entreprises en démarrage.

Le **contenu**, qui a plu à certains et qui, pour d'autres, était le seul élément important, a soulevé plus de questions qu'il n'a apporté de réponses, sur la raison d'être de la publicité comme sur le programme de certification. Même si nous leur avons expliqué que la publicité avait pour but

d'attirer l'attention et d'inciter les auditeurs à se rendre sur le site Web, le concept a raté la cible puisque, compte tenu de leur première impression, la plupart des participants ne seraient pas tentés d'en savoir plus.

**Sur le plan de la créativité**, bien que les couleurs vives aient réussi à capter l'attention des participants et que ceux-ci aient trouvé un certain mérite à l'idée de la tarte et de l'information présentée en sections, le concept est tombé à plat. La représentation de la tarte était la principale raison pour laquelle le concept a déplu aux participants en tant que décideurs d'entreprises. Outre l'impression générale selon laquelle la publicité était destinée aux consommateurs, à première vue, certains pourraient présumer qu'elle a quelque chose à voir avec la vente de tartes ou d'autres produits de boulangerie, ou bien une recette, d'où leur manque d'intérêt. Quelques participants ont qualifié l'exécution de maladroite, enfantine ou de style « clipart », loin de l'image professionnelle à laquelle on pourrait s'attendre de la part du gouvernement du Canada. L'exécution a nui au message selon lequel les gens devraient faire confiance à la certification ou au programme et se sentir en sécurité.

Un des **messages principaux** de cette publicité provenait du titre qui laissait entendre que la cybersécurité est facile (de la tarte), une prémisse qui n'a pas fait l'unanimité. D'autres ont mentionné que le message principal était l'obtention d'une certification et par conséquent, une augmentation du volume d'affaires. De nombreux participants étaient d'avis que le message s'est perdu dans l'exécution quelque peu encombrée et qu'il leur faudrait lire les petits caractères ou la banderole au complet, ou bien regarder la vidéo jusqu'à la fin pour en savoir plus. Bien que dans l'ensemble, les participants étaient d'avis que le texte en petits caractères puisse contenir de l'information utile et intéressante, l'exécution maladroite et le sentiment général selon lequel ils ne porteraient pas beaucoup d'attention au message au-delà du titre ou de la première image, il était peu probable qu'ils se rendent jusqu'au message principal. L'allusion à la « tranquillité d'esprit » a été perçue comme positive et pertinente.

Le logo du gouvernement du Canada a permis à pratiquement tous les participants de **comprendre qu'il s'agissait d'une publicité du gouvernement du Canada**. Quelques-uns se sont demandé si une tierce partie était impliquée dans la certification parce qu'ils n'ont pas bien compris comment le programme serait déployé.

La plupart ont bien compris que l'**appel à l'action** était de cliquer sur le lien. Toutefois, en raison de la mauvaise exécution, la majorité des participants ont admis qu'ils n'étaient pas tentés de le faire.

**Concept B – Un premier pas**


Ce concept a suscité des réactions variées et s'est classé au deuxième rang. Seulement quelques participants en ont fait leur premier choix. Cependant, comme ce fut le cas pour le concept A, quelques critiques ont été formulées, en particulier pour l'exécution et les perceptions concernant le public cible. De plus, les participants n'ont pas nécessairement compris que la publicité portait sur la certification en cybersécurité; ils ont d'abord cru qu'il s'agissait d'une publicité d'espadrilles ou d'un programme d'emploi, d'un programme communautaire, d'un programme de mise en forme, d'un refuge pour jeunes ou d'un programme collégial.

Certains participants n'avaient pas l'impression d'être **ciblés** par la publicité, mais que celle-ci s'adressait à un jeune public, comme les étudiants de niveau collégial. Cette impression était attribuable non seulement à l'image de l'espadrille et à l'approche créative dans son ensemble, mais également au message du « premier pas ». Les participants avaient le sentiment qu'on s'adressait aux (petites) entreprises en démarrage qui n'avaient pas encore touché à la

cybersécurité, plutôt qu'à des entreprises établies qui étaient depuis longtemps confrontées à cet enjeu. Certains participants ont mentionné que le « premier pas » avait été fait il y a des décennies avec l'arrivée de l'Internet.

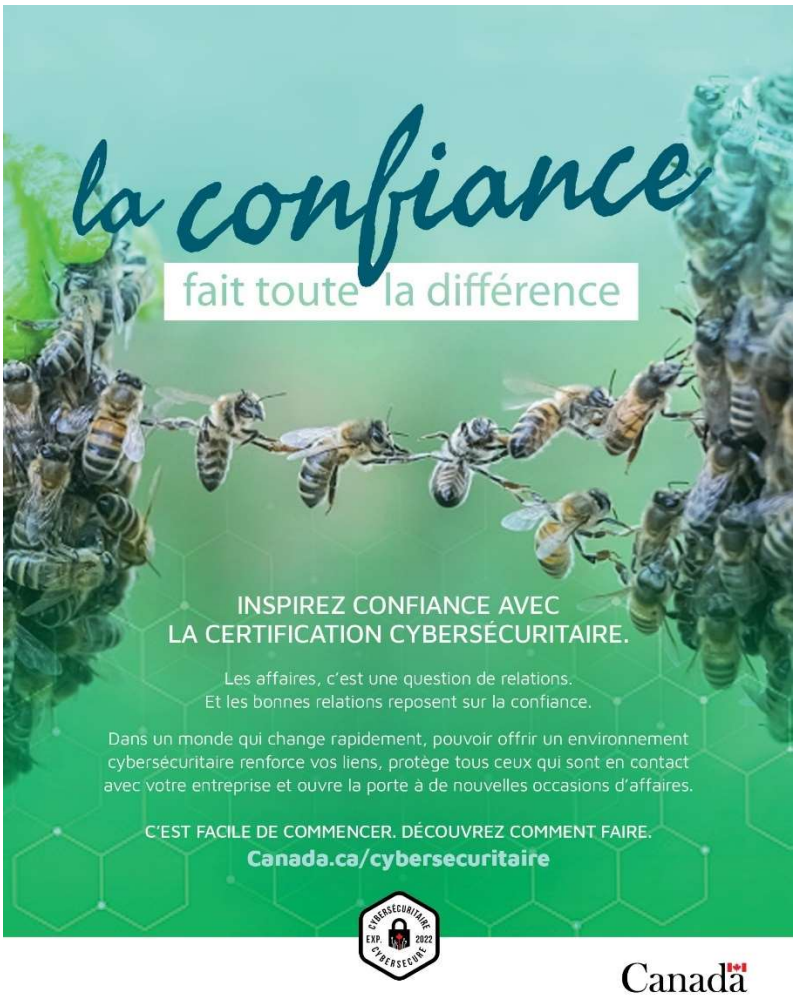
D'autres ont cependant compris que le **message principal** était un encouragement pour les entreprises à faire un premier pas vers la certification (plutôt qu'un premier pas vers la cybersécurité en général). Selon eux, ce message était plus convaincant et plus pertinent que les autres, et les convaincrait d'agir. L'idée que les entreprises devraient poser un geste pour atteindre la cybersécurité plutôt qu'on leur serve sur un plateau d'argent leur a plu. Dans l'ensemble, le texte de la publicité a suscité des réactions favorables, notamment pour ce qui est de l'approche multidimensionnelle utilisée dans la bannière et la vidéo. Cependant, quelques participants avaient toujours l'impression qu'il manquait de l'information, ce qui a semé la confusion dans leur esprit.

L'**approche créative** a été qualifiée d'accrocheuse et la plupart des participants ont admis qu'elle capterait leur attention. Plusieurs ont eu de la difficulté à lire ce qui était écrit sur l'espadrille; par conséquent, ils ont trouvé que l'image était trop chargée. Étant donné que les messages ont plu, certains ont suggéré de les transmettre d'une autre façon. Quelques participants étaient d'avis que l'approche globale ne reflétait pas la gravité qu'ils associent normalement à la cybersécurité des entreprises.

L'**appel à l'action** qui les invite à cliquer sur le lien était clair. Toutefois, ce ne sont pas tous les participants qui répondraient à l'appel étant donné qu'ils n'avaient pas l'impression que le programme ou la certification s'adressaient à eux. Par ailleurs, certains ont indiqué que l'information était suffisamment intéressante pour les inciter à aller en ligne pour obtenir des réponses aux questions qu'ils se sont posées en regardant ou en lisant la publicité.

Les participants ont remarqué le **logo du gouvernement du Canada logo** qui, selon eux, a donné de la crédibilité à la publicité et à la certification. En le voyant, les participants étaient plus réceptifs à l'idée d'obtenir une certification; d'autres ont admis que si ce n'était pas du logo, ils auraient cru que la publicité provenait d'une entreprise privée.

**Concept C – La confiance**




Ce concept était de loin le favori parmi les trois présentés, non pas parce qu'il était parfait, mais parce qu'il s'est démarqué des autres concepts, qui étaient plus ou moins réussis. Les principales raisons qui expliquent le choix de ce concept étaient sa plus grande pertinence ou son lien plus direct avec la cybersécurité, et pour l'utilisation du thème de la « confiance ». Ce concept était le plus efficace pour convaincre les participants de cliquer sur le lien pour en apprendre davantage sur la certification.

Ce concept a été le plus souvent perçu comme **ciblant** un auditoire plus vaste de gens d'affaires, principalement en raison de son ton plus sérieux comparativement aux deux autres. Les participants s'entendaient pour dire que ce concept utilisait un langage qu'ils comprenaient bien et qu'il était moins axé sur les consommateurs.

L'**approche créative** a été qualifiée d'accrocheuse et de bien exécutée. Le thème des abeilles qui travaillent ensemble, à la chaîne, était clairement véhiculé et avait un lien direct avec le message

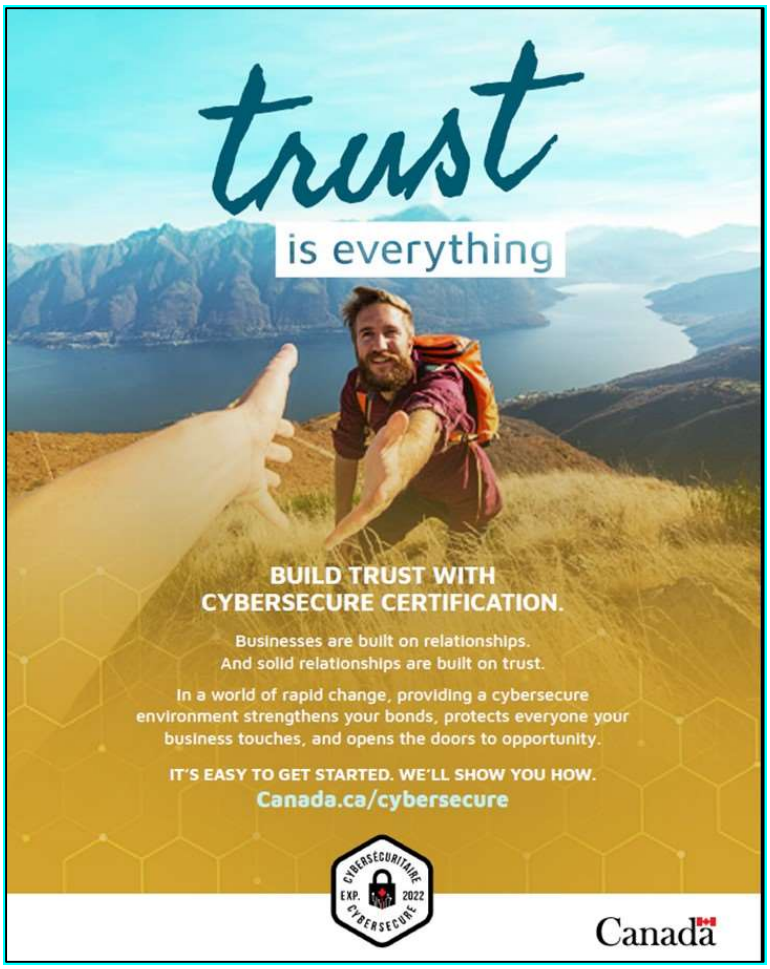
principal de la publicité. Certains participants ont aussi remarqué les ruches en arrière-plan qui leur ont rappelé les connexions de réseau. Toutefois, certains n'ont pas saisi le lien entre les abeilles et la cybersécurité alors que d'autres qui avaient une aversion pour les insectes ou les abeilles ont suggéré d'utiliser des personnes afin que la publicité soit plus attrayante pour eux.

Quelques participants ont exprimé l'opinion que la vidéo était trop lente à transmettre son message et qu'il serait peu probable qu'ils la regardent jusqu'au bout.

Le **message principal** de la confiance et que celle-ci « fait toute la différence » a bien été compris et a été considéré comme pertinent dans le contexte de la cybersécurité. L'idée que le lien de confiance pourrait aisément être rompu par un seul maillon faible – que ce soit une abeille ou un membre de l'équipe dans l'entreprise, ou bien une défaillance dans un système des TI – a également trouvé écho auprès des participants. À leur avis, la cybersécurité requiert un réseau solide, qu'il soit interne ou externe, dans toute la chaîne logistique. Ils ont également fait valoir qu'en augmentant sa cybersécurité, une entreprise bâtissait des liens et attirait davantage de clients.

L'**appel à l'action** qui consiste à se renseigner et à visiter le site Web du gouvernement du Canada pour obtenir sa certification a bien été compris de la majorité des participants. La présence du logo leur a également permis d'identifier le **gouvernement du Canada** comme commanditaire.

Dans les quatre derniers groupes de discussion, nous avons présenté une variante du concept C (La confiance) après la première version. Nous avons testé uniquement une publicité imprimée qui contenait le même texte que le concept original : seule l'image était différente.




Ce concept publicitaire alternatif a été produit uniquement en anglais pour les quatre derniers groupes de discussion organisés, notamment les groupes de la région de Saskatoon/Regina, de la région de Winnipeg, de la région de Calgary/Edmonton et de la région de Vancouver.

Le concept révisé a suscité des réactions variées et a été de loin considéré comme moins efficace que la version avec les abeilles.

Les participants qui ont bien accueilli l'idée d'utiliser un humain plutôt que des insectes se sont sentis davantage interpellés par cette image qu'ils ont trouvée plus attrayante. Le message portant sur la confiance a plu, mais certains participants n'ont pas vu immédiatement la main qui se tendait et n'ont donc pu faire le lien entre l'image et le message. D'autres ont mentionné que l'homme ne semblait pas nécessairement avoir besoin d'aide ou d'être dans une position trop précaire. Comme l'ont fait remarquer certains participants – il ne tombe pas d'une falaise périlleuse, il fait seulement une belle randonnée dans un endroit magnifique.

Des participants ont expliqué que l'image leur rappelait davantage une publicité pour le tourisme, avec ses airs de liberté et d'exploration, plutôt qu'une publicité sur la cybersécurité ou

sur l'établissement de liens ou de rapports de confiance. Pour cette raison, ils seraient moins tentés de la lire au complet ou d'essayer d'en savoir plus.

## Placement publicitaire

Dans certains groupes, nous avons demandé aux participants à quel endroit ISDE devrait diffuser ces publicités pour qu'elles soient vues de leur public cible.

Voici les réponses que nous avons obtenues :

- Sites Web de nouvelles (comme CTV, CBC, CNN, La Presse, Le Monde, Globe and Mail, Msn.ca)
- Sites Web de chroniques financières ou d'affaires (comme Forbes, The Economist, Business Insider)
- Sites Web de technologies
- Pages du gouvernement du Canada (comme Mon dossier d'entreprise de l'ARC ou autres pages de programmes pour entreprises) ou du gouvernement provincial
- Site Web de la Chambre de commerce
- Sites Web d'associations professionnelles ou magazines en ligne (comme CPA Magazine)
- Sites Web ou magazines spécialisés (comme Investment Executive)
- Médias sociaux (comme LinkedIn, Facebook, Twitter, Instagram)

## Réactions au programme de certification CyberSécuritaire

Avant de discuter du programme, nous avons demandé aux participants s'ils se souvenaient avoir vu le nom de celui-ci dans les publicités que nous leur avons présentées. Dans chaque groupe, au moins un participant s'est rappelé l'avoir vu alors que les autres n'étaient pas certains ou donnaient de mauvaises réponses.

La description suivante a été présentée aux participants :

**Le programme de certification CyberSécuritaire Canada est un programme à participation volontaire de certification en cybersécurité mis en œuvre par le gouvernement du Canada.**

**Pour obtenir la certification, les entreprises doivent mettre en place 13 domaines de contrôle de sécurité couvrant un vaste éventail de points vulnérables pour les petites et moyennes entreprises, comme la formation du personnel, la protection des mots de passe, les plans d'intervention en cas d'incident, et plus encore.**

**Ces domaines de contrôle de sécurité ont été créés par le Centre canadien de la cybersécurité, les experts de la cybersécurité au Canada pour les petites et moyennes entreprises.**

Avant de participer à la discussion de groupe, aucune des entreprises ne connaissait le nouveau programme.

Après avoir pris connaissance de la description, presque tous les participants souhaitaient en apprendre davantage sur le programme et bon nombre d'entre eux songeraient à réserver du temps à leur horaire pour obtenir la certification.

Même si la plupart des participants croyaient que la certification serait « bonne pour les affaires » et n'y voyaient que des avantages, ils n'ont pas toujours bien compris ce qu'ils pourraient en tirer et la manière dont leur entreprise en profiterait. Certains se sont demandé si, par exemple, ils pouvaient mentionner le fait qu'ils ont obtenu la certification à leur compagnie d'assurances pour obtenir un rabais sur leur assurance-responsabilité (comme c'est le cas pour quelques certifications internationales). Le fait de pouvoir utiliser le sceau sur le matériel publicitaire a été vu comme un avantage. Des participants étaient d'avis que si toutes choses étaient par ailleurs égales, les entreprises seraient tentées de choisir un partenaire ou un fournisseur qui possède la certification et qui affiche le logo, ce qui leur donnerait une longueur d'avance sur la compétition.

Compte tenu de l'information qui leur a été fournie, les participants ont parfois eu de la difficulté à évaluer comment la certification pourrait améliorer leur cybersécurité. Certains avaient toutefois espoir qu'elle permettrait à tout le moins de déterminer comment rehausser le niveau de cybersécurité ou confirmer qu'ils font déjà tout ce qu'il faut.

Ceux qui ont démontré de l'intérêt pour le programme s'entendaient pour dire que si le processus de certification révélait des problèmes nécessitant des changements pour rehausser

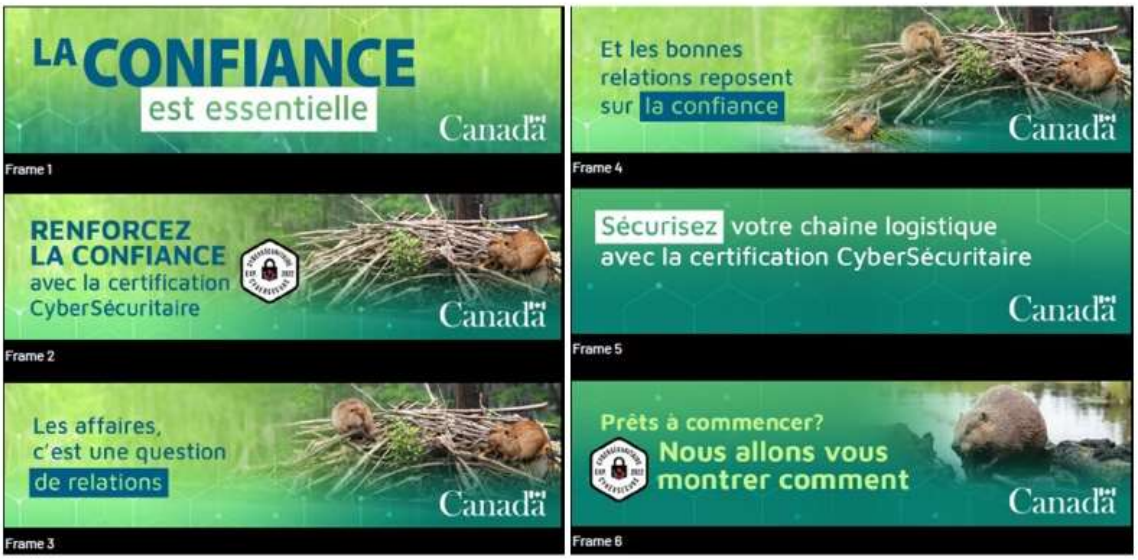
le niveau de protection, ils seraient disposés à investir dans des logiciels, du matériel informatique et de la formation. Par contre, quelques participants ont indiqué qu'il y avait des limites aux dépenses qu'ils seraient prêts à faire pour obtenir la certification s'ils avaient le moindre doute qu'ils seraient beaucoup mieux protégés.

La référence au Centre canadien de la cybersécurité a rassuré plusieurs participants qui ont suggéré de l'inclure dans la publicité pour la rendre plus crédible.

# Phase 1 – Groupes de discussion : vérification du succès

Après la première ronde de groupes de discussion, deux autres ont eu lieu (une en anglais et l'autre en français) pour tester deux nouveaux concepts publicitaires créés sur la base des commentaires reçus durant la ronde initiale et la préférence manifestée envers les concepts ayant pour thème « la confiance ». Ceux nouveaux concepts ont été présentés aux participants sous forme de bannières vidéo en ligne. Durant la discussion, nous avons conservé la séquence des images à l'écran pour aider les participants à se rappeler le contenu de chacune dans la bannière vidéo.

**Concept A – Les castors**




Ce concept a suscité des réactions diverses.

De façon générale, les participants ont bien compris le message, mais se sont posé des questions sur les étapes à suivre pour obtenir la certification. Certains croyaient qu'il s'agissait d'un cours alors que d'autres étaient incertains. Toutefois, la plupart ont compris qu'ils pouvaient obtenir plus d'information en ligne sur le programme et obtenir des réponses à leurs questions.

Il y a eu des discussions à savoir si la référence à la chaîne logistique (image 5) était pertinente pour tous ou s'il s'agissait d'un élément essentiel. Certains étaient d'avis que cela pourrait démotiver ceux qui n'ont pas de chaîne logistique ou qui estiment qu'il n'est pas important pour leur entreprise d'en avoir une, et que cette image pourrait être mieux utilisée pour fournir un

peu plus d'information sur le programme lui-même. Par exemple, certains participants ont fait valoir que les entreprises peuvent uniquement se protéger elles-mêmes et contrôler les comportements de leurs employés, et qu'elles n'ont aucune influence sur les autres éléments de la chaîne logistique – sauf si une certification devient obligatoire. D'autres ont dit ne pas avoir remarqué cette référence, mais que cela ne les empêchait pas de comprendre le message ou l'appel à l'action pour obtenir plus d'information.

Ceux qui ont aimé ce concept ont souligné ce qui suit :

- L'exécution créative avec l'image des castors qui travaillent ensemble, et la séquence où d'autres castors viennent s'ajouter, passant d'un à trois, où sont illustrés les thèmes de la confiance et des relations;
- L'image de la construction de quelque chose de solide;
- La structure alvéolaire en arrière-plan qui représente l'interdépendance, la cohésion et le lien avec la cybersécurité;
- La police de caractères et les couleurs qui ajoutent à la gravité du message;
- La visibilité du mot « confiance » qui est essentielle dans les relations et le sentiment de (cyber) sécurité;
- L'enchaînement logique de l'histoire jusqu'au message « Nous allons vous montrer comment » et l'appel à l'action;
- Le sceau de certification présenté au début de la publicité (dans la deuxième image) et sa visibilité au centre de la bannière; et
- L'image du castor, réel emblème du Canada associé au gouvernement fédéral.

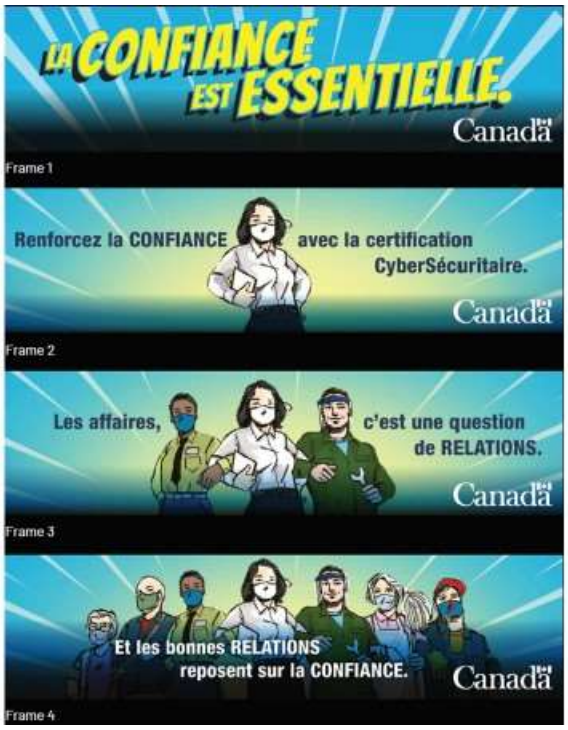
Ceux qui n'ont pas aimé ce concept ont fourni les raisons suivantes :

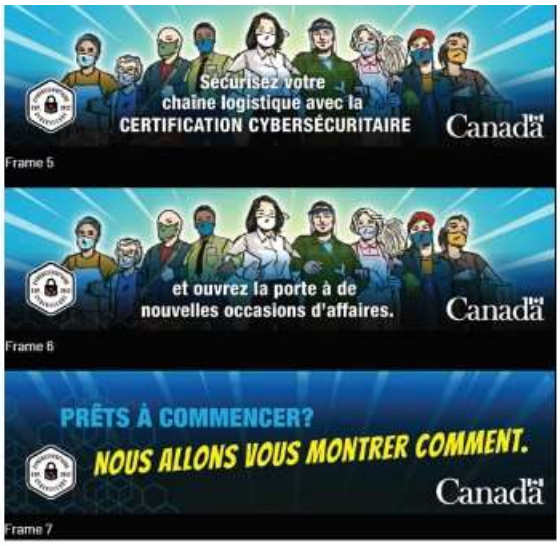
- Ils n'ont pas fait le lien entre les castors et la cybersécurité ou toute autre chose qui pourrait être considérée comme une menace – ils ont trouvé les castors « adorables », ce qui est loin d'illustrer la gravité de l'enjeu que représente selon eux la cybersécurité;
- Il n'y avait aucun lien avec les gens ou les systèmes de TI dans les images;
- Le cadre naturel représenté était déconcertant;
- Dans l'ensemble, le concept ne semblait pas les cibler ou cibler les décideurs du monde des affaires en général, et il est peu probable qu'ils iraient plus loin en cherchant de l'information supplémentaire;
- Étant donné la prévalence de la technologie utilisée pour bloquer les publicités, certains participants ont indiqué qu'un concept de publicité Web ne parviendrait pas à les rejoindre et qu'il serait préférable d'utiliser une approche multivoie.

Les participants ont fait les suggestions suivantes :

- Ajouter l’adresse du site Web à la dernière image afin que les gens puissent facilement cliquer pour obtenir de l’information supplémentaire;
- Ajouter le sceau à la première image pour attirer immédiatement l’attention;
- Inclure des images ayant un lien plus littéral avec la cybersécurité, comme des ordinateurs qui communiquent ensemble, des gens qui travaillent ou qui utilisent les médias sociaux; et
- Remplacer certaines couleurs par d’autres qui attirent davantage l’attention, comme le rouge, même si ce n’est que dans le logo ou le drapeau du gouvernement du Canada.

**Concept B – La chaîne de confiance**




Ce concept a également obtenu des réactions diverses, notamment en raison de son exécution.

Ceux qui l'ont aimé ont mentionné ce qui suit :

- Sa représentation littérale de gens qui travaillent ensemble, des relations humaines et d'une « chaîne » humaine;
- La diversité des gens qu'on voit et la façon dont ceux-ci représentent les différentes parties d'une chaîne logistique ou d'entreprises ou de secteurs connexes qui travaillent ensemble;
- L'utilisation du logo du gouvernement du Canada qui ajoute de la crédibilité et inspire confiance;
- L'image d'un super héros de dessin animé qui distingue cette publicité des autres et qui capte l'attention des participants et les incite à regarder la publicité jusqu'au bout et à vouloir en savoir davantage; et
- L'accent sur le mot « confiance ».

Ceux qui n'ont pas aimé le concept ont donné les raisons suivantes :

- Le style dessin animé et le ton sont tombés à plat et ont fait abstraction de la gravité associée à la cybersécurité et pour certains, ont remis en question la légitimité du programme;
- Le concept n'avait pas l'allure habituelle d'une publicité du gouvernement du Canada qui attirerait les gens ou leur donnerait confiance pour obtenir plus d'information;

- Il ne semblait pas s'adresser à tous les décideurs d'entreprises, mais attirerait uniquement de jeunes entrepreneurs ou des entreprises en démarrage;
- Le sceau du programme est présenté trop tard;
- Le fait de voir des gens avec des masques a semé la confusion, étant donné que ce programme continuerait d'exister au-delà de la pandémie. Certains avaient l'impression que leur attention était tournée vers les masques et ils ont cherché en vain un lien entre la santé ou la protection contre la COVID-19 et la protection contre les pirates informatiques ou la cybersécurité en général;
- Étant donné la prévalence de la technologie utilisée pour bloquer les publicités, certains participants ont indiqué qu'un concept de publicité Web ne parviendrait pas à les rejoindre et qu'il serait préférable d'utiliser une approche multivoie.

Plusieurs améliorations ont été suggérées, notamment :

- Remplacer les personnages de dessins animés par de vraies personnes;
- Retirer les masques;
- Présenter le sceau plus tôt dans la publicité; et
- Ajouter l'adresse du site Web à la fin, de manière à ce que les gens puissent facilement cliquer sur le lien, ce qui ajouterait de la légitimité et inspirerait la confiance qu'il s'agit bien d'une publicité et d'un programme de certification du gouvernement du Canada.

# Phase 2 – Résultats : entrevues en profondeur avec les parties intéressées

Pour cette phase de la recherche, nous avons fait appel à deux groupes de parties intéressées et leur avons présenté deux séries de questions différentes. Les participants qui représentaient des groupes ou des associations de l'industrie ont été interrogés sur l'importance de la cybersécurité pour leur industrie en général, l'impact de la pandémie, l'état de préparation de l'industrie et ce qui devait se produire pour que l'industrie s'améliore sur ce plan. Les participants qui représentaient les entreprises du secteur privé disposant de chaînes logistiques importantes ont été interrogés au sujet de leur état de préparation en matière de cybersécurité, de l'impact de la pandémie, et ont dû répondre à diverses questions sur l'approvisionnement et leur opinion de l'état de préparation de leur chaîne logistique en matière de cybersécurité.

Dans les deux groupes, nous avons demandé aux participants quel était selon eux le rôle du gouvernement du Canada; les représentants de l'industrie devaient se concentrer sur le segment vertical de leur industrie en général, et les participants du secteur privé, sur leur chaîne logistique en particulier.

En dernier lieu, nous avons fourni aux participants un aperçu du programme CyberSécuritaire Canada et leur avons demandé s'ils en avaient déjà entendu parler et ce qu'ils en pensaient. Les représentants de l'industrie étaient également invités à nous dire si ce type de programme leur serait utile et s'il serait utilisé dans leur industrie, s'il aurait un impact sur leur état de préparation en matière de cybersécurité, les obstacles qui les empêcheraient de s'inscrire au programme, et le rôle du gouvernement du Canada en lien avec ce programme. Nous avons posé des questions similaires aux participants du secteur privé, en leur demandant de se concentrer sur leur chaîne logistique.

## Préparation en matière de cybersécurité

En ce qui a trait à la préparation en matière de cybersécurité, peu d'entreprises avaient l'impression d'être entièrement protégées ou que les entreprises de leur industrie le sont. Tous s'entendaient pour dire qu'au moins une partie de leur approche ou de leur système pouvait être améliorée. Même les entreprises les plus sophistiquées ont hésité à se donner une note parfaite sur ce plan.

La présente recherche a révélé que les entreprises des différentes industries couvraient tout l'éventail de la préparation à la cybersécurité – certaines semblaient faire mieux que d'autres.

La recherche a également fait ressortir plusieurs facteurs qui contribuent à l'état de préparation à la cybersécurité, notamment ceux-ci :

- L'intensité des données de l'industrie était un facteur clé – plus une entreprise ou une industrie dépend des données ou en génère, plus elle est susceptible de croire qu'elle performe relativement bien sur le plan de la cybersécurité. La relation entre l'importance des données et la pertinence de la cybersécurité était évidente dans les industries comme les services de soins spécialisés et les études de marché. Les représentants de ces industries ont expliqué les raisons pour lesquelles la cybersécurité était une préoccupation constante et qu'ils utilisaient des ressources considérables pour maximiser leur niveau de sécurité. Ce sont également ces industries qui doivent gérer un volume important de données, y compris des données personnelles. Un représentant d'un autre secteur a expliqué pourquoi la cybersécurité était de plus en plus préoccupante, principalement parce que les entreprises de cette industrie géraient un volume croissant de données.

  Le lien entre l'intensité des données et la préparation en matière de cybersécurité n'est pas parfait et on remarque un paradoxe intéressant dans certaines industries. Certaines entreprises ne considèrent pas que les données qu'elles possèdent, gèrent ou produisent sont « délicates » de nature et par conséquent, elles ne font pas de la cybersécurité une priorité absolue. De plus, un représentant d'industrie a expliqué que les entreprises dans son secteur (professionnels de la santé) géraient des volumes importants de données personnelles, mais il considérait que le niveau de préparation en matière de cybersécurité était relativement bas. Pour cette industrie en particulier, les propriétaires et les exploitants ne sont pas négligents, non plus qu'ils ne sous-estiment l'importance des données qu'ils gèrent – en fait, ils accordent une grande importance à la protection de la vie privée. Cependant, d'autres activités, comme la prestation de soins (« prendre soin de leurs patients ») l'emportent et d'autres facteurs, décrits ci-dessous, les empêchent de protéger complètement ces données.

- De nombreux participants s'entendaient pour dire que la taille de l'entreprise était un facteur clé de rendement en matière de cybersécurité d'une entreprise ou d'un fournisseur. Tous les participants ont reconnu que plus une entreprise est grande, plus il est probable qu'elle soit bien préparée sur le plan de la cybersécurité puisqu'elle dispose de ressources pour gérer les systèmes de TI, ce qui n'est pas le cas des petites entreprises. Ce fait a également été reconnu par de grandes entreprises qui peuvent compter sur des chaînes logistiques importantes – elles savent ou ont un fort sentiment que leurs gros fournisseurs sont mieux équipés et disposent d'une main-d'œuvre plus importante pour gérer la cybersécurité. La taille devient un problème pour les très petites et les

microentreprises puisque le propriétaire ou l'exploitant se concentre presque exclusivement à générer des revenus, ce qui est le cas de l'industrie des soins de santé, où des milliers de petits bureaux sont gérés par des professionnels de la santé qui ont comme principal objectif le bien-être des patients. Leur domaine d'expertise, ce sont les soins et leur priorité, les patients, alors que la gestion des affaires et des systèmes de TI est reléguée au second rang. Ce fut particulièrement le cas durant la pandémie.

- Le coût ou du moins, la perception de celui-ci est un autre obstacle qui empêche les entreprises de mieux se préparer pour assurer leur cybersécurité. Aussi occupées soient-elles, certaines entreprises n'ont pas les revenus nécessaires pour maintenir des ressources affectées aux TI, même si elles gèrent un volume élevé de données. De plus, certains exploitants d'entreprises diraient qu'ils ne peuvent se permettre des systèmes de TI plus robustes ou plus modernes, parce que cela représenterait un investissement important.

- Les représentants de l'industrie ont expliqué que même si les entreprises souhaitaient améliorer leur niveau de cybersécurité, plusieurs lacunes les en empêcheraient :

    - Elles ne possèdent pas les connaissances fondamentales des TI – par exemple, le concept de base de sauvegarde des données n'est pas compris de tous,

    - elles ne sauraient pas par où commencer,

    - elles ne sauraient pas quels logiciels ou quel matériel utiliser, et

    - elles ne sauraient pas quoi faire pour maintenir une efficacité constante en matière de cybersécurité, comme rester au fait des nouvelles technologies, des nouveaux processus et des nouvelles menaces.

- Pour bon nombre d'entreprises dans certaines industries, il n'y a pas, ou très peu d'attentes de la part des clients, de normes ou de réglementation gouvernementale qui requièrent le maintien d'un seuil minimum de cybersécurité. Par conséquent, ces entreprises s'autoréglementent, à l'exception des industries qui gèrent des volumes importants de données, comme le secteur des études de marché où les entreprises subissent les pressions des clients et des groupes et associations de l'industrie.

- La différenciation concurrentielle est un facteur, mais pas pour tous. Dans certaines industries, comme les études de marché, la gestion des données est un enjeu. Dans d'autres secteurs, comme les soins de santé et les réparations et l'entretien de véhicules, les clients ne choisissent pas un fournisseur en fonction de sa capacité à gérer ses données. Étant donné l'importance croissante des données dans l'industrie des

réparations et l'entretien de véhicules, la ***possibilité*** que la gestion des données devienne un facteur de différentiation concurrentielle est bien réelle. D'autre part, les représentants de l'industrie des soins de santé (notamment les soins primaires) ont expliqué que tout argument qui fait de la cybersécurité une différentiation concurrentielle serait vain puisque les médecins de premier recours et les hôpitaux ne fonctionnent pas vraiment dans un environnement compétitif. Il convient de noter que pour les fins de la présente recherche, le groupe représentant l'industrie des soins de santé était surtout concentré sur le système public de santé et non sur les fournisseurs de soins du secteur privé ou les autres soignants, comme les dentistes, les physiothérapeutes, et ainsi de suite.

Il semble que la pandémie ait eu des répercussions variées sur les diverses industries qui ont participé à la première phase de la recherche. Dans plusieurs cas, elle a entraîné le recours à la technologie et forcé de nombreuses entreprises à utiliser celle-ci comme elles ne l'avaient jamais fait auparavant (p. ex., soins virtuels pour les professionnels de la santé, télétravail, nouveaux systèmes en ligne pour le commerce électronique). Certaines de ces initiatives ont été mises en œuvre de façon sécuritaire et d'autres, de manière disparate.

La pandémie a également forcé les entreprises à concentrer toutes leurs énergies à maintenir leurs activités et à demeurer prospères, reléguant ainsi la gestion ou la mise à niveau des systèmes informatiques à l'arrière-plan à court terme. Cela étant dit, la nécessité de déployer de nouveaux systèmes, comme ceux liés au commerce électronique, a mis la question de la cybersécurité à l'avant-plan pour certains qui ont été forcés d'accomplir en quelques mois ce que d'autres avaient pris des années à réaliser.

## Considérations relatives à la chaîne logistique

Les discussions avec les représentants de grandes entreprises ont révélé deux approches relativement différentes sur le plan de la gestion de la chaîne logistique dans le contexte de la cybersécurité. Ces discussions n'avaient pas pour but de révéler une approche commune à toutes les entreprises canadiennes, mais plutôt de découvrir l'éventail de perspectives et de priorités sur le plan de la gestion de la chaîne logistique et de la cybersécurité.

Les approches pour chaque type d'entreprise sont résumées ci-dessous :

**Structure et affectation des ressources pour les TI**

| Fabrication | Soins de santé spécialisés |
|---|---|
| Possède des ressources et des employés dédiés aux TI et à la gestion de la chaîne logistique. | Possède des ressources et des employés dédiés aux TI et à la gestion de la chaîne logistique. |

### Types de données gérées et approche en matière de gestion des données

| Fabrication | Soins de santé spécialisés |
|---|---|
| Types de données hébergées : procédés de fabrication, données opérationnelles, données sur le personnel, données sur les fournisseurs, données sur les clients.<br><br>L'entreprise voit son approche en matière de gestion des données comme se limitant à ses propres données. Sa priorité est sur les données qu'elle héberge, sans se préoccuper des données gérées par les fournisseurs ou la façon dont elles sont gérées.<br><br>Elle ne voit pas une vulnérabilité dans sa chaîne logistique comme une vulnérabilité pour son propre niveau de cybersécurité.<br><br>Elle ne sait pas exactement comment sa chaîne logistique s'est adaptée durant la pandémie ou son degré de résilience. Elle ignore également si la pandémie a exposé ou introduit des vulnérabilités ou des défis sur le plan de la cybersécurité parmi ses fournisseurs, lesquelles ont également eu des répercussions sur son entreprise. | Types de données hébergées : données opérationnelles, données sur le personnel, données sur les fournisseurs, données sur les clients.<br><br>L'entreprise considère son infrastructure de données comme complexe et nécessitant des systèmes et des procédés sophistiqués pour assurer une protection continue et l'intégrité de ces données. Elle recueille et héberge un volume important de données personnelles du grand public et par conséquent, prend les mesures qui s'imposent pour protéger au maximum ces données de toutes les perspectives possibles, y compris la façon dont les fournisseurs recueillent et gèrent leurs données.<br><br>Elle considère que ses fournisseurs font partie intégrante de son plan et sa stratégie de gestion des données. Dans le même ordre d'idées, son sentiment d'être « entièrement protégé » tient compte de la chaîne logistique. En fait, pour cette entreprise, la plus grande source d'inquiétude est l'intégrité de sa chaîne logistique.<br><br>Elle est assez convaincue de bien comprendre à quel point la pandémie a eu un impact ou non sur sa chaîne logistique. Elle a le sentiment que même si cette dernière n'a pas été imperméable aux cyberattaques qui se sont multipliées durant la pandémie, elle est demeurée passablement résiliente. |

### Exigences relatives à la gestion des données de la chaîne logistique

| Fabrication | Soins de santé personnalisés |
|---|---|
| La cybersécurité n'est pas un facteur dans le choix d'un fournisseur non plus qu'elle n'est une préoccupation constante une fois la relation établie avec celui-ci. Les fournisseurs ne sont pas tenus de fournir de l'information sur l'intégrité de leurs systèmes de TI, leurs procédés ou les balises qu'ils ont mis en place pour assurer leur cybersécurité. | Le niveau de cybersécurité des fournisseurs est intégré au processus d'approvisionnement et dans certains cas, influe sur le choix des fournisseurs. Il peut arriver que des chargés de projets favorisent des fournisseurs, peu importe leur niveau de cybersécurité, ce qui exerce une certaine pression sur la logistique. Lorsqu'un fournisseur est choisi, sans égard au niveau de |

| | |
|---|---|
| Même si elle voulait commencer à le faire, l'entreprise ne saurait pas quels renseignements demander. Étant donné que bon nombre de ses fournisseurs sont à l'international, elle ne sait pas comment elle pourrait vérifier ou renforcer les exigences relatives à la cybersécurité.<br><br>La discussion sur les vulnérabilités de la chaîne logistique a semblé faire réfléchir ce participant à l'importance d'examiner de plus près en quoi les vulnérabilités de sa chaîne logistique en matière de cybersécurité pourrait influencer ses propres opérations et d'intégrer cela à sa stratégie de gestion des risques. | cybersécurité, des efforts sont déployés après-coup pour vérifier et maximiser son niveau de cybersécurité.<br><br>L'entreprise a développé son propre processus d'audit ou de vérification auxquels doivent se soumettre les fournisseurs. Durant ce processus, des indicateurs et des rapports sont recueillis pour établir le niveau de cybersécurité des fournisseurs. On s'assure ainsi de la cohérence de l'information recueillie auprès de ces derniers.<br><br>Bien que ce processus soit rigoureux et étroitement suivi, il n'y a aucune inspection sur place ni aucune vérification à distance des systèmes des fournisseurs. Par conséquent, en l'absence de rapports normalisés et reconnus par l'industrie pour les TI, l'entreprise peut uniquement se fier à ce que ses fournisseurs font et à ce qu'ils affirment au sujet de leur niveau de cybersécurité. |

## Rôle du gouvernement du Canada en matière de cybersécurité

Les participants se sont entendus pour dire que le gouvernement du Canada et, dans certains cas, le gouvernement provincial, avaient un rôle à jouer pour aider les petites et moyennes entreprises à devenir cybersécuritaires, notamment en faisant ce qui suit :

- **Informer, éduquer et former :** Les participants ont reconnu le manque flagrant de connaissances de la part de nombreuses entreprises dans leurs industries respectives et ont suggéré que le gouvernement fédéral offre de l'information, de l'éducation et de la formation sur la cybersécurité et notamment sur l'importance de la cybersécurité pour leurs entreprises ainsi que les étapes à suivre pour atteindre, maximiser et gérer la cybersécurité. Il devrait également établir des pratiques exemplaires. Dans le même ordre d'idées, les participants souhaiteraient que le gouvernement mette à leur disposition une liste de fournisseurs recommandés, notamment pour le matériel informatique et les logiciels, et des consultants en TI qui conseilleraient les entreprises en matière de cybersécurité. À défaut de cela, il pourrait fournir des conseils aux entreprises sur les critères à considérer dans le choix d'un fournisseur de TI.

- **Soutien et incitatif :** Les participants ont suggéré que le gouvernement offre de meilleurs incitatifs financiers aux petites et moyennes entreprises. Ils étaient surtout préoccupés par le fait que même si elles sont plus conscientes de la cybersécurité, les entreprises

n'investissent pas suffisamment dans leurs systèmes pour améliorer comme il se doit leur niveau de cybersécurité.

- **Établissement de normes :** Pour assurer une approche uniforme dans tout le pays, les participants ont proposé que le gouvernement du Canada établisse des normes pour les entreprises. Un participant qui n'avait jamais entendu parler du programme CyberSécuritaire Canada a suggéré que le gouvernement fédéral crée un programme national de certification. D'autres ont aussi mentionné que tout effort visant à élaborer un ensemble de normes devrait tenir compte de ce que font d'autres pays. Autant qu'ils souhaiteraient voir le Canada jouer un rôle de premier plan à cet égard, ils voudraient éviter une situation où les normes nuiraient à la compétitivité des entreprises canadiennes à l'échelle mondiale.

- **Efforts plus soutenus pour combattre la cybercriminalité :** Conscients de l'importance d'appuyer les entreprises dans leurs efforts pour atteindre un niveau supérieur de cybersécurité, les participants ont dit souhaiter que le gouvernement en fasse davantage pour combattre la cybercriminalité.

Aucun des participants n'a suggéré que le gouvernement du Canada rende obligatoire pour les entreprises d'avoir un certain niveau de cybersécurité ou de démontrer une diligence raisonnable. Lorsque nous leur avons demandé si cette approche était envisageable, les participants ont émis des opinions variées; ils ont mentionné quelques avantages, mais également des préoccupations.

Conscients que la cybersécurité est un enjeu qui a pris de l'ampleur durant la pandémie, les participants étaient favorables à tout effort visant à améliorer le rendement des petites et moyennes entreprises canadiennes à ce chapitre. La raison pour cette exigence est facile à comprendre et, à plusieurs égards, justifiée. Ceux qui disposent de chaînes logistiques importantes ont également fait valoir qu'une telle exigence leur faciliterait la tâche pour évaluer le niveau de cybersécurité de leurs fournisseurs et rehausser leur confiance envers la chaîne logistique.

Dans la mesure où les représentants de l'industrie et les entreprises qui peuvent compter sur d'importantes chaînes logistiques ont bien accueilli l'idée de rendre obligatoire un certain niveau de cybersécurité pour les entreprises, tous les participants ont également exprimé des inquiétudes face à cette approche. Premièrement, ils souhaiteraient que cette exigence soit considérée comme un soutien plutôt qu'une punition ou un fardeau supplémentaire. Ils ont expliqué que le gouvernement ne pouvait pas rendre cette mesure obligatoire sans offrir un soutien financier aux entreprises. Les préoccupations visaient principalement les petites

entreprises, dont bon nombre n'ont pas les mêmes types de ressources que les moyennes et grandes entreprises pour surveiller leurs systèmes informatiques.

Certains se sont aussi demandé comment cette exigence serait mise en application. Ils s'inquiétaient qu'à elle seule, la surveillance soit trop fastidieuse pour le gouvernement et s'entendaient pour dire qu'une telle exigence pourrait, à certains égards, mener à une surveillance excessive du secteur privé de la part du gouvernement. D'autres étaient d'avis que ce genre d'obligation ne devrait pas s'appliquer à tous les types d'entreprises, mais uniquement à celles qui recueillent ou gèrent un certain volume ou certains types de données.

Quelques participants se sont demandé comment une telle exigence pourrait s'appliquer aux fournisseurs internationaux. Certains ont exprimé des doutes quant à la capacité du gouvernement du Canada à imposer une telle exigence aux entreprises étrangères. Même s'il y parvenait, plusieurs s'inquiétaient que cela dissuade les fournisseurs internationaux à transiger avec des acheteurs canadiens. Bien que ces fournisseurs soient très importants pour les entreprises canadiennes, à l'échelle mondiale, celles-ci ne représentent pas nécessairement une proportion importante des revenus des fournisseurs qui n'hésiteraient pas à abandonner ces relations en cas d'exigences excessives. Finalement, certains participants craignaient que cette obligation nuise à la compétitivité des entreprises canadiennes à l'international en augmentant leurs coûts d'exploitation.

## Réactions au programme CyberSécuritaire Canada

Nous avons fourni à chaque participant l'information suivante au sujet du programme :

---

Le programme CyberSécuritaire permet aux PME de démontrer qu'elles prennent les mesures nécessaires pour protéger leurs systèmes, se mettre à l'abri des cyberattaques et protéger les renseignements concernant les clients et les fournisseurs.

Pour être admissible à la certification, l'organisation doit revoir et appliquer les 13 contrôles de sécurité établis par le Centre canadien pour la cybersécurité :

- Élaborer un plan d'intervention en cas d'incident
- Appliquer automatiquement les correctifs aux systèmes d'exploitation et aux applications
- Configurer les appareils de manière à les sécuriser
- Activer les logiciels de sécurité
- Utiliser une authentification forte
- Donner de la formation pour sensibiliser les employés
- Faire des copies de sauvegarde et chiffrer les données
- Sécuriser les services mobiles

- Établir un périmètre de défense de base
- Sécuriser l'environnement infonuagique et les services de TI externalisés
- Sécuriser les sites Web
- Mettre en œuvre des contrôles d'accès et autorisation
- Sécuriser les supports amovibles

Un organisme de certification (agréé par le Conseil canadien des normes) évaluera la mise en œuvre des 13 contrôles de sécurité. L'organisme discutera avec l'organisation pour :

- déterminer si l'organisation répond aux critères de certification;
- donner un aperçu des coûts de la certification CyberSécuritaire;
- évaluer la mise en œuvre des contrôles de sécurité.

Lorsqu'une entreprise obtient la certification CyberSécuritaire, elle est certifiée pour une période de deux ans et elle peut afficher la marque de certification sur son site Web, sa devanture et son matériel promotionnel.

---

Les participants étaient modérément au courant du programme. Une des associations de l'industrie qui connaissait bien le programme l'avait découvert pendant qu'elle développait le programme d'accréditation pour son propre groupe.

L'aperçu du programme a suscité beaucoup d'intérêt chez les participants. Les représentants de l'industrie avaient le sentiment qu'un programme de certification comme celui-là serait profitable pour leurs « membres » et l'ensemble de l'industrie. Ils n'hésiteraient pas à en faire la promotion pour inciter les membres à s'inscrire. Le représentant d'une association de recherche marketing qui avait développé un programme d'accréditation pour ses membres était désireux de trouver une façon d'effectuer un audit de ses membres par l'entremise d'un tiers. Le processus d'audit irait au-delà des systèmes informatiques et du niveau de cybersécurité des membres, mais si l'un d'eux obtenait sa certification, cela simplifierait le processus d'audit pour ce dernier. De plus, le programme pourrait sembler davantage à la portée des membres, compte tenu des coûts élevés associés à d'autres types de certification (comme ISO).

Les participants qui pouvaient compter sur de grandes chaînes logistiques s'entendaient également pour dire que ce type de programme aurait une influence positive. Bien qu'ils n'exigeraient peut-être pas de leurs fournisseurs qu'ils soient certifiés, ils leur recommanderaient sans doute le programme.

Les participants ont jugé que le programme était suffisamment complet et approprié pour une certification en cybersécurité. Le représentant de l'entreprise spécialisée en soins de santé

disposant d'une chaîne logistique importante était d'avis que la certification correspondait très bien à ce qu'il recherchait pour évaluer le niveau de cybersécurité de ses fournisseurs.

Quelques participants ont exprimé des inquiétudes envers le programme, lesquelles reflétaient largement celles émises précédemment au sujet des défis que doivent affronter les entreprises en matière de cybersécurité. Peu d'entre eux auraient l'expertise interne requise pour entreprendre les démarches en vue d'obtenir ce type de certification. Les participants s'entendaient également pour dire que les entreprises n'étaient pas suffisamment familiarisées avec les concepts décrits dans l'aperçu, sans compter les exigences technologiques requises pour remplir les conditions de la certification. Finalement, même s'ils s'engageaient dans le processus de certification pour cerner leurs plus importantes lacunes, ils n'étaient pas convaincus que les entreprises de leur industrie seraient en mesure de payer pour l'infrastructure requise. Certains soupçonnaient que les lacunes étaient importantes pour bon nombre d'entreprises de leur industrie et que les recommandations formulées seraient accablantes et trop coûteuses à mettre en application.

Quelques représentants du groupe de l'industrie ont mentionné que des programmes ou des processus d'audit en matière de cybersécurité étaient déjà en place dans leur organisation. Après avoir pris connaissance de l'aperçu, ils ont conclu que le programme fédéral serait un bon complément et qu'il leur permettrait sans doute d'obtenir les résultats qu'ils recherchent à travers leurs propres initiatives. Cela étant dit, les groupes de l'industrie accueilleraient favorablement l'occasion de collaborer avec le gouvernement fédéral pour s'assurer que les exigences de certification tiennent compte des besoins particuliers de leurs industries respectives. Quelques participants étaient d'avis que tout effort pour trouver une solution universelle ne répondrait pas aux besoins particuliers de chacun.

Un participant s'inquiétait que l'objectif du programme, qui vise les petites et moyennes entreprises, pourrait suggérer que la certification est « allégée » ou simplifiée pour répondre aux besoins des plus petites entreprises canadiennes. Il a ajouté que si les grandes entreprises étaient elles aussi certifiées, cela conférerait beaucoup de crédibilité au programme et à la certification qui en résulte.

En dernier lieu, certains ont dit souhaiter que la certification ne devienne pas une activité unique ou « à cocher » sur la liste. Ils ont suggéré d'intégrer une formation continue, un engagement et un renouvellement de la certification au processus, de manière à garantir la réussite du programme à long terme.

# Méthodologie détaillée

**La méthodologie de recherche consistait en dix groupes de discussion en ligne et six entrevues individuelles sur le Web.** Les groupes de discussion étaient composés de représentants de petites et moyennes entreprises (PME) canadiennes, avec un accent sur celles qui comptent un plus grand nombre d'employés (40 et plus). Les séances ont eu lieu partout au pays, dans de moyennes et grandes villes ainsi que des régions rurales et éloignées. Des entrevues individuelles sur le Web ont été organisées avec un éventail de grandes entreprises et de groupes et d'associations de l'industrie (p. ex., des associations professionnelles ou de gens d'affaires).

Quorus était responsable de coordonner tous les aspects du projet de recherche, y compris de collaborer avec ISDE pour la conception et la traduction du questionnaire de recrutement, des courriels d'invitation et des guides de l'animateur, de recruter les participants, de gérer la plateforme pour les entrevues en ligne et la logistique associée, d'animer toutes les séances et diriger les entrevues, et de livrer tous les rapports exigés au terme de la collecte de données. La méthodologie de recherche est décrite plus en détail ci-dessous.

## Groupes cibles et échantillon

La recherche a été menée avec deux larges segments du milieu des affaires :

- **Premier groupe cible – Petites et moyennes entreprises (PME) canadiennes :** Ce groupe était composé de PME canadiennes et d'organismes sans but lucratif, avec un accent sur les plus grandes organisations (40 employés et plus). Dans ce groupe, la recherche visait un sous-segment d'entreprises d'intérêt pour ISDE, notamment des entreprises faisant partie d'une chaîne logistique, des entreprises du secteur de la fabrication et d'autres qui avaient adopté un modèle numérique en ligne durant la pandémie. Au sein de chaque organisation, la recherche ciblait un décideur en matière de cybersécurité ou une personne jouant un rôle de premier plan dans les opérations quotidiennes et la direction de l'entreprise.

  Pour ce segment, nous avons fait de notre mieux pour recruter des participants provenant des groupes démographiques suivants :

  - Des femmes, des Autochtones, des Noirs et des personnes handicapées propriétaires d'entreprises ou occupant un poste de direction
  - Des entreprises de régions rurales ou éloignées

- **Deuxième groupe cible – Groupes et organisations de l'industrie et grandes entreprises canadiennes :** Ce groupe était largement défini comme dépendant de chaînes logistiques ou d'organisations susceptibles d'influencer les PME d'une quelconque façon ou qui

coordonnent ces chaînes ou organisations. Plusieurs types d'organisations avaient été sélectionnés par ISDE, notamment :

- des entreprises qui gèrent ou qui utilisent des chaînes logistiques
- des associations professionnelles de l'industrie en mesure d'influencer les PME
- des associations de gens d'affaires en mesure d'influencer les PME

En plus des critères généraux susmentionnés, d'autres mesures ont été utilisées pour recruter des participants de qualité :

- Nous avons exclu tout participant qui occupait un poste au sein d'un ministère ou d'un organisme gouvernemental, d'une agence de publicité, d'une firme d'études de marché, d'un cabinet de relations publiques ou des médias (radio, télévision, journaux, production vidéo ou cinématographique, etc.). Cette exclusion s'appliquait également aux membres de la famille ou du ménage d'un participant.
- De plus, nous avons exclu tout participant qui avait occupé un tel poste au cours des cinq années précédentes, en fonction des objectifs de la recherche.
- Nous avons exclu tous les participants qui se connaissaient, à moins qu'ils soient à des séances différentes, tenues à des moments différents.
- Nous avons exclu tout participant qui aurait pris part à une séance de recherche qualitative au cours des six mois précédents.
- Nous avons également exclu tout participant qui avait pris part à cinq séances ou plus de recherche qualitative au cours des cinq années précédentes.
- Nous avons exclu tout participant qui avait pris part à une séance de recherche qualitative sur le même sujet, tel que défini par le chercheur ou l'animateur au cours des deux années précédentes.

**Deuxième groupe cible :** Nous avons recruté les participants à partir d'une liste remise à Quorus par ISDE, laquelle incluait le nom de l'organisation ou de l'entreprise, le nom d'une personne-ressource, un numéro de téléphone et/ou une adresse de courriel. Nous avons obtenu les coordonnées d'autres participants par l'entremise d'associations contactées par des consultants de Quorus. Pour s'assurer qu'elles étaient admissibles à participer à cette phase de l'étude, toutes les organisations ont été approuvées par ISDE avant d'être contactées.

## Description des procédures de collecte des données

La collecte de données a été effectuée exclusivement durant les discussions de groupes en ligne et les entrevues individuelles sur le Web. La durée des séances était comme suit :

- Groupes de discussion de la phase 1 – Test de concept initial : 90 minutes
- Groupes de discussion de la phase 1 – Vérification du succès : 60 minutes
- Entrevues en profondeur de la phase 2 : 45 minutes

Les participants du premier groupe cible ont été sélectionnés par Quorus au téléphone; nous en avons recruté six pour nous assurer de la présence de quatre à six dans chaque groupe. Le choix des participants a été effectué par une combinaison d'appels téléphoniques aléatoires et le recours à une base de données exclusive. Ces candidats ont été recrutés à l'aide d'un questionnaire pour s'assurer qu'ils répondaient aux critères établis pour cette étude.

Le recrutement pour le deuxième groupe cible a été effectué exclusivement à partir des listes fournies par ISDE, par les consultants de Quorus, avec le soutien du personnel d'ISDE qui entretenaient déjà des relations de travail avec certains des candidats visés par cette étude. Ces personnes ont été informées par ISDE avant le début du projet qu'elles seraient contactées par un consultant de Quorus pour une entrevue.

Le recrutement des participants pour les groupes de discussion et les entrevues en profondeur a été fait conformément aux règles de sélection, de recrutement et de protection de la vie privée établies dans les *Normes pour la recherche sur l'opinion publique effectuée par le gouvernement du Canada – Recherche qualitative.* Les exigences suivantes ont également été respectées :

- Toutes les activités de recrutement se sont déroulées dans la langue officielle de préférence du participant, en français ou en anglais selon le cas
- Nous avons informé les participantes de l'accès aux résultats de recherche, sur demande.
- Nous avons fourni l'énoncé de confidentialité de Quorus, sur demande.
- La procédure de recrutement a permis de confirmer la capacité de chaque participant de pouvoir communiquer, comprendre, lire et écrire dans la langue utilisée dans leur séance.
- Nous avons informé les participants de leurs droits en vertu de la *Loi sur la protection des renseignements personnels,* de la *Loi sur la protection des renseignements personnels et les documents électroniques* et de la *Loi sur l'accès à l'information* et nous leur avons donné l'assurance que ces droits seraient protégés tout au long du processus de recherche. Plus précisément, nous avons informé les participants du but de la recherche; de l'identité du ministère ou de l'agence ou le gouvernement du Canada globalement qui la parrainait, et que leur participation à cette étude était tout à fait volontaire. Enfin, nous avons informé les participantes que l'administration des renseignements donnés respecterait les exigences de la *Loi sur la protection des renseignements personnels.*

À l'étape du recrutement et au début de chaque groupe de discussion, nous avons informé les participants que cette recherche se faisait pour le compte du gouvernement du Canada /ISDE.



Nous avons aussi informé les participants que les séances seraient enregistrées et que des observateurs du gouvernement du Canada et ISDE seraient présents. Quorus s'est assuré d'obtenir le consentement préalable des participants lors de l'étape du recrutement ainsi qu'au début de chaque séance de discussion.

Tous les groupes de discussion en ligne ont eu lieu en soirée, après les heures normales de bureau, alors que les entrevues individuelles se sont déroulées durant les heures normales de bureau ou en soirée (selon les disponibilités et les préférences des participants). L'équipe de recherche a utilisé la plateforme Zoom pour héberger et enregistrer les séances (avec des microphones et des webcams connectés aux appareils électroniques de l'animateur et des participants, tels qu'ordinateurs portables et tablettes) pour permettre à nos clients d'observer les échanges à distance.

La recherche comportait deux phases :

**Phase 1 – Groupes de discussion en ligne**

Au total, il y avait dix séances de discussion de groupes divisées en deux étapes :

- **Étape 1 – Un test de concept initial** qui consistait en huit groupes de discussion et qui avait pour but de recueillir les premiers commentaires sur les concepts, dans ces régions (toutes les séances avaient lieu en anglais, sauf à Montréal et les environs :
    - Vancouver et les environs
    - Calgary/Edmonton et les environs
    - Saskatoon/Regina et les environs
    - Winnipeg et les environs
    - Toronto et les environs
    - Centres urbains de l'Ontario autres que Toronto
    - Montréal et les environs
    - Canada atlantique (mélange des quatre provinces)

- **Étape 2 – Une vérification du succès** qui consistait en deux groupes de discussion et qui avait pour but de recueillir des commentaires sur les versions définitives des concepts de la part d'entreprises dans les régions suivantes :
    - Manitoba, Saskatchewan et Alberta (en anglais)
    - Québec, Nouveau-Brunswick et Ontario (en français)

Les renseignements au sujet de ces groupes sont présentés ci-dessous.

| Ville | Segment | Langue | Nombre de participants | Date et heure | Prime |
|---|---|---|---|---|---|
| **Phase 1 – Étape 1 (travail préparatoire)** | | | | | |
| **Région de Toronto** | PME | Anglais | 5 | 25 janvier 17 h 30 | 200 $ |
| **Ontario, à l'exception de Toronto** | PME | Anglais | 5 | 25 janvier 19 h 30 | 200 $ |
| **Canada atlantique** | PME | Anglais | 6 | 26 janvier 17 h 30 | 200 $ |
| **Région de Montréal** | PME | Français | 6 | 26 janvier 19 h 30 | 200 $ |
| **Saskatoon/ Regina** | PME | Anglais | 6 | 27 janvier 18 h 30 | 200 $ |
| **Région de Winnipeg** | PME | Anglais | 6 | 27 janvier 20 h 30 | 200 $ |
| **Calgary/ Edmonton** | PME | Anglais | 6 | 28 janvier 19 h 30 | 200 $ |
| **Région de Vancouver** | PME | Anglais | 4 | 28 janvier 21 h 30 | 200 $ |
| **Phase 1 – Étape 2 (vérification du succès)** | | | | | |
| **Québec/Nouveau-Brunswick/Ontario** | PME | Français | 5 | 16 février 17 h 30 | 200 $ |
| **Manitoba/ Saskatchewan/Alberta** | PME | Anglais | 5 | 16 février 19 h | 200 $ |

**Phase 2 – Entrevues en profondeur**

Au total, six entrevues individuelles sur le Web ont été réalisées avec des participants du deuxième groupe cible, dans la langue officielle choisie par ceux-ci.

Les renseignements au sujet des séances sont présentés ci-dessous :

| Entrevue | Langue | Date et heure | Prime |
|---|---|---|---|
| **Entrevue 1 : secteur privé** | Anglais | 22 avril à 10 h 30 | 250 $ |
| **Entrevue 2 : association ou organisation professionnelle de l'industrie** | Anglais | 6 mai à 10 h | 250 $ |
| **Entrevue 3 : association ou organisation professionnelle de l'industrie** | Bilingue | 10 mai à 13 h | 250 $ |
| **Entrevue 4 : association ou organisation professionnelle de l'industrie** | Anglais | 11 mai à 11 h | 250 $ |
| **Entrevue 5 : association ou organisation professionnelle de l'industrie** | Anglais | 12 mai à 8 h | 250 $ |
| **Entrevue 6 : secteur privé** | Anglais | 26 mai à 11 h | 250 $ |

# Annexes

# Phase 1 – Questionnaire de recrutement pour les PME

| **Groupes de discussion en ligne**<br>(A = anglais; F = français) | **Détails :**<br>Sélectionner 6 participants pour s'assurer de la présence de 4 à 6 d'entre eux<br><br>Incitatif : 200 $<br><br>Séances de 90 minutes |
|---|---|
| **Groupe 1 :** Toronto et régions avoisinantes (A); 25 janvier, 17 h 30 HNE | |
| **Groupe 2 :** Centres urbains de l'Ontario autres que Toronto (A); 25 janvier, 19 h 30 HNE | |
| **Groupe 3 :** Canada atlantique (mélange des 4 provinces) (A); 26 janvier, 17 h 30 HNM | |
| **Groupe 4 :** Montréal et régions avoisinantes (F); 26 janvier, 19 h 30 HNE | |
| **Groupe 5 :** Saskatoon/Regina et régions avoisinantes (A); 27 janvier, 17 h 30 HNC | |
| **Groupe 6 :** Winnipeg et régions avoisinantes (A); 27 janvier, 19 h 30 HNC | |
| **Groupe 7 :** Calgary/Edmonton et régions avoisinantes (A); 28 janvier, 17 h 30 HNR | |
| **Groupe 8 :** Vancouver et régions avoisinantes (A); 28 janvier, 18 h 30 HNP | |
| **Groupe 9 :** Québec/Nouveau-Brunswick/Ontario (F); 16 février, 17 h 30 HNE | |
| **Groupe 10 :** Manitoba/ Saskatchewan/Alberta (A); 16 février, 19 h 00 HNE | |

**Public cible**

Les PME canadiennes et les organismes sans but lucratif, avec l'accent sur les petites organisations de plus grande taille (qui comptent 40 employés et plus). Dans ce groupe, la recherche ciblera un sous-segment d'entreprises d'intérêt pour ISED, y compris des entreprises de chaîne d'approvisionnement, du secteur manufacturier et celles qui ont adopté un modèle numérique en ligne durant la pandémie. Dans chaque organisation, la recherche ciblera un décideur en matière de cybersécurité ou une personne qui joue un rôle de premier plan dans les opérations quotidiennes et la direction de l'entreprise.

Dans ce segment, la recherche tiendra également compte, dans la mesure du possible, des groupes démographiques suivants dans ses efforts de recrutement. Toutefois, compte tenu de l'échéancier du projet, leur représentation ne peut être garantie.

- Des femmes, des propriétaires d'entreprise / gestionnaires Autochtones, des propriétaires d'entreprise / gestionnaires Noirs et des personnes handicapées propriétaires d'entreprise ou occupant un poste de direction;
- Des entreprises situées en zones rurales ou éloignées.

## A. Introduction

Bonjour. Je m'appelle _____et je téléphone du groupe-conseil Quorus, une firme canadienne de recherche sur l'opinion publique, au nom du gouvernement du Canada.

Préférez-vous continuer en anglais ou en français ? / Would you prefer to continue in English or French?

**[NOTE POUR L'INTERVIEWEUR : POUR LES DISCUSSIONS OU LES ENTREVUES EN ANGLAIS, SI LE PARTICIPANT PRÉFÈRE CONTINUER EN FRANÇAIS, RÉPONDRE : « Malheureusement, nous recherchons des gens qui parlent anglais pour participer à cette recherche. Nous vous remercions de votre intérêt. » POUR LES DISCUSSIONS OU LES ENTREVUES EN FRANÇAIS, SI LE PARTICIPANT PRÉFÈRE CONTINUER EN ANGLAIS, RÉPONDRE : « Unfortunately, we are looking for people who speak French to participate in this research. We thank you for your interest. »]**

De temps à autre, nous sollicitons des opinions en discutant avec des gens. Nous nous apprêtons à mener plusieurs discussions pour le gouvernement du Canada. J'aimerais m'entretenir avec la personne dans votre organisation qui joue un rôle de premier plan dans les opérations courantes et la direction de l'entreprise, et qui connaît bien ses systèmes de TI et les pratiques de gestion des données. Est-ce que la personne qui répond à ces critères est disponible pour discuter avec moi ? Il pourrait s'agir du propriétaire ou du président de l'entreprise, ou encore de la personne responsable des TI.

**UNE FOIS QUE LA BONNE PERSONNE EST AU BOUT DU FIL, RÉPÉTER L'INTRODUCTION, AU BESOIN ET CONTINUER.**

Nous vous téléphonons aujourd'hui pour vous inviter à une séance de recherche où vous pourrez partager vos commentaires sur les opportunités qui s'offrent à votre entreprise et les défis qu'elle doit affronter, et sur le rôle que devrait jouer le gouvernement du Canada, selon vous, en rapport avec ceux-ci.

D'autres décideurs de petites et moyennes entreprises canadiennes participeront à ce projet de recherche. Pour la discussion, nous n'utiliserons que les prénoms des participants. Personne, y compris le gouvernement du Canada, ne saura quelles sont les entreprises représentées. En guise de remerciement, les participants recevront une prime en argent.

La participation est strictement volontaire. Toutes les opinions demeureront anonymes et elles serviront uniquement aux fins de la recherche, conformément aux lois visant à pour protéger votre vie privée. Nous voulons simplement entendre vos opinions. Personne ne tentera de vous vendre quoi que ce soit. La discussion prendra la forme d'une discussion en ligne menée par un professionnel de la recherche.

La protection de la santé et de la prospérité économique des Canadiens en période de pandémie de COVID-19 est une priorité du gouvernement du Canada. Les résultats de sondages comme celui-ci lui permettront au gouvernement canadien de continuer à remplir son mandat et améliorer son travail.

**[NOTE POUR L'INTERVIEWEUR : SI ON VOUS QUESTIONNE AU SUJET DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, DITES : « Les renseignements recueillis durant la recherche sont régis par les dispositions de la *Loi sur la protection des* renseignements personnels, les lois du**

**gouvernement du Canada et les lois provinciales en matière de protection des renseignements personnels. »]**

Avant de vous inviter à participer, j'aimerais vous poser quelques questions pour m'assurer qu'une bonne variété d'entreprises soit représentée. Cela ne prendra que 5 minutes. Si vous hésitez, je tiens à souligner que **toutes mes questions concernent les activités de votre entreprise au Canada.** Puis-je vous poser quelques questions?

| | | |
|---|---|---|
| Oui | 1 | **CONTINUER.** |
| Non | 2 | **REMERCIER ET METTRE FIN À L'ENTRETIEN.** |

## B. Profil de l'entreprise et du répondant

1. Comment évaluez-vous votre niveau de connaissance à l'égard de la sécurité et de la confidentialité des renseignements en lien avec l'utilisation des technologies numériques dans un contexte d'entreprise ? Diriez-vous que le sujet vous est… **LIRE LES CHOIX DE RÉPONSES ET RECRUTER UNE VARIÉTÉ DE PARTICIPANTS.**

   **AU BESOIN :** Dans toute entreprise, les risques et les défis associés à l'utilisation des technologies numériques (par exemple, lorsqu'un ordinateur est connecté à Internet) sont nombreux lorsqu'il s'agit de gérer la sécurité et la confidentialité des données. Comment évaluez-vous votre niveau de familiarité à l'égard de ces risques et de ces défis ?

   - Très familier
   - Plutôt familier
   - Pas très familier
   - Pas du tout familier

**SI A RÉPONDU PAS TRÈS FAMILIER OU PAS DU TOUT FAMILIER, DEMANDER :** ***Puisque ce sera un des thèmes de la discussion, y a-t-il quelqu'un d'autre dans votre entreprise qui connaîtrait mieux ces enjeux ?***

- **SI OUI, DEMANDER À PARLER À CETTE PERSONNE.**
- **SINON, CONTINUER.**

2. En vous comptant, environ combien d'employés à temps plein (ETP) votre entreprise compte-t-elle au Canada? **(NOTER LE NOMBRE EXACT.)**

   _____ employés à temps plein

   - De 1 à 5 **[PETITE ENTREPRISE ET MICROENTREPRISE]**
   - De 6 à 99 **[PETITE ENTREPRISE]**
   - De 100 à 499 **[MOYENNE ENTREPRISE]**
   - 500 ou plus **[REMERCIER ET METTRE FIN À L'ENTRETIEN.]**

3. Faites-vous partie de l'une de ces catégories ?

| | | Oui | Non |
|---|---|---|---|
| a) | Êtes-vous aveugle ou avez-vous de la difficulté à voir, même en portant des lunettes ou des verres de contact ? **(SI LA RÉPONSE EST OUI, REMERCIER ET METTRE FIN À L'ENTRETIEN.)** | ❑ | ❑ |
| b) | Êtes-vous atteint d'un handicap physique ou avez-vous de la difficulté à marcher, à utiliser des escaliers, à vous servir de vos mains ou de vos doigts ou à faire d'autres activités physiques ? | ❑ | ❑ |
| c) | Avez-vous de la difficulté à apprendre, à retenir de l'information ou à vous concentrer ? | ❑ | ❑ |
| d) | Avez-vous un trouble d'ordre émotionnel, psychologique ou mental ? | ❑ | ❑ |
| e) | Votre entreprise est-elle située dans une municipalité, un village ou une zone rurale de moins de 10 000 habitants et à au moins deux heures de route d'une ville de 50 000 habitants et plus ? | ❑ | ❑ |

*Source : Enquête Canadienne sur l'incapacité de 2017

- *SI A RÉPONDU OUI À Q3A-D – RECRUTER COMME ENTREPRENEUR/EXPLOITANT D'ENTREPRISE/DÉCIDEUR HANDICAPÉ.*
- *SI A RÉPONDU OUI À Q3E – RECRUTER COMME ENTREPRENEUR/EXPLOITANT D'ENTREPRISE/DÉCIDEUR EN ZONE RURALE OU ÉLOIGNÉE.*

4. Vous identifiez-vous comme… ?

   - un Autochtone (Premières nations, Inuit ou Métis); les Premières nations incluent les Indiens inscrits et non-inscrits
   - un membre d'un groupe ethnoculturel ou d'une minorité visible autre qu'Autochtone
   - Aucune de ces réponses

- *SI A RÉPONDU OUI À Q4=1 : RECRUTER COMME ENTREPRENEUR/EXPLOITANT D'ENTREPRISE/DÉCIDEUR AUTOCHTONE.*
- *SI A RÉPONDU OUI À Q4=2 : RECRUTER COMME ENTREPRENEUR/EXPLOITANT D'ENTREPRISE/DÉCIDEUR ISSU D'UNE COMMUNAUTÉ ETHNIQUE.*

5. **[DEMANDER SEULEMENT SI Q4=2]** Quelle est votre origine ethnique?

   **NOTER L'ORIGINE ETHNIQUE :** _____

6. Dans quelle industrie ou quel secteur votre entreprise exerce-t-elle ses activités? Si elle est active dans plus d'un secteur, veuillez indiquer le secteur principal. **NE PAS LIRE LA LISTE. N'ACCEPTER QU'UNE SEULE RÉPONSE. CONFIRMER LE RÉSULTAT AVEC LE RÉPONDANT, AU BESOIN. RECRUTER UN MÉLANGE DE PARTICIPANTS.**

   - Agriculture/pêche/chasse/ foresterie
   - Pétrole/gaz/mines
   - Services publics
   - Construction
   - Fabrication
   - Commerce de gros
   - Commerce de détail
   - Transport et entreposage
   - Industrie de l'information et industrie culturelle
   - Finances et assurances/services immobiliers et services de location
   - Services professionnels, scientifiques et techniques/TI/ informatique
   - Services administratifs et services de soutien
   - Gestion des déchets
   - Services d'assainissement
   - Arts/spectacles/loisirs
   - Hébergement/services alimentaires/tourisme
   - Organisme sans but lucratif/organisme de bienfaisance
   - Autre (préciser)

7. Quel poste occupez-vous? _____

8. Votre entreprise livre-t-elle des biens ou des services à l'intérieur d'une chaîne d'approvisionnement? Autrement dit, une ou plusieurs entreprises offrent des produits et des services à votre organisation et en retour, vous fournissez des produits et des services à une ou plusieurs autres entreprises.

   - Oui **ENTREPRISES DE CHAÎNE D'APPROVISIONNEMENT : EN RECRUTER AU MOINS 2 DANS CHAQUE GROUPE.**
   - Non

9. Depuis le début de la pandémie de COVID-19, votre entreprise a-t-elle dû compter davantage sur l'Internet pour poursuivre ses activités? Par exemple, le personnel a fait davantage de télétravail qu'auparavant, vous avez commandé ou vendu des produits et des services en ligne plus souvent, et ainsi de suite.

   - Oui **ADAPTÉS EN LIGNE DURANT LA PANDÉMIE : EN RECRUTER AU MOINS 2 DANS CHAQUE GROUPE.**
   - Non

10. Les participants aux discussions de groupe ou aux entrevues sont invités à exprimer leurs opinions et leurs pensées. Dans quelle mesure êtes-vous à l'aise de vous exprimer devant d'autres personnes? Êtes-vous…? **LIRE LES RÉPONSES**

| | |
|---|---|
| o Très à l'aise | **MINIMUM DE 5 PAR GROUPE** |
| o Assez à l'aise | |
| o Pas très à l'aise | **METTRE FIN À L'ENTRETIEN.** |
| o Pas à l'aise du tout | **METTRE FIN À L'ENTRETIEN.** |

11. Puisque nous voulons recruter une variété de participants, pourriez-vous me dire comment vous vous identifiez? Diriez-vous que vous êtes… ?

**Note 1 :** Recruter une bonne variété de participants parmi tous les groupes.
**Note 2 : *NE PAS LIRE :*** *Genre – Confirmer le genre actuel, qui pourrait être différent de celui à la naissance (masculin ou féminin) ou de celui qui figure sur les documents juridiques.*

- o Genre masculin
- o Genre féminin
- o Diversité de genre
- o Préfère ne pas répondre

12. Avez-vous déjà participé à une discussion de groupe ou à une entrevue portant sur un sujet établi à l'avance et pour laquelle vous avez été rémunéré ?

| | |
|---|---|
| o Oui | **MAXIMUM DE 5 PAR GROUPE** |
| o Non | **PASSER À L'INVITATION.** |

13. À quand remonte cette dernière discussion de groupe ou entrevue ?

| | |
|---|---|
| o Au cours des 6 derniers mois | **METTRE FIN À L'ENTRETIEN.** |
| o Il y a plus de 6 mois | |

14. À combien de discussions de groupe ou entrevues avez-vous participé au cours des 5 dernières années ?

| | |
|---|---|
| o Moins de 5 | |
| o 5 ou plus | **METTRE FIN À L'ENTRETIEN.** |

## C. Invitation pour le groupe de discussion en ligne

J'aimerais vous inviter à participer à une discussion de groupe en ligne dirigée par un expert-conseil d'une entreprise canadienne de recherche sur l'opinion publique, le groupe-conseil Quorus. La séance pour les entreprises de votre région aura lieu le **[JOUR] [DATE]** à **[HEURE]** et durera 90 minutes. Les participants recevront 200 $ en guise de remerciement. Nous vous ferons parvenir ce montant par virement courriel ou par chèque envoyé par la poste, une fois la séance terminée.

Acceptez-vous de participer ?

- ○ Oui
- ○ Non **METTRE FIN À L'ENTRETIEN.**

La séance sera enregistrée sur support audiovisuel pour les fins de la recherche. Des membres de l'équipe de recherche du gouvernement du Canada observeront la discussion en ligne. Vous devrez reconnaître que vos propos seront enregistrés. Les enregistrements seront utilisés uniquement par l'équipe de recherche du groupe-conseil Quorus. Ils ne seront pas partagés avec des tierces parties. Comme je l'ai mentionné précédemment, tous les renseignements recueillis durant la discussion demeureront strictement anonymes et serviront uniquement aux fins de la recherche, conformément aux lois qui protègent votre vie privée.

Pour la séance, nous utiliserons une application de vidéoconférence afin que vous puissiez voir le matériel qui vous sera présenté. Nous vous enverrons les directives de connexion par courriel. L'utilisation d'un ordinateur est nécessaire pour voir le matériel et partager vos réactions. Ce sera un volet important de la discussion. **Si vous le désirez, vous pouvez utiliser une tablette, mais pas un téléphone intelligent, car l'écran est trop petit.**

**SI LE RÉPONDANT POSE LA QUESTION :** On vous demandera d'utiliser une webcam pour la discussion. Assurez-vous que votre appareil est doté d'un microphone et d'une caméra qui fonctionnent.

Au cours des prochains jours, nous vous enverrons par courriel le lien pour vous connecter en ligne, de même que la date et l'heure de la séance.

Nous vous recommandons de cliquer sur le lien que nous vous enverrons quelques jours avant la date prévue pour la séance afin de nous assurer que vous pourrez avoir accès à la plateforme en ligne qui aura été aménagée. Vous devrez répéter les étapes au moins 10 à 15 minutes avant la séance.

Puisque nous n'invitons qu'un nombre restreint de participants, votre présence est essentielle. Si vous n'êtes pas en mesure de participer, pour quelque raison que ce soit, veuillez nous contacter dans les plus brefs délais afin que nous puissions vous trouver un remplaçant. Vous pouvez nous joindre au **1 800 XXX-XXXX**. Demandez à parler à **[nom de la personne à contacter]**. Quelqu'un vous téléphonera la veille pour confirmer votre présence.

Afin que nous puissions vous envoyer le courriel de directives, vous téléphoner pour le rappel ou vous contacter pour vous informer d'un changement, pourrais-je avoir votre nom et vos coordonnées ?
**NOTER LES RENSEIGNEMENTS SUR LA PREMIÈRE PAGE.**

**Merci de votre collaboration !**

# Guide du modérateur pour les entrevues de groupe – PME (Phase 1)

## A. Introduction (8 minutes)

- Présentation du modérateur : mentionner qu'il travaille pour le groupe-conseil Quorus et que la recherche est menée au nom du gouvernement du Canada (préciser que le modérateur n'est pas un employé du GdC).
- Merci de votre présence.
- Expliquer le but des groupes de discussion :
    - Nous voulons connaitre vos *opinions* sur certains enjeux, concepts ou produits.
    - Il ne s'agit pas d'un test de connaissances ; il n'y a pas de bonnes ou de mauvaises réponses (nous voulons simplement connaître vos opinions).
    - La séance d'aujourd'hui durera environ 90 minutes.
    - Vous pouvez être en désaccord. Nous vous encourageons à vous exprimer ouvertement, même si vos opinions diffèrent des autres.
    - Vous n'êtes pas obligés de m'adresser tous vos commentaires; vous pouvez aussi échanger entre vous.
    - Nous vous encourageons à parler en toute franchise. Les commentaires recueillis demeureront anonymes et seront présentés sous forme agrégée. L'enregistrement audiovisuel et la prise de notes nous serviront à rédiger le rapport. Des observateurs assisteront à la séance par cyberconférence.
    - Tous les commentaires recueillis demeureront confidentiels. Personne d'autre que nous aura accès aux enregistrements. Pour partager ces enregistrements ou vos renseignements personnels, il nous faudrait obtenir d'abord votre consentement par écrit.
    - Veuillez éteindre vos téléphones cellulaires.
    - Pour participer, assurez-vous que votre webcam et votre microphone sont activés et que vous m'entendez bien. Quand vous ne parlez pas, je vous suggère de désactiver le son afin de réduire le plus possible les bruits ambiants. N'oubliez pas d'activer le son si vous souhaitez prendre la parole.
    - Je partagerai mon écran avec vous pour vous montrer des éléments visuels.

- Nous utiliserons fréquemment la fonction de clavardage (*chat*). Pour y accéder, veuillez faire défiler votre écran jusqu'en bas. Vous verrez apparaître la commande « clavardage » et une fenêtre s'ouvrira à la droite de l'écran. Je vous demande d'utiliser cette fonction tout au long de la discussion. Faisons un essai rapide maintenant. Ouvrez la fenêtre de clavardage et envoyez un court message au groupe (p. ex., Bonsoir tout le monde). Si vous avez la réponse à une question qui ne vous était spécifiquement adressée, tapez votre réponse ici. Nous lirons tous vos commentaires à la fin du projet.

- Si vous n'avez pas l'occasion de vous exprimer durant la séance, vous pouvez commenter en utilisant la fonction de clavardage. La plupart du temps, discutez entre vous, à moins que vous ressentiez le besoin de m'envoyer un message en privé.

Prenons quelques minutes pour faire les présentations. J'aimerais savoir :

- Quel type d'entreprise possédez-vous, exploitez-vous ou gérez-vous?
- Quel est votre rôle au sein de l'entreprise?
    - Êtes-vous responsables des questions relatives aux TI ou à la cybersécurité?
- À ce titre, quelle est votre plus grande préoccupation ces jours-ci? Qu'est-ce qui vous empêche de dormir?
    - Que signifie la cybersécurité pour vous?

## B. Confiance de l'entreprise envers le niveau actuel de cybersécurité (20 minutes)

Tout d'abord, combien parmi vous ont dû augmenter leur présence en ligne en raison de la pandémie ou adopter rapidement de nouvelles technologies Internet pour continuer leurs activités? **AU BESOIN :** … médias sociaux, plateformes de commerce électronique ou autres applications?

- Pouvez-vous me donner des exemples des moyens qu'a pris votre entreprise pour s'adapter?

Dans l'ensemble, que pensez-vous de votre niveau de cybersécurité ces jours-ci, compte tenu des répercussions majeures de la pandémie sur l'économie numérique? Je parle ici de votre sentiment quant à la sécurité de l'ensemble de votre système des TI – y compris vos ordinateurs, vos réseaux Internet et Wi-Fi, votre système de stockage et de protection des données de votre entreprise, ainsi que toute information sur vos clients, fournisseurs, employés, etc.

- Pour m'aider à comprendre, utilisez la fonction de clavardage et répondez à la question suivante : sur une échelle de 0 à 10, où 0 signifie que vous vous sentez extrêmement vulnérable et 10, que vous vous sentez entièrement protégé, comment évaluez-vous votre niveau de cybersécurité ces jours-ci? Allez-y, écrivez dans la fenêtre de clavardage, puis nous en discuterons ensemble. **LE MODÉRATEUR NOTE LES RÉSULTATS.**

- Qu'est-ce qui vous inquiète au juste? Y a-il-place à amélioration?
- Vos clients se soucient-ils du niveau de cybersécurité de votre entreprise?
    - Si c'est le cas, croyez-vous qu'ils remarquent tous vos investissements en matière de cybersécurité? Comment le savez-vous? Comment peuvent-ils le savoir?

**<u>Télétravail et transition vers le commerce électronique</u>**

J'aimerais discuter des façons dont certains parmi vous ont dû s'adapter à la pandémie. Parlons d'abord du télétravail qui est à la hausse.

- Levez la main si vous avez des employés en télétravail.

- Vos employés étaient-ils déjà en télétravail avant la pandémie?
    - **DANS L'AFFIRMATIVE :** Quels sont les infrastructures, les systèmes ou les procédures que vous avez mis en place?
        - **AU BESOIN :** Vos employés utilisent-ils leurs appareils personnels?
- Quels sont les infrastructures, les systèmes ou les procédures que vous avez dû mettre en place? **SONDER AU BESOIN :**
    - Avez-vous dû établir des politiques pour les espaces de travail sur les appareils personnels? Ou fournir des appareils que les employés doivent utiliser exclusivement pour le travail?
    - Votre entreprise a-t-elle accéléré la migration vers les infrastructures et applications infonuagiques?
    - Votre entreprise a-t-elle été forcée d'accroître sa fonctionnalité et son utilisation des outils de collaboration en ligne, comme MS Teams, Zoom, Google Meetings, etc.?

Parlons maintenant de la **transition vers le commerce électronique**.

- Avez-vous constaté une augmentation de votre commerce électronique ?
- Levez la main si c'est le cas pour votre entreprise.
    - Dans quelle mesure êtes-vous convaincus d'avoir fait la transition de manière sécuritaire ?

- Votre entreprise s'est-elle adaptée pour mener des évaluations de risques et mettre en place des mesures coercitives en adoptant ces nouvelles technologies, que ce soit pour le télétravail ou le commerce électronique ?

- Avez-vous été victimes de cyberattaques liées à l'augmentation du télétravail ?

- Qu'en est-il des cyberattaques liées à l'augmentation du commerce électronique ?

- Étiez-vous au courant qu'il y avait eu augmentation du nombre de cyberattaques depuis le début de la pandémie ?

    - **DANS L'AFFIRMATIVE :** Avez-vous fait quoi que ce soit pour préparer votre entreprise ?
    - **SINON :** Êtes-vous étonnés d'entendre parler de l'augmentation du nombre de cyberattaques depuis le début de la pandémie ?

## C. Évaluation globale des concepts (50 minutes – Concepts A, B et C)

Regardons maintenant quelques concepts publicitaires.

Le gouvernement a lancé un programme de certification en cybersécurité pour les petites et moyennes entreprises. Celles qui remplissent les critères sont « certifiées » et peuvent en faire mention en affichant la marque de certification de CyberSécuritaire Canada.

Nous aimerions obtenir vos commentaires sur des concepts publicitaires destinés à une campagne nationale visant à promouvoir l'importance de la cybersécurité en général, et à faire connaître le programme, plus précisément.

Je tiens à souligner qu'il s'agit de versions provisoires des concepts. Je suis impatient d'avoir vos opinions. Ces publicités apparaitront dans la section affaire des médias nationaux publiés et enligne (p. ex. La section affaire du Globe and Mail, de La Presse, etc.), sur des sites Internet sur les TI, etc.

Je vais partager quelques images avec vous à l'écran. Vous ne devez ni les copier ni prendre de captures d'écran. Vous ne pouvez pas non plus les partager avec d'autres personnes.

***POUR USAGE INTERNE SEULEMENT :***

**LE MODÉRATEUR PRÉSENTE LES CONCEPTS (CHACUN EST IDENTIFIÉ PAR UNE LETTRE) UN PAR UN (L'ORDRE CHANGE D'UNE SÉANCE à L'AUTRE).**

**CONCEPT A = PLUS FACILE**

**CONCEPT B = PREMIÈRE ÉTAPE**

**CONCEPT C = CONFIANCE**

**<u>Pour chaque groupe, randomiser les concepts comme suit :</u>**

| | |
|---|---|
| **Séance 1 : A, B, C** | **Séance 5 : B, A, C** |
| **Séance 2 : B, C, A** | **Séance 6 : C, B, A** |
| **Séance 3 : C, A, B** | **Séance 7 : A, B, C** |
| **Séance 4 : A, C, B** | **Séance 8 : B, C, A** |

Pour chaque concept, je vous présenterai (dans cet ordre) :

- une publicité imprimée
- une bannière publicitaire affichée dans le haut de chaque page Web que vous visitez

- une courte vidéo publicitaire qui serait diffusée en ligne (ET NON à LA TÉLÉVISION)

**LE MODÉRATEUR PRÉSENTE CHAQUE CONCEPT ET DONNE LE TEMPS AUX PARTICIPANTS DE LIRE CETTE QUESTION (autoquestionnaire)**

Veuillez considérer ce qui suit en regardant chaque publicité – vous pouvez prendre des notes, mais nous attendrons que tous aient terminé avant d'en discuter ensemble :

**LE MODÉRATEUR PRÉSENTE CE QUI SUIT À L'ÉCRAN APRÈS CHAQUE CONCEPT :**

*Quel est le but de cette publicité ?*
*Que ressentez-vous en la voyant ? À quoi pensez-vous ?*
*Feriez-vous quoi que ce soit après l'avoir vue ?*

**UNE FOIS QUE TOUS LES PARTICIPANTS ONT TERMINÉ, COMMENCER à SONDER :**

- Que pensez-vous de la publicité ? Aidez-moi à comprendre vos réactions…
- Quelles sont vos premières impressions? Qu'est-ce que vous avez aimé du concept? Et maintenant dites-moi ce que vous avez moins aimé.

J'aimerais avoir vos opinions du concept. Nous nous pencherons sur les trois composants clés de toute publicité :

1. le **message principal**, ce qu'on essaie de vous dire
2. l'**idée créative**, comment on essaie de vous transmettre ou vous présenter le message
3. l'**appel à l'action**, ce qu'on veut que vous fassiez ou pensiez.

**QUESTIONS EXPLORATOIRES POUR LE MESSAGE PRINCIPAL**

- Quel est le principal message du concept, qu'essaie-t-on de vous dire ?
- Est-ce que le message principal est…
  - clair ? Pourquoi ou pourquoi pas ?
  - nouveau pour vous ? De quelle façon ?
  - utile ou pertinent pour vous ? Pourquoi ou pourquoi pas ?
  - persuasif ? Pourquoi ou pourquoi pas ?
  - mémorable ? Pourquoi ou pourquoi pas ?

- Était-ce clair pour vous qu'il s'agissait d'une publicité du gouvernement du Canada ?

**QUESTIONS EXPLORATOIRES POUR L'IDÉE CRÉATIVE**

- Que pensez-vous de l'idée créative envisagée pour faire passer le message ? **SONDER :**
  - Décrivez-le-moi en vos propres mots.
    - Comment décririez-vous le ton de publicité ? Positif, négatif, dynamique, réaliste ? Est-ce approprié compte tenu du message ?
    - Qu'est-ce qui vous a plu ou déplu ?

- Qu'est-ce qui a capté votre attention : éléments visuels, texte, etc. ? Vers quoi votre regard a-t-il été attiré ?

**QUESTIONS EXPLORATOIRES POUR L'APPEL À L'ACTION**

- Qu'essaie-t-on de vous faire faire ou penser ? Le feriez-vous ? Pourquoi ou pourquoi pas ?
- Si vous alliez plus loin, sauriez-vous quelles seraient les prochaines étapes ?
- Vous rappelez-vous le nom du programme ? Quelle impression ce concept vous laisse-t-il de ce programme ? Pourquoi ?
- Visiteriez-vous le site Web après avoir vu cette publicité ? Pourquoi ou pourquoi pas ?
    - Quel site Web vous a-t-on présenté dans la publicité ?
    - Est-ce que le concept en fait suffisamment pour vous convaincre que le site Web contient de l'information utile aux propriétaires et exploitants d'entreprise comme vous ? Comment ?

**QUESTIONS EXPLORATOIRES APRÈS LA PRÉSENTATION DES TROIS CONCEPTS :**

- **LE MODÉRATEUR PRÉSENTE UN ÉCRAN CONTENANT LES TROIS CONCEPTS AVEC LES LETTRES QUI Y SONT ASSOCIÉES :** Lequel des trois concepts préférez-vous et pourquoi ? J'aimerais que vous répondiez tous à cette question. **Utilisez la fonction de clavardage et indiquez A, B ou C.**

- Pourrait-on faire quoi que ce soit pour améliorer la façon dont l'information est présentée dans le concept publicitaire que vous préférez ? Que suggérez-vous et pourquoi ?

- Où devrait-on diffuser cette publicité pour qu'elle attire votre attention ? Quelles sources consultez-vous pour obtenir de l'information pour votre entreprise ?

## D. Attentes définies par les publicités (12 minutes)

J'aimerais avoir vos premières réactions au programme de certification CyberSécuritaire lui-même. Ce programme de certification a été développé avec le Centre canadien de la cybersécurité.

**LE MODÉRATEUR PARTAGE SON ÉCRAN :**
Le programme de certification CyberSécuritaire Canada est un programme à participation volontaire de certification en cybersécurité mis en œuvre par le gouvernement du Canada.

Pour obtenir la certification, les entreprises doivent mettre en place 13 domaines de contrôle de sécurité couvrant un vaste éventail de points vulnérables pour les petites et moyennes entreprises, comme la formation du personnel, la protection des mots de passe, les plans d'intervention en cas d'incident, et plus encore.

Ces domaines de contrôle de sécurité ont été créés par le Centre canadien de la cybersécurité, les experts de la cybersécurité au Canada pour les petites et moyennes entreprises.

- Aviez-vous entendu parler de ce programme de certification avant la discussion d'aujourd'hui ?
    - Si c'est le cas, de quelle manière ?

- Envisageriez-vous d'obtenir votre certification ou prendriez-vous le temps qu'il faut pour le faire ? Aidez-moi à comprendre votre position là-dessus.

    **AU BESOIN :**

    - Vous sentiriez-vous mieux protégé ?
    - Avez-vous déjà envisagé d'autres programmes de certification ?

- Pensez-vous qu'il y a des avantages pour votre entreprise à s'associer à la marque CyberSécuritaire Canada ? De quelle façon ?

- Certains parmi vous faites partie de chaînes d'approvisionnement. Si ces chaînes exigeaient dorénavant une preuve de cybersécurité de leurs fournisseurs, est-ce que cela changerait votre opinion de la cyber certification ?

- Pour obtenir la certification, seriez-vous prêts et en mesure d'investir dans votre cybersécurité…
    - en effectuant une mise à jour de vos logiciels ?
    - en effectuant la mise à jour de votre matériel, comme les téléphones cellulaires, les ordinateurs, etc. ?
    - en effectuant une mise à niveau de votre infrastructure des TI ?
    - en investissant dans un audit de sécurité en vue d'obtenir une certification en cybersécurité ?

## E. REMERCIEMENTS ET CONCLUSION (2 minutes)

**[LE MODÉRATEUR CONSULTE L'ÉQUIPE DU CLIENT POUR VOIR SI ELLE A D'AUTRES QUESTIONS OU SI ELLE A BESOIN DE PRÉCISIONS.]**

En terminant, y a-t-il quelque chose que j'aurais dû vous demander, mais que je n'ai pas fait ?

Merci ! L'équipe qui vous a invité à participer à la séance communiquera avec vous pour obtenir des renseignements afin de vous faire parvenir l'incitatif que nous vous avons promis.

Bonne soirée à tous !

# Guide du modérateur pour les entrevues de groupe – PME (Phase 1 – vérification finale)

## A. Introduction (10 minutes)

- Présentation du modérateur : mentionner qu'il travaille pour le groupe-conseil Quorus et que la recherche est menée au nom du gouvernement du Canada (préciser que le modérateur n'est pas un employé du GdC).

- Merci de votre présence.

- Expliquer le but des groupes de discussion :

    - Nous voulons connaitre vos *opinions* sur certains enjeux, concepts ou produits.

    - Il ne s'agit pas d'un test de connaissances ; il n'y a pas de bonnes ou de mauvaises réponses (nous voulons simplement connaître vos opinions).

    - La séance d'aujourd'hui durera environ 60 minutes.

    - Vous pouvez être en désaccord. Nous vous encourageons à vous exprimer ouvertement, même si vos opinions diffèrent des autres.

    - Vous n'êtes pas obligés de m'adresser tous vos commentaires; vous pouvez aussi échanger entre vous.

    - Nous vous encourageons à parler en toute franchise. Les commentaires recueillis demeureront anonymes et seront présentés sous forme agrégée. L'enregistrement audiovisuel et la prise de notes nous serviront à rédiger le rapport. Des observateurs assisteront à la séance par cyberconférence.

    - Tous les commentaires recueillis demeureront confidentiels. Personne d'autre que nous aura accès aux enregistrements. Pour partager ces enregistrements ou vos renseignements personnels, il nous faudrait obtenir d'abord votre consentement par écrit.

    - Veuillez éteindre vos téléphones cellulaires.

    - Pour participer, assurez-vous que votre webcam et votre microphone sont activés et que vous m'entendez bien. Quand vous ne parlez pas, je vous suggère de désactiver le son afin de réduire le plus possible les bruits ambiants. N'oubliez pas d'activer le son si vous souhaitez prendre la parole.

    - Je partagerai mon écran avec vous pour vous montrer des éléments visuels.

    - Nous utiliserons fréquemment la fonction de clavardage (*chat*). Pour y accéder, veuillez

faire défiler votre écran jusqu'en bas. Vous verrez apparaître la commande « clavardage » et une fenêtre s'ouvrira à la droite de l'écran. Je vous demande d'utiliser cette fonction tout au long de la discussion. Faisons un essai rapide maintenant. Ouvrez la fenêtre de clavardage et envoyez un court message au groupe (p. ex., Bonsoir tout le monde). Si vous avez la réponse à une question qui ne vous était spécifiquement adressée, tapez votre réponse ici. Nous lirons tous vos commentaires à la fin du projet.

- Si vous n'avez pas l'occasion de vous exprimer durant la séance, vous pouvez commenter en utilisant la fonction de clavardage. La plupart du temps, discutez entre vous, à moins que vous ressentiez le besoin de m'envoyer un message en privé.

Prenons quelques minutes pour faire les présentations. J'aimerais savoir :

- Quel type d'entreprise possédez-vous, exploitez-vous ou gérez-vous?
- Quel est votre rôle au sein de l'entreprise?
  - Êtes-vous responsables des questions relatives aux TI ou à la cybersécurité?
  - Que signifie la cybersécurité pour vous?

## B. Confiance de l'entreprise envers le niveau actuel de cybersécurité (10 minutes)

Tout d'abord, combien parmi vous ont dû augmenter leur présence en ligne en raison de la pandémie ou adopter rapidement de nouvelles technologies Internet pour continuer leurs activités? **AU BESOIN :** … médias sociaux, plateformes de commerce électronique ou autres applications?

Pouvez-vous me donner des exemples des moyens qu'a pris votre entreprise pour s'adapter?

Dans l'ensemble, que pensez-vous de votre niveau de cybersécurité ces jours-ci, compte tenu des répercussions majeures de la pandémie sur l'économie numérique? Je parle ici de votre sentiment quant à la sécurité de l'ensemble de votre système des TI – y compris vos ordinateurs, vos réseaux Internet et Wi-Fi, votre système de stockage et de protection des données de votre entreprise, ainsi que toute information sur vos clients, fournisseurs, employés, etc.

- Pour m'aider à comprendre, utilisez la fonction de clavardage et répondez à la question suivante : sur une échelle de 0 à 10, où 0 signifie que vous vous sentez extrêmement vulnérable et 10, que vous vous sentez entièrement protégé, comment évaluez-vous votre niveau de cybersécurité ces jours-ci? Allez-y, écrivez dans la fenêtre de clavardage, puis nous en discuterons ensemble. **LE MODÉRATEUR NOTE LES RÉSULTATS.**
- Qu'est-ce qui vous inquiète au juste? Y a-il-place à amélioration?
- Étiez-vous au courant qu'il y avait eu augmentation du nombre de cyberattaques depuis le début de la pandémie ?

- **DANS L'AFFIRMATIVE :** Avez-vous fait quoi que ce soit pour préparer votre entreprise ?
- **SINON :** Êtes-vous étonnés d'entendre parler de l'augmentation du nombre de cyberattaques depuis le début de la pandémie ?

## C. Évaluation globale des concepts (30 minutes – Concepts A et B)

Regardons maintenant quelques concepts publicitaires.

Le gouvernement a lancé un programme de certification en cybersécurité pour les petites et moyennes entreprises. Celles qui remplissent les critères sont « certifiées » et peuvent en faire mention en affichant la marque de certification de CyberSécuritaire Canada.

Nous aimerions obtenir vos commentaires sur des concepts publicitaires destinés à une campagne nationale visant à faire connaître le programme.

Je tiens à souligner qu'il s'agit de versions provisoires des concepts. Je suis impatient d'avoir vos opinions. Ces publicités apparaitront dans la section affaire des médias nationaux publiés et enligne (p. ex. La section affaire du Globe and Mail, de La Presse, etc.), sur des sites Internet sur les TI, etc.

Je vais partager quelques images avec vous à l'écran. Vous ne devez ni les copier ni prendre de captures d'écran. Vous ne pouvez pas non plus les partager avec d'autres personnes.

***POUR USAGE INTERNE SEULEMENT :***

**LE MODÉRATEUR PRÉSENTE LES CONCEPTS (CHACUN EST IDENTIFIÉ PAR UNE LETTRE) UN PAR UN (L'ORDRE CHANGE D'UNE SÉANCE à L'AUTRE).**

**CONCEPT A = CASTORS**

**CONCEPT B = CHAINE DE CONFIANCE**

**<u>Pour chaque groupe, randomiser les concepts comme suit :</u>**
**Séance 1 : A, B**
**Séance 2 : B, A**

Pour chaque concept, je vous présenterai (dans cet ordre) :

- une animation d'une bannière publicitaire affichée dans le haut de chaque page Web que vous visitez
- une version de la même publicité telle qu'elle pourrait paraitre enligne sur des sites d'affaire comme celui du Globe and Mail, de La Presse, etc.

**LE MODÉRATEUR PRÉSENTE CHAQUE CONCEPT ET DONNE LE TEMPS AUX PARTICIPANTS DE LIRE CETTE QUESTION (autoquestionnaire)**

Veuillez considérer ce qui suit en regardant chaque publicité – vous pouvez prendre des notes, mais nous attendrons que tous aient terminé avant d'en discuter ensemble :

**LE MODÉRATEUR PRÉSENTE CE QUI SUIT À L'ÉCRAN APRÈS CHAQUE CONCEPT :**

*Quel est le but de cette publicité ?*
*Quel est le message principal ?*
*À quoi pensez-vous quand vous voyez cette publicité ?*
*Feriez-vous quoi que ce soit après l'avoir vue ?*

**UNE FOIS QUE TOUS LES PARTICIPANTS ONT TERMINÉ, COMMENCER à SONDER :**

- Que pensez-vous de la publicité ? Aidez-moi à comprendre vos réactions…
- Quelles sont vos premières impressions? Qu'est-ce que vous avez aimé du concept? Et maintenant dites-moi ce que vous avez moins aimé.

J'aimerais avoir vos opinions du concept. Nous nous pencherons sur les trois composants clés de toute publicité :

4. le **message principal**, ce qu'on essaie de vous dire
5. l'**idée créative**, comment on essaie de vous transmettre ou vous présenter le message
6. l'**appel à l'action**, ce qu'on veut que vous fassiez ou pensiez.

**QUESTIONS EXPLORATOIRES POUR LE MESSAGE PRINCIPAL**

- Quel est le principal message du concept, qu'essaie-t-on de vous dire ?
- Est-ce que le message principal est…
  - clair ? Pourquoi ou pourquoi pas ?
  - nouveau pour vous ? De quelle façon ?
  - utile ou pertinent pour vous ? Pourquoi ou pourquoi pas ?
  - persuasif ? Pourquoi ou pourquoi pas ?
  - mémorable ? Pourquoi ou pourquoi pas ?

- Était-ce clair pour vous qu'il s'agissait d'une publicité du gouvernement du Canada ?

**QUESTIONS EXPLORATOIRES POUR L'IDÉE CRÉATIVE**

- Que pensez-vous de l'idée créative envisagée pour faire passer le message ? **SONDER :**
  - Décrivez-le-moi en vos propres mots.
    - Comment décririez-vous le ton de publicité ? Positif, négatif, dynamique, réaliste ? Est-ce approprié compte tenu du message ?
    - Qu'est-ce qui vous a plu ou déplu ?
    - Qu'est-ce qui a capté votre attention : éléments visuels, texte, etc. ? Vers quoi votre regard a-t-il été attiré ?

**QUESTIONS EXPLORATOIRES POUR L'APPEL À L'ACTION**

- Qu'essaie-t-on de vous faire faire ou penser ? Le feriez-vous ? Pourquoi ou pourquoi pas ?
- Si vous alliez plus loin, sauriez-vous quelles seraient les prochaines étapes ?
- Vous rappelez-vous le nom du programme ? Quelle impression ce concept vous laisse-t-il de ce programme ? Pourquoi ?
- Visiteriez-vous le site Web après avoir vu cette publicité ? Pourquoi ou pourquoi pas ?
    - Quel site Web vous a-t-on présenté dans la publicité ?
    - Est-ce que le concept en fait suffisamment pour vous convaincre que le site Web contient de l'information utile aux propriétaires et exploitants d'entreprise comme vous ? Comment ?

**QUESTIONS EXPLORATOIRES APRÈS LA PRÉSENTATION DES DEUX CONCEPTS :**

- **LE MODÉRATEUR PRÉSENTE UN ÉCRAN CONTENANT LES DEUX CONCEPTS AVEC LES LETTRES QUI Y SONT ASSOCIÉES :** Lequel des deux concepts préférez-vous et pourquoi ? J'aimerais que vous répondiez tous à cette question. **Utilisez la fonction de clavardage et indiquez A ou B.**

- Pourrait-on faire quoi que ce soit pour améliorer la façon dont l'information est présentée dans le concept publicitaire que vous préférez ? Que suggérez-vous et pourquoi ?

- Avez-vous une chaîne d'approvisionnement ou votre entreprise livre-t-elle des biens ou des services à l'intérieur d'une chaîne d'approvisionnement?

- Où devrait-on diffuser cette publicité pour qu'elle attire votre attention ? Quelles sources consultez-vous pour obtenir de l'information pour votre entreprise ?

## F. REMERCIEMENTS ET CONCLUSION (2 minutes)

**[LE MODÉRATEUR CONSULTE L'ÉQUIPE DU CLIENT POUR VOIR SI ELLE A D'AUTRES QUESTIONS OU SI ELLE A BESOIN DE PRÉCISIONS.]**

En terminant, y a-t-il quelque chose que j'aurais dû vous demander, mais que je n'ai pas fait ?

Merci ! L'équipe qui vous a invité à participer à la séance communiquera avec vous pour obtenir des renseignements afin de vous faire parvenir l'incitatif que nous vous avons promis.

Bonne soirée à tous !

# Programme CyberSécuritaire, phase 2 : guide d'entrevue en profondeur

## A. Introduction (7 minutes)

L'intervieweur se présente : Je m'appelle [NOM DE L'INTERVIEWEUR] et je travaille pour le groupe-conseil Quorus. Nous menons une étude pour le gouvernement du Canada.

- Merci de participer à cette entrevue individuelle en profondeur de 45 minutes.

Expliquer le but de cette entrevue :

- La protection de la santé et du bien-être économique des Canadiens en période de COVID-19 est au cœur des priorités du gouvernement du Canada. Tout au long de la pandémie, la cybersécurité est devenue un enjeu de plus en plus important pour les entreprises.

- Dans un effort soutenu pour mieux comprendre les défis que doivent surmonter les entreprises de toutes tailles dans ce domaine, Innovation, Sciences et Développement économique Canada (ISDE) a fait appel au groupe-conseil Quorus, une entreprise d'études de marché à Ottawa, pour mener une étude auprès du milieu des affaires canadien.

  Nous souhaitons explorer le thème de la cybersécurité et recueillir vos réactions à un programme de cybercertification récemment mis en place par le gouvernement du Canada. Pour la discussion, veuillez garder à l'esprit que :

  - Nous recherchons la franchise et la sincérité. Les commentaires seront traités de manière confidentielle ; aucun nom, qu'il s'agisse des participants ou des entreprises/organisations qu'ils représentent ne figurera dans l'analyse ou le rapport. Les résultats seront regroupés. La séance sera enregistrée sur bande vidéo ; nous prendrons des notes pour rédiger le rapport. Des observateurs sont présents par la webconférence.

  - Le rapport sera disponible à la Bibliothèque du Parlement ou à Archives Canada.

Si vous n'avez pas d'autres questions, commençons !

### Introduction

J'aimerais tout d'abord obtenir quelques renseignements à votre sujet et au sujet de votre organisation.

- Comment décririez-vous votre organisation – quel est son objectif premier ?
- Quel est votre rôle ou votre poste ?
    - Êtes-vous responsable de quoi que ce soit qui a rapport aux TI, à la cybersécurité, la chaîne d'approvisionnement ou sa sécurité, ou aux achats ?
- Dans cette fonction, quelle est votre plus grande préoccupation ces jours-ci ? Qu'est-ce qui vous empêche de dormir la nuit ?
    - Que signifie la cybersécurité pour vous en tant que représentant de votre organisation ?

## B. Achats, chaîne d'approvisionnement, fournisseurs et cybersécurité (15 minutes)

- De façon générale, que pensez-vous du niveau de cybersécurité de votre entreprise ?
    - Que pensez-vous du niveau de cybersécurité de votre entreprise ces jours-ci, sur une échelle de 0 à 10, où 0 signifie que vous vous sentez extrêmement vulnérable et 10, entièrement protégé ? **NOTER LE RÉSULTAT.**
- Dans quelle mesure considérez-vous votre chaîne d'approvisionnement comme une source de préoccupation pour la cybersécurité de votre organisation ? Aidez-moi à comprendre.
- Selon vous, jusqu'à quel point votre chaîne d'approvisionnement et vos fournisseurs ont-ils fait preuve de résilience durant la pandémie ? De quelle manière ?
    - Est-ce que la pandémie a exposé ou introduit des vulnérabilités ou des défis en matière de cybersécurité parmi vos fournisseurs, lesquels ont eu des répercussions sur votre entreprise ?
    - Avez-vous perdu des fournisseurs durant la pandémie (p. ex., des entreprises qui ont dû fermer définitivement leurs portes) ?
- À quel point votre chaîne d'approvisionnement et vos fournisseurs étaient-ils prêts à affronter les défis liés à la cybersécurité ?
    - Avez-vous remarqué si la cybersécurité est devenue plus importante pour vos fournisseurs au cours de la dernière année ?

- Quels sont les attributs des fournisseurs ou des entreprises de votre chaîne d'approvisionnement qui obtiennent de bons résultats (**sonder :** taille de l'entreprise, expérience, connaissances) ?

- Êtes-vous préoccupé par la cybersécurité au sein de votre chaîne d'approvisionnement ? Que faites-vous pour remédier à la situation ?
- Avez-vous été forcé de modifier vos pratiques d'approvisionnement ?
- En ce qui concerne la gestion du risque, avez-vous déjà exigé un niveau de cybersécurité de vos fournisseurs ?
    - **DANS L'AFFIRMATIVE :** L'exigez-vous de tous vos fournisseurs ou seulement de certains d'entre eux ? Quels critères utilisez-vous pour déterminer ceux qui doivent avoir un niveau de cybersécurité ?
    - **SINON :** Avez-vous déjà *envisagé* de l'exiger de vos fournisseurs ?
- Exigez-vous de vos fournisseurs qu'ils démontrent ou prouvent leur niveau de cybersécurité ?
    - Est-ce facile ou difficile pour vos fournisseurs de vous fournir cette preuve ? Encore une fois, y a-t-il certains types d'entreprises qui réussissent mieux que d'autres dans ce domaine ?
    - Est-ce facile ou difficile pour votre entreprise d'évaluer si cette information lui est relayée de façon uniforme ?
    - Dans quelle mesure avez-vous confiance en vos fournisseurs et ce qu'ils vous disent ?
    - Croyez-vous que les entreprises avec lesquelles vous faites affaire devraient pouvoir démontrer leur niveau de cybersécurité ?

## C. Rôle du gouvernement en matière de cybersécurité (10 minutes)

Votre organisation utilise de petites et moyennes entreprises comme fournisseurs pour sa chaîne d'approvisionnement. Quel est le rôle que le gouvernement du Canada pourrait ou devrait jouer pour aider ces entreprises à devenir cybersécuritaires ?

**NOTE POUR L'ANIMATEUR :** S'assurer que la discussion demeure axée sur le rôle du gouvernement fédéral et non pas celui du gouvernement provincial ou de l'administration municipale.

- Que pourrait faire le gouvernement du Canada pour mieux aider les PME à améliorer le niveau de cybersécurité de votre chaîne d'approvisionnement ?

    - Peut-il faire quelque chose pour accroître la sécurité de votre chaîne d'approvisionnement ou de vos fournisseurs ?

- Le gouvernement devrait-il exiger des entreprises qu'elles prennent des mesures pour atteindre un certain niveau de cybersécurité ou qu'elles prouvent la diligence raisonnable ?
    - Selon vous, quel impact cela pourrait-il avoir sur vos opérations ?
    - Pour ce qui est de la gestion de la chaîne d'approvisionnement, est-ce que le fait de rendre obligatoire un certain niveau de cybersécurité allégerait le fardeau de la cybersécurité ou atténuerait les risques pour les organisations comme la vôtre ?
    - Si cela n'est pas obligatoire, quelles seraient les meilleures approches à utiliser pour encourager les organisations comme la vôtre et les entreprises de votre chaîne d'approvisionnement à accroître ou à améliorer leurs mesures de cybersécurité ?
- À votre avis, si vos divers fournisseurs obtenaient une cybercertification quelconque, est-ce que cela aurait un impact sur ce qui suit :
    - la confiance envers votre organisation ?
    - une protection accrue des renseignements confidentiels (dossiers des clients, données sur l'entreprise) ?
    - la protection de votre marque ?
    - une meilleure connaissance et gestion des risques ?
    - une meilleure gestion (plus sûre) de la chaîne d'approvisionnement ?
    - Quelles seraient les autres répercussions possibles d'une cybercertification de votre chaîne d'approvisionnement ?

## D. Évaluation du programme CyberSécuritaire (13 minutes)

J'aimerais vous parler du programme CyberSécuritaire du gouvernement du Canada et recueillir vos premières réactions. Ensuite, nous reviendrons sur les chaînes d'approvisionnement – plus particulièrement les petites et moyennes entreprises qui supportent votre organisation.

**L'INTERVIEWEUR LIT CE QUI SUIT :**
Le programme CyberSécuritaire Canada vise à renforcer la confiance envers l'économie numérique du Canada, au pays comme à l'étranger. Son but est d'accroître la cybersécurité de base des petites et moyennes entreprises (PME) canadiennes, de rehausser la confiance des

consommateurs envers l'économie numérique, de promouvoir la normalisation internationale et mieux positionner les PME pour leur permettre de concurrencer à l'échelle mondiale.

**L'INTERVIEWEUR PRÉSENTE LE SOMMAIRE DU PROGRAMME À L'ÉCRAN ET DONNE LE TEMPS AU PARTICIPANT DE LIRE L'INFORMATION, QUI DEMEURE À L'ÉCRAN POUR LE RESTE DE LA DISCUSSION.**

Le programme CyberSécuritaire permet aux PME de démontrer qu'elles prennent les mesures nécessaires pour protéger leurs systèmes, se mettre à l'abri des cyberattaques et protéger les renseignements concernant leurs clients et leurs fournisseurs.

Pour être admissible à la certification, l'organisation doit revoir et appliquer les 13 contrôles de sécurité établis par le **Centre canadien pour la cybersécurité** :

- Élaborer un plan d'intervention en cas d'incident
- Appliquer automatiquement les correctifs aux systèmes d'exploitation et aux applications
- Configurer les appareils de manière à les sécuriser
- Activer les logiciels de sécurité
- Utiliser une authentification forte
- Donner de la formation pour sensibiliser les employés
- Faire des copies de sauvegarde et chiffrer les données
- Sécuriser les services mobiles
- Établir un périmètre de défense de base
- Sécuriser l'environnement infonuagique et les services de TI externalisés
- Sécuriser les sites Web
- Mettre en œuvre des contrôles d'accès et autorisation
- Sécuriser les supports amovibles

Un organisme de certification (**agréé par le Conseil canadien des normes**) évaluera la mise en œuvre des 13 contrôles de sécurité. L'organisme discutera avec l'organisation pour :

- déterminer si l'organisation répond aux critères de certification ;
- donner un aperçu des coûts de la certification CyberSécuritaire ;
- évaluer la mise en œuvre des contrôles de sécurité.

Lorsqu'une entreprise obtient la certification CyberSécuritaire, elle est certifiée pour une période de deux ans et elle peut afficher la marque de certification sur son site Web, sa devanture et son matériel promotionnel.

**L'INTERVIEWEUR POURSUIT :**

- Avez-vous déjà entendu parler de cette certification ou de toutes autres certifications de cybersécurité ? Quelles sont celles dont vous avez entendu parler ?
- Que pensez-vous de ces types de programmes ?
    - Songeriez-vous à exiger de votre chaîne d'approvisionnement et de vos fournisseurs qu'ils obtiennent la cybercertification ?
        - Quels seraient les défis associés à l'obtention d'une cybercertification ?
        - Quels seraient les avantages pour votre entreprise ?
- Quelle serait la réaction de vos clients/citoyens/intervenants (selon le cas) si vos fournisseurs étaient certifiés en vertu de ce programme ? Est-ce que cette certification changerait quoi que ce soit ?
- Quelles sont vos attentes quant à l'implication du gouvernement dans ce programme ?
- Compte tenu des éléments de contrôle de sécurité sur lesquels les entreprises devraient s'attarder, avez-vous l'impression que les fournisseurs de votre chaîne d'approvisionnement ont les outils et l'expertise nécessaires pour mettre en place ces contrôles afin d'obtenir la certification ?
    - **SINON :** Qu'est-ce qui manque selon vous ?

        **EXPLORER AU BESOIN :**

        - Connaissances en matière de cybersécurité
        - Personnel des TI dédié
- Croyez-vous que vos fournisseurs devraient embaucher un consultant pour mettre en place les contrôles afin d'obtenir la certification ?
    - Sinon, croyez-vous que le gouvernement devrait proposer des solutions pour combler les lacunes ?
    - À quel point faites-vous confiance à la cybersécurité qu'offrent ces tiers ?
    - Auriez-vous davantage confiance à ces tiers s'ils étaient eux-mêmes certifiés cybersécuritaires ?
- Si les membres de votre chaîne d'approvisionnement obtenaient leur certification dans le cadre de ce programme, en quoi cela changerait-il votre sentiment de la cybersécurité de votre entreprise ? Revoyons la note que vous avez donnée au début de la discussion :

sur une échelle de 0 à 10 où 0 signifie que vous vous sentiriez extrêmement vulnérable et 10, entièrement protégé. **L'INTERVIEWEUR NOTE LE RÉSULTAT.**

### Site Web de CyberSécuritaire Canada *(si le temps le permet)*

Avant de terminer, j'aimerais prendre une minute pour regarder le site Web du programme : Canada.ca/cybersecure. **L'INTERVIEWEUR PRÉSENTE LE SITE À L'ÉCRAN.**

- Avez-vous déjà visité le site Web auparavant ?
- Quel est le principal message que vous retenez de la page Web ?
- Est-ce que le but premier du programme est clairement communiqué ?
- Compte tenu de ce que vous avez retenu de cette visite…
    - Est-ce que le site vous semble facile à comprendre ?
    - L'information est-elle bien organisée ?
    - Est-ce que vous l'exploreriez ou le présenteriez à vos fournisseurs ?
    - Y a-t-il un appel clair à l'action ?
- Ajouteriez-vous ou changeriez-vous quoi que ce soit pour que le site soit mieux adapté à vos fournisseurs ?
- Ajouteriez-vous ou changeriez-vous quoi que ce soit pour que le site soit mieux adapté aux entreprises comme la vôtre qui auraient des fournisseurs avec ce type de certification ?

## E. REMERCIEMENT ET CONCLUSION (2 minutes)

**[L'INTERVIEWEUR VÉRIFIE AUPRÈS DE L'ÉQUIPE DU CLIENT POUR SAVOIR S'IL ELLE A D'AUTRES QUESTIONS OU SI ELLE A BESOIN DE PRÉCISIONS.]**

En terminant, y a-t-il quoi que ce soit que j'aurais dû vous demander, mais que je n'ai pas fait ?

Merci ! Bonne *[journée/soirée*] !