RAPPORT DES CONSULTATIONS SUR L'EXAMEN DE LA CYBERSÉCURITÉ

PRÉPARÉ POUR SÉCURITÉ PUBLIQUE CANADA
PRÉPARÉ PAR NIELSEN

17 JANVIER 2017

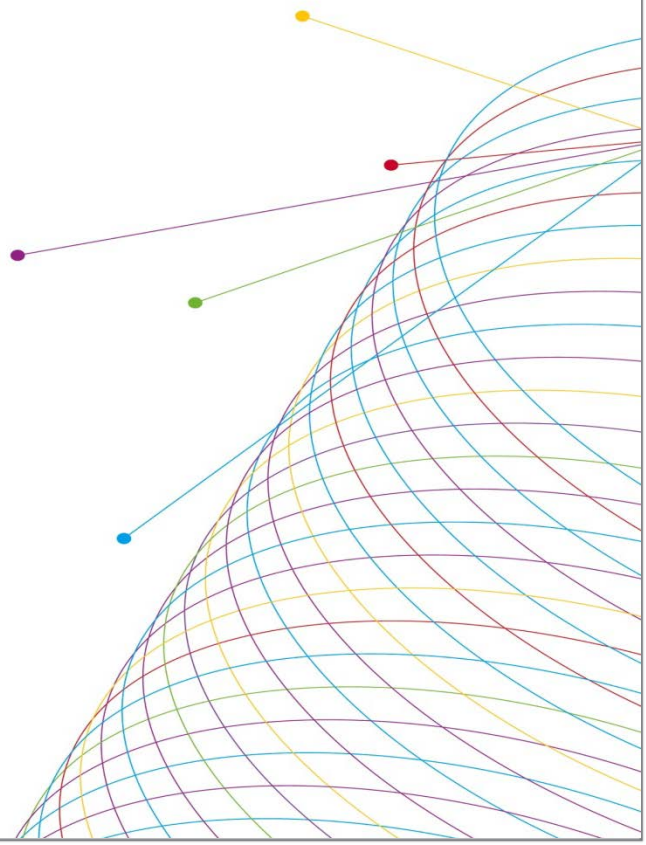


TABLE DES MATIÈRES

SOMMAIRE

Contexte et objectifs

CONTEXTE DE LA CONSULTATION

L'environnement de cybersécurité canadien est en évolution. Les changements rapides apportés à la technologie numérique ont d'importantes conséquences sociales et économiques ainsi que des répercussions sur la sécurité. Conscient que la technologie numérique joue un rôle de premier plan dans la vie quotidienne des Canadiens, le gouvernement du Canada voulait connaître leur opinion à ce sujet.

OBJECTIFS

Dans le cadre de cet examen, le gouvernement a lancé et administré un processus de consultation publique en ligne pour obtenir l'opinion des Canadiens, du secteur privé, du milieu universitaire et d'autres intervenants compétents sur le paysage de la cybersécurité au Canada. Les objectifs de cette consultation étaient les suivants :

- donner un aperçu des tendances et des défis en matière de cybersécurité;
- présenter la voie à suivre proposée pour la cybersécurité au Canada;
- obtenir des réponses aux 18 questions posées.

Méthodologie

Au total, 2 005 soumissions sur le portail Web et 90 exposés de position ont été présentés. Ensemble, ces 2 095 documents contenaient 2 399 réponses aux questions individuelles sur 4 sujets principaux, soit :

1. **l'évolution de la cybermenace :** 1 728 réponses;
2. **l'importance économique croissante de la cybersécurité :** 364 réponses;
3. **l'élargissement des frontières de la cybersécurité :** 190 réponses;
4. **les prochaines étapes relatives à la cybersécurité au Canada :** 117 réponses.

Résumé des principales constatations

La consultation publique a permis de confirmer que la cybersécurité au Canada est une question hautement complexe comportant de multiples défis et offrant un nombre croissant de possibilités. Les gouvernements, le secteur privé, les organismes d'application de la loi et le public doivent ensemble relever ces défis et saisir ces occasions.

Dans le cadre de la consultation, trois idées ont immanquablement été mentionnées comme étant importantes et applicables à la cybersécurité au Canada : **la protection de la vie privée, la collaboration et le recours à des employés qualifiés en cybersécurité.** Dans l'ensemble des sujets de consultation, les

participants ont souligné le besoin de maintenir les droits à la vie privée de tous les Canadiens, le besoin pour les intervenants de collaborer les uns avec les autres (gouvernements, secteur privé, organismes d'application de la loi, milieu universitaire, organismes sans but lucratif), et le besoin de pouvoir compter sur les spécialistes de la cybersécurité.

En plus de ces trois idées qui prévalaient dans les résultats, la consultation sur la cybersécurité du gouvernement du Canada a produit des recommandations sur des domaines d'intervention, des besoins, des moyens, des contraintes et des obstacles précis. Ces constatations sont résumées ci-après.

DOMAINES D'INTERVENTION

Des domaines d'intervention potentiels ont été cernés dans le cadre de la consultation, notamment :

- accroître la sensibilisation et l'éducation du public;
- améliorer la formation des professionnels de la cybersécurité et des organismes d'application de la loi;
- établir des normes, des pratiques exemplaires, une certification et des mesures législatives, et en faire la promotion;
- accroître le financement et les ressources pour tous les domaines de la cybersécurité.

Accroître la sensibilisation et l'éducation du public

Les participants ont indiqué que le public assume une certaine responsabilité quant à sa protection contre les cybermenaces, tout en reconnaissant que le grand public ne connaît pas bien l'importance de la cybersécurité et ne comprend pas bien les mesures de sécurité de base.

Les participants ont recommandé que l'éducation et la sensibilisation du public soient améliorées afin d'accroître la cybersécurité au Canada, d'établir une base de connaissances du XXI^{e} siècle, de renforcer la confiance des consommateurs dans le commerce électronique, et d'accroître la mobilisation du public. Les recommandations pour améliorer l'éducation du public comprenaient l'élaboration d'un programme normalisé de cybersécurité et la prestation de fonds pour les programmes d'éducation.

Améliorer la formation des professionnels de la cybersécurité et des organismes d'application de la loi

Les participants ont souligné la nécessité d'améliorer la formation en cybersécurité afin de traiter de la cybercriminalité et des cybermenaces au Canada, de promouvoir la croissance et l'innovation en matière de cybersécurité, et de protéger les infrastructures essentielles. Le renforcement de la sensibilisation et de l'éducation du public était considéré comme appuyant cet effort, surtout si les jeunes étaient sensibilisés à la cybersécurité, puisqu'il permettrait d'enrichir la base de connaissances. Les recommandations relatives à l'amélioration de la formation des professionnels de la cybersécurité comprenaient l'élaboration d'un programme de certification et le soutien de la formation.

Les organismes d'application de la loi jouent un rôle clé en matière de cybersécurité, et la consultation a révélé un certain consensus de la part des participants voulant qu'une meilleure formation de ces organismes en cybersécurité soit essentielle. Sans cette formation, l'application de la loi dans le

cyberespace ne serait pas efficace. De plus, un manque de formation spécialisée contribue aux préoccupations exprimées sur la violation des droits à la vie privée.

Normalisation, pratiques exemplaires, certification et mesures législatives

La consultation a permis de découvrir que l'élaboration de normes, des pratiques exemplaires, une certification et des mesures législatives étaient proposées pour protéger les infrastructures essentielles, prévenir les cyberattaques évoluées, améliorer la sécurité de la technologie émergente, encourager la croissance et l'innovation, et accroître la mobilisation du public.

Des mesures législatives et des normes en matière de cybersécurité ont également été mentionnées comme moyens d'encourager l'adoption de régimes améliorés de cybersécurité, y compris l'échange de renseignements, des conséquences étant prévues pour ceux qui ne s'y conforment pas.

Accroître le financement et les ressources

Un domaine d'intervention clé cerné lors de la consultation concerne le besoin d'accroître le financement et les ressources en matière de cybersécurité puisque les participants estiment généralement que le secteur de la cybersécurité souffre d'un manque de financement et d'effectifs. L'augmentation du financement et des ressources est particulièrement importante pour encourager l'adoption de mesures de sécurité plus rigoureuses (chiffrement et réseaux privés virtuels), la réalisation de vérifications et d'essais de système, et la promotion de meilleures pratiques en matière de cybersécurité.

MOYENS

La consultation a révélé des moyens potentiels supplémentaires de traiter des questions de cybersécurité au Canada, notamment :

- réaliser régulièrement des audits et des essais à l'égard des systèmes de sécurité;
- utiliser des mesures rigoureuses en matière de cybersécurité, surtout le chiffrement et les réseaux privés virtuels;
- être transparent, y compris dans le cadre de la surveillance publique;
- être proactif.

Vérifications internes et essais de système

Selon les participants, le fait de réaliser régulièrement des vérifications internes et des essais à l'égard des systèmes de sécurité aiderait à protéger les infrastructures essentielles et à prévenir les cyberattaques évoluées.

Mesures rigoureuses en matière de cybersécurité

L'application de mesures de sécurité plus rigoureuses, comme le chiffrement et les réseaux privés virtuels, des mesures fréquemment mentionnées, aiderait à protéger les systèmes contre des cybermenaces évoluées et à améliorer la sécurité de la technologie.

Transparence et surveillance publique

Afin d'apaiser les préoccupations quant à la protection de la vie privée et d'accroître la mobilisation du public, les participants ont indiqué que les organismes d'application de la loi, le gouvernement et, dans une moindre mesure, le secteur privé devaient faire preuve de davantage de transparence. Cette transparence permettrait une responsabilisation et une surveillance publique accrues. La transparence des organismes d'application de la loi pourrait également aider à améliorer les perceptions négatives quant à l'application de la loi dans le cyberespace et à accroître la confiance dans ces organismes.

Être proactif

Les participants étaient d'avis que pour améliorer la cybersécurité au Canada, appliquer efficacement la loi dans le cyberespace et protéger les systèmes contre les cybermenaces évoluées, il est nécessaire de privilégier la prévention : les mesures prises doivent être de nature proactive.

CONTRAINTES ET OBSTACLES

Les participants ont également reconnu un certain nombre d'obstacles et de contraintes touchant la cybersécurité au Canada, notamment :

- une réticence à échanger des renseignements avec le public et les concurrents;
- le manque de mesures incitatives et de répercussions pour ceux qui n'améliorent pas leur cybersécurité;
- les coûts associés au renforcement de la cybersécurité;
- le manque de confiance dans les organismes d'application de la loi;
- l'absence d'un moyen clair pour signaler les cybercrimes, les menaces, les incidents ou les attaques.

Réticence à échanger des renseignements

Même si de nombreux participants ont parlé de la nécessité d'échanger des renseignements pour améliorer la cybersécurité au Canada, la réticence à échanger des renseignements sur les vulnérabilités, les incidents et les attaques dans le cyberespace en fait un important obstacle. Il n'existe aucun accord général sur les raisons de cette réticence. Les participants ont parlé de la peur de créer davantage de vulnérabilités, de nuire à l'image de marque et à la réputation, et de donner aux autres un avantage concurrentiel.

Manque de mesures incitatives et de répercussions

Malgré le consensus quant à la nécessité d'adopter des mesures plus rigoureuses en ce qui concerne la cybersécurité, la consultation a révélé qu'il n'existait aucune mesure incitative significative (p. ex. crédits d'impôt) ou répercussion pour ceux qui ne le font pas (p. ex. poursuites). Les participants ont exigé des mesures incitatives supplémentaires et des répercussions plus importantes, ainsi qu'un financement supplémentaire (p. ex. crédit budgétaire) ou des mesures législatives, afin de surmonter cet obstacle.

Coûts

Le coût lié à l'adoption de mesures plus rigoureuses en matière de cybersécurité est un obstacle important pour les entreprises, les organisations et les particuliers. Tant que des mesures rigoureuses en matière de cybersécurité continueront d'avoir une incidence considérable sur les « résultats nets», les coûts continueront d'être un obstacle important. Cet obstacle est amplifié s'il n'existe aucune répercussion financière pour le non-respect des normes établies de cybersécurité.

Préoccupation quant à la capacité des organismes d'application de la loi

La consultation a révélé un manque de confiance envers les organismes d'application de la loi. Alors que de nombreux participants étaient compréhensifs quant aux difficultés d'appliquer la loi dans le cyberespace (p. ex. difficile de cibler un cybercriminel, complexité des administrations), il existe des perceptions selon lesquelles les employés des organismes d'application de la loi n'ont pas reçu la formation nécessaire pour enquêter sur des cybercrimes et ne parviennent pas à les prévenir et à entreprendre des poursuites. De plus, bon nombre de participants se sont dits inquiets de savoir que l'application de la loi dans le cyberespace entrave leurs droits à la vie privée, surtout en ce qui concerne la surveillance généralisée. Les participants ont mentionné l'amélioration de la formation en cybersécurité pour les employés des organismes d'application de la loi, ainsi qu'une meilleure transparence et une surveillance publique accrue.

Aucun moyen clair de signalement

Selon les participants, il n'existe aucun moyen clair de signaler les cybercrimes, les menaces, les incidents ou les attaques. Il existe un lien avec l'obstacle précédent. En ne sachant pas comment signaler un cybercrime, ni où le faire ou qui informer, il est impossible de lutter contre les menaces, les incidents et les attaques.

APERÇU GÉNÉRAL

Contexte et objectifs

CONTEXTE DE LA CONSULTATION

L'environnement de cybersécurité canadien est en évolution. Les changements rapides apportés à la technologie numérique ont d'importantes conséquences sociales et économiques ainsi que des répercussions sur la sécurité. Conscient que la technologie numérique joue un rôle de premier plan dans la vie quotidienne des Canadiens, le gouvernement du Canada voulait connaître leur opinion à ce sujet.

OBJECTIFS

Dans le cadre de cet examen, le gouvernement a lancé et administré un processus de consultation publique en ligne pour obtenir l'opinion des Canadiens, du secteur privé, du milieu universitaire et

d'autres intervenants compétents sur le paysage de la cybersécurité au Canada. Les objectifs de cette consultation étaient les suivants :

- donner un aperçu des tendances et des défis en matière de cybersécurité;
- présenter la voie à suivre proposée pour la cybersécurité au Canada;
- obtenir des réponses aux 18 questions posées.

Méthodologie

APERÇU

La participation à la consultation se faisait sur une base volontaire. Des questions étaient posées pour recueillir des renseignements seulement. Les données présentées et analysées fondées sur les réponses fournies sont agrégées ou ont été rendues anonymes. Des données brutes peuvent être diffusées en ligne, mais tous les renseignements d'identification seront supprimés avant la divulgation. Tous les renseignements recueillis seront traités conformément à la *Loi sur la protection des renseignements personnels*.

Les constatations ne sont pas statistiquement extrapolables à une population élargie et aucune estimation des erreurs d'échantillonnage ne peut être calculée.

Au total, 2 005 soumissions sur le portail Web et 90 exposés de position ont été présentés. Ensemble, ces 2 095 documents contenaient 2 399 réponses aux questions individuelles sur 4 sujets principaux, soit :

1. **l'évolution de la cybermenace :** 1 728 réponses;
2. **l'importance économique croissante de la cybersécurité :** 364 réponses;
3. **l'élargissement des frontières de la cybersécurité :** 190 réponses;
4. **les prochaines étapes relatives à la cybersécurité au Canada :** 117 réponses.

Une ventilation des réponses par région et catégorie est présentée à l'annexe A.

CONCEPTION DE LA CONSULTATION

Sécurité publique Canada a dirigé la conception des questions et celles-ci ont été présentées dans les deux langues officielles. Toutes les questions étaient des questions ouvertes, et les participants ont pu répondre à certaines ou à toutes les questions, comme ils l'entendaient.

Une liste complète des questions des sous-thèmes est présentée à l'annexe B.

ADMINISTRATION DE LA CONSULTATION

Des Canadiens et des intervenants clés en cybersécurité étaient invités à participer à la consultation volontaire du 16 août au 15 octobre 2016. Les questions étaient affichées sur le site Web du gouvernement du Canada et certains participants ont choisi de donner leurs réponses par courriel. Certains des courriels de réponses ont été reçus après la date limite du 15 octobre, mais ont été inclus dans l'analyse.

ANALYSE DES DONNÉES

Sécurité publique Canada a fourni à Nielsen les réponses à la consultation. Nielsen a combiné les données et examiné le fichier pour s'assurer que toutes les données reçues étaient valides.

L'équipe de codage de Nielsen a lu chacune des réponses et les a classées sous des thèmes communs, attribuant un code précis à chaque réponse afin qu'elle soit analysée sous forme agrégée. L'équipe de Nielsen a lu tous les commentaires et s'est assurée que tous les codes avaient été attribués correctement. Nielsen a ensuite comparé les résultats qualitatifs en se fondant sur la catégorie de participants.

Les quatre types de participants examinés de plus près dans le présent rapport sont les suivants : les citoyens mobilisés, le gouvernement, l'industrie de la cybersécurité et les autres industries (p. ex. application de la loi, finances, santé). Les participants d'autres catégories (milieu universitaire et étudiants) ont été représentés dans les résultats globaux, mais n'ont pas été représentés seuls en raison du nombre limité de participants (surtout du milieu universitaire) ou du manque de cohérence et de clarté des réponses (surtout des étudiants). Aussi, certains participants ont choisi de demeurer anonymes.

Des efforts ont été déployés pour analyser les données selon la région du participant, mais l'analyse a révélé que les participants n'étaient pas répartis également dans l'ensemble du Canada. Ainsi, les différences étaient davantage déterminées par la catégorie du participant et non en réalité par leur lieu de résidence.

Notes importantes concernant le processus de consultation

La décision de mener une consultation publique en ligne a maximisé la possibilité pour les Canadiens du pays d'y participer. Certaines répercussions inhérentes aux consultations publiques en ligne devraient être prises en considération lors de la lecture du présent rapport.

- Bien que les données aient été examinées pour détecter les soumissions multiples de la part d'une même personne, il est tout de même possible que les données comprennent des réponses multiples provenant du même participant.
- Certaines soumissions reçues représentent la rétroaction collective d'un groupe de personnes (p. ex. soumission d'une association professionnelle).
- Puisqu'aucun contingent n'a été établi pour équilibrer la composition de l'échantillon, et que les participants ont choisi de formuler leur opinion en se fondant sur leur niveau de sensibilisation, de mobilisation et d'intérêt personnel, les résultats ne peuvent pas être interprétés comme étant représentatifs de la population canadienne.
- Aucune marge d'erreur d'échantillonnage ou inférence statistique ne peut être calculée relativement aux données de cette consultation publique.
- Le questionnaire ne comprenait que des questions ouvertes dans le cadre desquelles les participants pouvaient exprimer leur opinion. Par conséquent, bon nombre des réponses fournies ne traitent pas directement du sujet présenté dans chaque question.

    - La consultation n’a offert aucune question de suivi ou moyen pour savoir ce que les participants pensaient des idées ou des suggestions supplémentaires. Ainsi, la profondeur des renseignements recueillis est parfois limitée.
- De nombreuses questions offraient des exemples de réponses possibles afin de clarifier la question. Même si cette façon de faire servait un objectif important étant donné l’encadrement limité offert aux participants, elle crée aussi certaines tendances relativement aux réponses en orientant potentiellement les participants.

En tenant compte de cette information, le lecteur du présent rapport devrait prendre note de ce qui suit :

- des mots de classement (p. ex. tous, certains, peu, première réponse) ont été utilisés pour montrer l’importance des opinions reçues, mais ne devraient pas être interprétés comme étant représentatifs de la population totale;
- les réponses ont été présentées par thème et pas nécessairement par question;
- le rapport comprend certaines réponses mot à mot pour souligner la nature qualitative de la recherche et qui ont été sélectionnées pour fournir un contexte supplémentaire;
- les participants semblaient utiliser les termes « secteur public » et « gouvernement » indistinctement. Puisque la consultation n’offrait pas la possibilité de demander des précisions, il est difficile de savoir avec certitude si un participant faisait référence au gouvernement alors qu’il parlait du secteur public, bien que cela semble le cas dans de nombreuses occasions;
    - de même, il est difficile de déterminer si les participants font référence au gouvernement du Canada, surtout lorsqu’ils disaient « gouvernement », et peu d’entre eux ont carrément mentionné le gouvernement du Canada;
- la collaboration avec les « partenaires stratégiques » était un thème commun dans l’ensemble de la consultation. Cependant, les partenaires précis mentionnés par les participants variaient souvent et comprenaient les organismes sans but lucratif, les organismes privés, d’autres pays, d’autres ministères et le milieu universitaire.

Avis de non-responsabilité

Cette analyse des résultats de la consultation en ligne a été menée par Nielsen Canada. Elle avait pour but d’aider Sécurité publique Canada à mieux comprendre les opinions des participants. Bien que la préparation du présent rapport et le résumé des constatations aient été faits avec le plus grand soin, le rapport ne présente qu’un examen subjectif des réponses. Les participants ont répondu aux questions sur une base volontaire, les réponses pourraient avoir été incomplètes, et l’interprétation des réponses peut varier. Nielsen a expressément établi un avis de non-responsabilité pour tout dommage découlant de l’utilisation du matériel contenu dans ce résumé.

CONCLUSIONS DÉTAILLÉES

Les conclusions du présent rapport ont été organisées par tendance conformément à la méthode selon laquelle les réponses ont été recueillies auprès des participants. Comme mentionné, les quatre tendances sont les suivantes : l'évolution de la cybermenace, l'importance économique croissante de la cybersécurité, l'élargissement des frontières de la cybersécurité, et les prochaines étapes relatives à la cybersécurité au Canada. Chacune de ces tendances a été présentée au moyen du même contenu fourni dans le cahier de travail des participants afin de bien faire comprendre le sujet avant de dévoiler les conclusions de la consultation.

Lorsqu'il y avait une divergence d'opinions selon le type de participant au cours de la consultation (citoyens mobilisés, gouvernement, industrie de la cybersécurité et autres industries), ces différences ont été soulignées. Lorsque le rapport n'en fait pas clairement mention, aucune différence importante n'était évidente, pouvant ainsi suggérer un certain consensus.

ÉVOLUTION DE LA CYBERMENACE

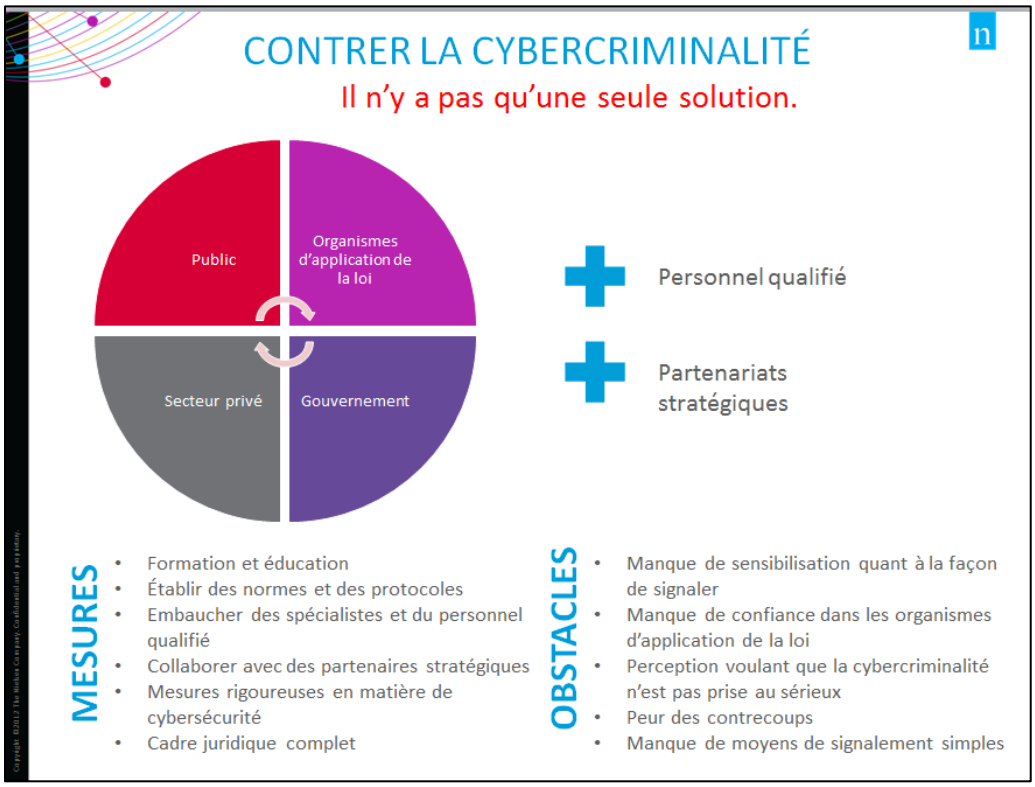
La croissance d'Internet et des réseaux numériques et l'utilisation accrue des appareils mobiles par les particuliers, les gouvernements et les entreprises ont donné lieu à la prolifération d'un certain nombre de menaces émanant du cyberespace. Les cybercapacités qui étaient autrefois rares et dispendieuses sont devenues chose courante et abordable. Les États-nations cherchent donc à établir leur présence dans le domaine cybernétique. Certains acteurs non étatiques acquièrent aussi des cybercapacités, et bien qu'ils n'aient bien souvent ni les ressources ni le niveau de sophistication des États-nations, ils peuvent tout de même être efficaces lorsqu'ils mènent des cyberactivités malveillantes et commettent des cybercrimes. Pour compliquer encore davantage les choses, contrairement à ce qui se produit dans le monde réel, il est difficile de cerner l'origine et le but d'une cyberattaque. Ces facteurs contribuent à une cybermenace grandissante à l'endroit du Canada.

Contrer la cybercriminalité

Le cahier de travail expliquait aux participants comment la cybercriminalité entre dans deux catégories : les activités criminelles traditionnelles qui utilisent la technologie comme outil et la cybercriminalité qui cible la technologie elle-même. Il précisait que la cybercriminalité est transnationale et que sa lutte nécessite une importante collaboration entre les frontières. Il résumait également les défis auxquels font face les organismes d'application de la loi, comme la fréquence accélérée des incidents, la complexité de la technologie, et le besoin grandissant d'obtenir des éléments de preuve numériques intelligibles.

On a demandé aux participants comment les organismes d'application de la loi pouvaient mieux s'attaquer aux défis que représente la cybercriminalité, comment les secteurs public et privé peuvent se protéger contre la cybercriminalité, et quels éléments (s'il y a lieu) font obstacle au signalement des cybercrimes auprès des organismes d'application de la loi.

Dans le cadre de ce thème, on a découvert que la cybercriminalité est un défi complexe qui ne peut pas être surmonté par une seule solution ou partie. Le public, les gouvernements, le secteur privé, les organismes d'application de la loi, le personnel qualifié et les partenaires stratégiques doivent tous jouer un rôle.



MESURES D'INTERVENTION

Les recommandations formulées par les participants dans cette partie de la consultation étaient les suivantes :

- améliorer la formation et l'éducation (pour les organismes de l'application de la loi, le personnel de la cybersécurité et le public);
- établir des normes, des protocoles et des pratiques exemplaires, autant pour les entreprises que pour les particuliers, qui sont clairs et faciles à suivre;
- avoir recours à des spécialistes et à du personnel qualifié;
- collaborer avec des partenaires stratégiques;
- utiliser des mesures plus rigoureuses en matière de cybersécurité (p. ex. chiffrement, réseau privé virtuel, pas de clés USB);
- élaborer un cadre juridique dans le contexte duquel les organismes d'application de la loi peuvent assumer leurs fonctions.

Comme les sections suivantes le montreront, ces recommandations ne s'appliquent pas à chaque groupe d'intervenants en cybersécurité (soit les organismes d'application de la loi, le gouvernement, le secteur privé et le public).

RÔLE DES ORGANISMES D'APPLICATION DE LA LOI

On a demandé aux participants comment les organismes d'application de la loi pouvaient relever plus efficacement le défi grandissant de la cybercriminalité. Selon eux, une collaboration avec des partenaires stratégiques est nécessaire.

« Le type de ressources humaines et techniques nécessaires pour intervenir et appliquer la loi dans le cyberespace ne peut pas être le même dans le monde réel. » [traduction]

Un grand nombre de participants ont mentionné la nécessité d'offrir une formation supplémentaire, en plus d'embaucher du personnel qualifié et des spécialistes de la cybersécurité, ce qui suggère que de nombreux participants ne croient pas que les organismes d'application de la loi possèdent actuellement la capacité de diriger dans ce domaine.

En ce qui concerne les organismes d'application de la loi, de nombreux participants se sont dits inquiets de la protection de leur vie privée et de la façon dont les mesures pour lutter contre la cybercriminalité (p. ex. la surveillance) pourraient miner ces droits. Bon nombre de participants estimaient qu'il devait y avoir une plus grande transparence et une sensibilisation accrue du public.

Certains participants ont demandé davantage de financement, l'adoption d'une meilleure technologie et le renforcement des capacités des organismes d'application de la loi.

« Nous mettons l'accent sur la prévention en raison des difficultés d'intervention à l'égard de la cybercriminalité. » [traduction]

De plus, les participants estimaient qu'il était important de mettre l'accent sur des mesures proactives et préventives.

RÔLE DU GOUVERNEMENT

« Le gouvernement du Canada peut assurer un leadership essentiel en créant, en adoptant et en modélisant des pratiques exemplaires en matière de cybersécurité, et en déployant des efforts pour transférer ce savoir vers le secteur privé. » [traduction]

Un grand nombre de participants estimaient que le gouvernement devait assurer l'échange de renseignements entre les différents organismes et travailler avec le secteur privé et d'autres partenaires stratégiques (p. ex. autres États-nations, organismes sans but lucratif, milieu universitaire).

De nombreux participants ont parlé de la nécessité d'accroître le financement et les ressources alloués aux efforts de lutte contre la cybercriminalité (p. ex. crédit budgétaire). Ils ont également suggéré que le gouvernement offre des mesures incitatives et des crédits d'impôt pour favoriser les pratiques exemplaires, surtout dans le secteur privé.

Bon nombre de participants ont également dit que le gouvernement doit embaucher du personnel qualifié et appliquer des mesures rigoureuses en matière de cybersécurité (p. ex. chiffrement, réseaux privés virtuels).

Selon certains participants, le gouvernement devrait démontrer davantage de leadership dans la lutte contre la cybercriminalité, alors que d'autres estimaient qu'il ne devrait qu'appuyer les efforts déployés en ce sens. Selon quelques participants, le gouvernement ne devrait pas y participer du tout.

Quelques participants estimaient que le gouvernement devait mettre à jour les mesures législatives actuelles concernant la cybercriminalité et la cybersécurité, ainsi que concevoir un cadre juridique sur la cybercriminalité. La plupart des participants qui ont indiqué la nécessité d'établir des mesures législatives et des cadres juridiques n'ont pas fourni de détails concernant leurs suggestions.

RÔLE DU SECTEUR PRIVÉ

De l'avis général, le secteur privé ne prend pas au sérieux la menace de la cybercriminalité en raison, du moins en partie, de l'incidence négative perçue sur leurs « résultats nets ».

De nombreux participants ont indiqué que le secteur privé devrait collaborer avec le gouvernement ainsi que d'autres partenaires stratégiques. Encore une fois, ils ont dit que le secteur privé devait embaucher du personnel qualifié pour gérer et appliquer des mesures rigoureuses en matière de cybersécurité.

Bon nombre d'entre eux ont mentionné que les entreprises doivent être tenues responsables lorsqu'elles ne protègent pas les données recueillies auprès du public.

FAÇONS DE SE PROTÉGER CONTRE LES CYBERMENACES

Les participants ont indiqué que le gouvernement et le secteur privé pouvaient se protéger contre la cybercriminalité de façons précises, notamment en adoptant des mesures de sécurité plus rigoureuses (p. ex. chiffrement, réseaux privés virtuels), en augmentant la surveillance de leurs systèmes, en menant des audits de système, et en corrigeant constamment leurs systèmes.

RÔLE DU PUBLIC

Alors que le rôle du public n'était pas au premier rang des réponses dans cette partie de la consultation, de nombreux participants ont indiqué que le public partage la responsabilité de la lutte contre la cybercriminalité, notamment en se tenant informé du sérieux de la cybersécurité et en étant sensibilisé à la façon de se protéger contre les cybermenaces. Cela comprend également le rôle du public de faire preuve de vigilance et de bon sens dans le cadre de l'utilisation de la technologie.

Certains participants ont expressément dit qu'il incombe à tous les membres du public de se protéger contre les cybermenaces.

OBSTACLES AU SIGNALEMENT

Lorsqu'on a demandé aux participants de préciser les obstacles possibles au signalement des cybercrimes, ils ont d'abord parlé du manque de sensibilisation quant à la façon de signaler, à l'endroit où le faire et à la personne à informer. Bon nombre d'entre eux ont souligné l'absence d'un moyen simple de signalement.

De nombreux participants ont perçu des lacunes dans la façon dont les organismes d'application de la loi traitent de la cybercriminalité, et estimaient que ces organismes ne prennent pas la cybercriminalité au sérieux. Ils ont aussi mentionné les faibles taux de condamnation pour les crimes commis dans le cyberespace. Certains participants étaient compréhensifs quant aux difficultés auxquelles font face les organismes d'application de la loi dans leurs enquêtes sur les cybercrimes (p. ex. difficulté à déterminer le lieu du crime et l'identité des cybercriminels, manque de formation spéciale), tout en croyant également qu'il y a peu de condamnations.

Certains croyaient que l'atteinte potentielle à la réputation et à la marque était au cœur des obstacles au signalement, en plus de la peur des obligations. Les participants de l'industrie de la cybersécurité étaient plus susceptibles de considérer ces éléments comme des obstacles.

Des participants des autres industries étaient moins susceptibles de nommer la peur des obligations, la honte, l'embarras et l'atteinte à la réputation comme obstacles, mais étaient plus susceptibles de dire que le manque de mesures législatives et de règlements exigeant le signalement était un obstacle.

Quelques participants ont dit qu'il n'existait actuellement aucun obstacle au signalement.

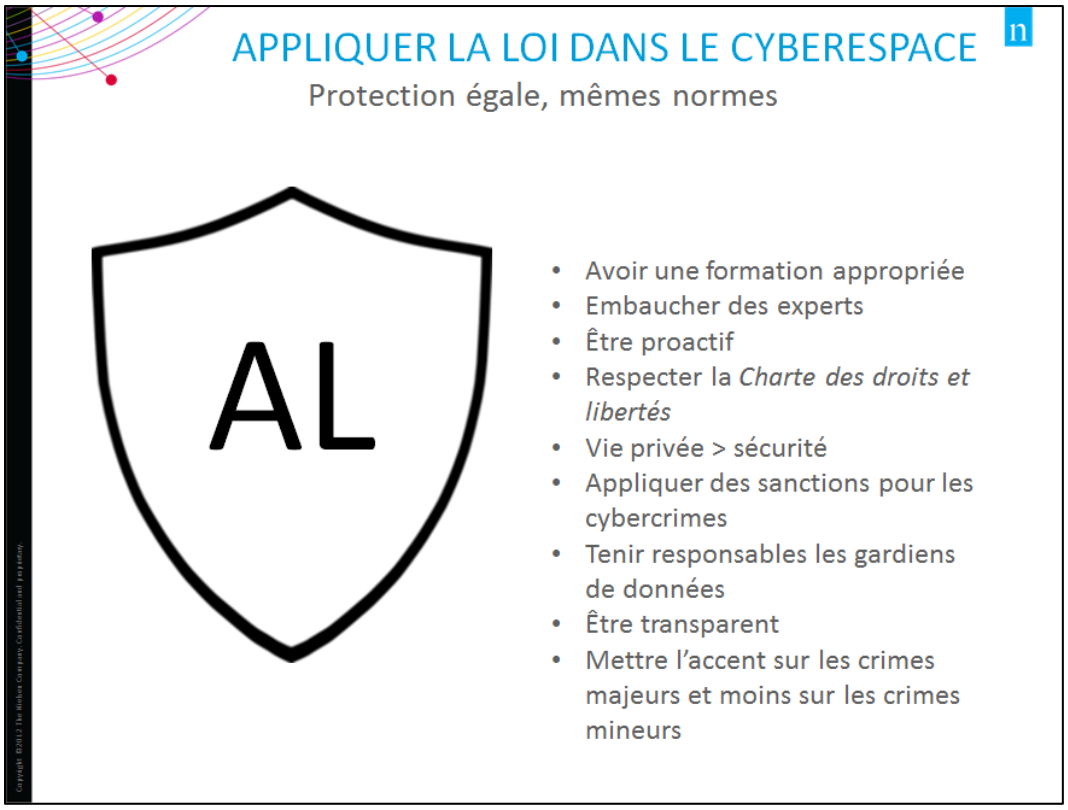
Appliquer la loi dans le cyberespace

Les questions pour les participants concernant l'application de la loi dans le cyberespace ont été précédées d'une description du paysage actuel et des défis auxquels les organismes d'application de la loi doivent faire face. Cette description confirmait que la police au Canada a pour mandat d'enquêter sur les activités criminelles dans les mondes virtuel et réel et reconnaissait que les attentes des organismes d'application de la loi dans le cyberespace ne sont pas bien comprises ni acceptées par les Canadiens. Le cahier de travail indiquait que l'efficacité des outils d'application de la loi et des autorités policières actuels est remise en question en raison des avancées technologiques, ainsi que des changements touchant les lois et les décisions judiciaires. À leur tour, les mêmes facteurs façonnent les attentes des Canadiens quant à la façon dont la police devrait travailler dans un monde virtuel.

On a demandé aux participants de formuler leurs attentes en ce qui concerne l'application de la loi dans le cyberespace et d'expliquer comment elles sont différentes de celles relatives à l'application de la loi dans le monde réel. On leur a également demandé comment contrer la cybercriminalité tout en respectant les droits des Canadiens relatifs à la protection de la vie privée et en protégeant la sécurité du public.

« En principe, mes attentes sont les mêmes. Si un crime est commis, je m'attends à ce qu'il fasse l'objet d'une enquête. » [traduction]

Dans l'ensemble, les participants étaient d'avis que l'application de la loi dans le cyberespace devait fournir une protection égale, tout en maintenant les mêmes normes, que dans le monde réel.



ATTENTES DES PARTICIPANTS À L'ÉGARD DES ORGANISMES D'APPLICATION DE LA LOI

Bon nombre de participants étaient d'accord pour dire que la cybercriminalité ne devrait pas être traitée différemment que la criminalité dans le monde réel. Ils sont également d'avis que les organismes d'application de la loi doivent respecter les mêmes normes autant lors d'enquêtes sur des cybercrimes que sur des crimes traditionnels, notamment en obtenant les mandats nécessaires, en n'enquêtant pas sur des personnes sans raison valable, et en maintenant le principe de présomption d'innocence.

« Cela signifie ne pas fouiller une propriété privée (téléphones et ordinateurs) sans mandat. Les policiers et les agents des services frontaliers ne peuvent pas demander des mots de passe ni menacer une personne de la faire arrêter. » [traduction]

Selon de nombreux participants, les droits à la vie privée des Canadiens qui sont protégés en vertu de la *Charte canadienne des droits et libertés* doivent être maintenus par les organismes d'application de la loi en tout temps. Un grand nombre de participants s'inquiètent du fait que ces droits pourraient être enfreints par certaines méthodes d'application de la loi dans le cyberespace (p. ex. surveillance). Cette

préoccupation a probablement amené certains participants à citer le besoin accru de transparence et de surveillance publique à l'égard des organismes d'application de la loi.

De nombreux participants étaient d'avis qu'il est beaucoup plus difficile de lutter contre la cybercriminalité que de lutter contre les autres crimes. Ils ont mentionné que la cybercriminalité n'avait pas de frontières, qu'elle ne se produit pas nécessairement à partir du Canada, et que les cybercriminels sont beaucoup plus difficiles à identifier. Le gouvernement et les membres de l'industrie de la cybersécurité étaient plus susceptibles de partager cette idée.

Les participants ont également mentionné la nécessité d'établir des niveaux appropriés et accrus de financement et de ressources afin de permettre aux organismes d'application de la loi de lutter contre la cybercriminalité. Bon nombre d'entre eux ont indiqué que ces ressources devraient être utilisées pour embaucher des experts dans le domaine, ou qu'une collaboration avec des partenaires stratégiques était nécessaire. Même si certains croient que ces experts ou partenaires devraient être des civils, d'autres ont indiqué que les agents actuels devraient être formés en matière de lutte contre la cybercriminalité.

De nombreux participants estimaient que les organismes d'application de la loi devaient être proactifs et accroître leur présence en ligne.

Pour certains participants, les attentes quant à la capacité des organismes d'application de la loi de lutter contre la cybercriminalité étaient faibles en raison de la perception voulant que la plupart des cybercrimes soient rarement sanctionnés.

« Pour appliquer la loi dans le cyberespace, il n'est pas nécessaire d'installer des logiciels anti-intrusion de qualité militaire à l'échelle des fournisseurs et des niveaux inférieurs pour surveiller l'utilisation de mots-clés subjectivement "suspects" dans l'ensemble de la population. De telles tactiques se fondent sur une science de pacotille. Il faut plutôt disposer d'un organisme d'application de la loi véritablement informé qui sait comment déployer des outils ciblés avec raffinement et furtivité afin de procéder à une arrestation. » [traduction]

Quelques participants ont suggéré que le cadre juridique du Canada soit mis à jour afin d'assurer une lutte plus efficace contre la cybercriminalité.

Quelques participants des autres industries estimaient que les organismes d'application de la loi devaient faire preuve d'une plus grande rigueur (p. ex. recours à des enquêteurs qualifiés et à des méthodes spécialisées) pour enquêter sur les cas de cybercriminalité.

GÉRER LA SÉCURITÉ ET LA VIE PRIVÉE

De nombreux participants, surtout les citoyens mobilisés et les membres de l'industrie de la cybersécurité, ont expressément dit que la protection de la vie privée devait l'emporter sur la sécurité. Ces participants se sont dits grandement inquiets que la surveillance démesurée exercée par les organismes d'application de la loi violait les droits à la vie privée des Canadiens. Bon nombre de participants ont indiqué qu'il était nécessaire que les organismes d'application de la loi augmentent l'imputabilité, la transparence et la surveillance.

Les participants du gouvernement étaient moins susceptibles d'exprimer les mêmes préoccupations quant à la protection de la vie privée, mais étaient plutôt susceptibles de citer la nécessité d'établir des cadres juridiques pour maintenir les droits à la vie privée et poursuivre les cybercriminels.

De nombreux participants estimaient que les sanctions à l'égard des cybercriminels doivent être renforcées et que les gardiens des données (p. ex. entreprises) doivent être tenus responsables lorsqu'ils ne protègent pas ces renseignements. Les citoyens mobilisés étaient plus susceptibles de soulever cette idée.

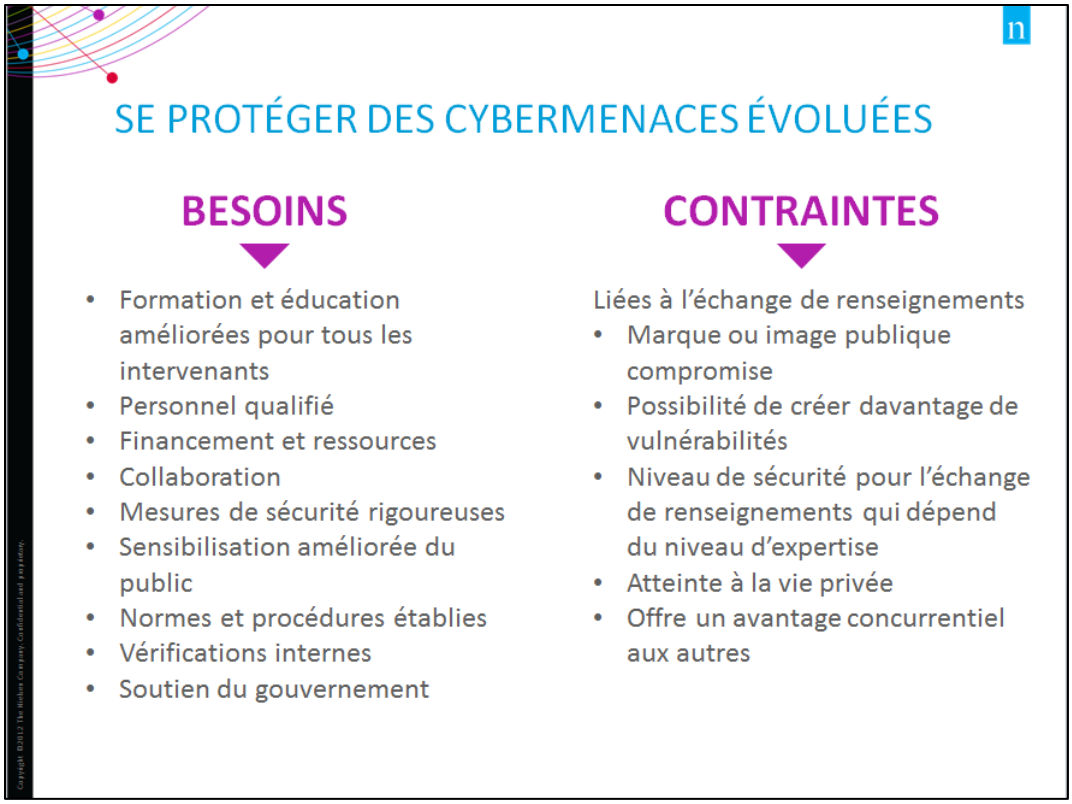
« La vie privée et la sécurité ne sont pas un jeu à somme nulle et nous pouvons avoir les deux. Il n'y a aucune sécurité sans la protection de la vie privée. Et la liberté exige la sécurité et la protection de la vie privée. La célèbre citation attribuée à Benjamin Franklin dit ceci : "Ceux qui sont prêts à renoncer à une liberté fondamentale pour obtenir temporairement un peu de sécurité ne méritent ni la liberté ni la sécurité." C'est également vrai que ceux qui renonceraient à leur vie privée pour assurer leur sécurité sont susceptibles de n'obtenir ni l'une ni l'autre. » [traduction]

Les participants ont également fréquemment mentionné que la sécurité et la vie privée pourraient être gérées au moyen de mesures de sécurité plus rigoureuses, comme le chiffrement et les réseaux privés virtuels.

Se protéger des cybermenaces évoluées

Le sujet de la consultation a été présenté aux participants par le biais d'un énoncé indiquant que les institutions publiques et les entreprises canadiennes étaient la cible de cyberattaques incessantes, bien financées et perfectionnées, autant par les entités étatiques que par les entités non étatiques. Les pays font de l'espionnage pour obtenir des renseignements en vue d'entreprendre des négociations, d'élaborer des plans militaires, de protéger la propriété intellectuelle et de créer des stratégies opérationnelles pour leur propre avantage concurrentiel. Ils élaborent également des cyberoutils pour menacer les systèmes informatiques qui contrôlent les infrastructures essentielles, une cible fréquente pour les acteurs non étatiques également.

On a également demandé aux participants de préciser les mesures nécessaires pour se protéger contre les cybermenaces évoluées et les possibles contraintes en matière d'échange de renseignements.



BESOINS EN MATIÈRE DE PROTECTION

« Nous avons besoin de personnes qui seront formées pour devenir des spécialistes de la prestation de formation en cyberdéfense, et les industries doivent prendre cet effort au sérieux. » [traduction]

La nécessité d'offrir une meilleure formation, aux organismes d'application de la loi et au personnel des technologies de l'information en particulier, est l'une des principales réponses données par les participants. La nécessité d'embaucher du personnel qualifié ou de consulter des experts de la cybersécurité au besoin a également été fréquemment mentionnée par les participants.

Les participants ont également précisé les mesures suivantes pour se protéger contre les cybermenaces évoluées :

- accroître le financement et les ressources;
- collaborer avec des partenaires stratégiques;
- appliquer des mesures de sécurité rigoureuses;
- établir des normes et des procédures;
- améliorer l'éducation et la sensibilisation du public;
- mener des vérifications internes et des tests de sécurité;
- accroître le soutien du gouvernement.

Les participants du gouvernement étaient plus susceptibles de recommander l'augmentation du financement, des ressources et de la sensibilisation du public, l'amélioration de la formation,

l'amélioration et l'uniformité des corrections des systèmes, l'uniformité et le renforcement de la surveillance, ainsi que la proactivité et l'appui de la gestion du risque.

Les participants de l'industrie de la cybersécurité étaient beaucoup plus susceptibles d'indiquer la nécessité de collaborer avec des partenaires stratégiques et d'augmenter le nombre de vérifications internes et de tests de sécurité.

CONTRAINTES EN MATIÈRE D'ÉCHANGE DE RENSEIGNEMENTS

Selon les participants, l'échange de renseignements est de la plus grande importance. Pourtant, bon nombre de participants ont également mentionné que la marque ou l'image publique pouvait être compromise, que l'échange de renseignements pouvait créer de nouvelles vulnérabilités, que la sécurité de l'échange de renseignements dépendait du niveau de formation des personnes effectuant l'échange, et que l'échange de renseignements donnait un avantage concurrentiel aux autres.

« Embarras, atteinte à la réputation et incidence sur les résultats. J'échange souvent avec mes amis et collègues dans l'ensemble du pays parce que nous nous connaissons et que nous avons établi un niveau de confiance. Ils m'aident et je les aide. Nous veillons les uns sur les autres. Lorsque cette notion atteint les présidents de ce monde, ils sont fermés comme des huîtres par peur de perdre leur avantage concurrentiel. » [traduction]

Certains participants se sont dits inquiets de la violation de leurs droits à la vie privée dans le cadre de l'échange de renseignements.

Les participants ont également fourni les réponses suivantes :

- les renseignements ne devraient pas être communiqués sans respecter les règlements et les lois applicables;
- l'importance de corriger les vulnérabilités;
- la peur des responsabilités et des répercussions juridiques;
- il faut retarder la diffusion des renseignements jusqu'à ce qu'une solution soit en place;
- l'importance des mesures législatives et de leur application;
- l'échange est compromis par le souci du profit;
- l'échange est compromis par une capacité insuffisante;
- seuls les renseignements non sensibles devraient être échangés;
- la peur d'avoir honte et d'être embarrassé.

Quelques participants n'ont constaté aucune contrainte quant à l'échange de renseignements.

Les participants du gouvernement étaient plus susceptibles de dire que la compromission potentielle de la marque et l'ébranlement de la confiance du public étaient des obstacles, tout comme la perte de bénéfices.

Les participants de l'industrie de la cybersécurité étaient plus susceptibles de suggérer que l'échange de renseignements donne aux autres un avantage concurrentiel et de considérer la perte de bénéfices, la

compromission de la marque et l'ébranlement de la confiance du public comme des obstacles. Ils étaient moins susceptibles de dire que l'échange de renseignements crée davantage de vulnérabilités.

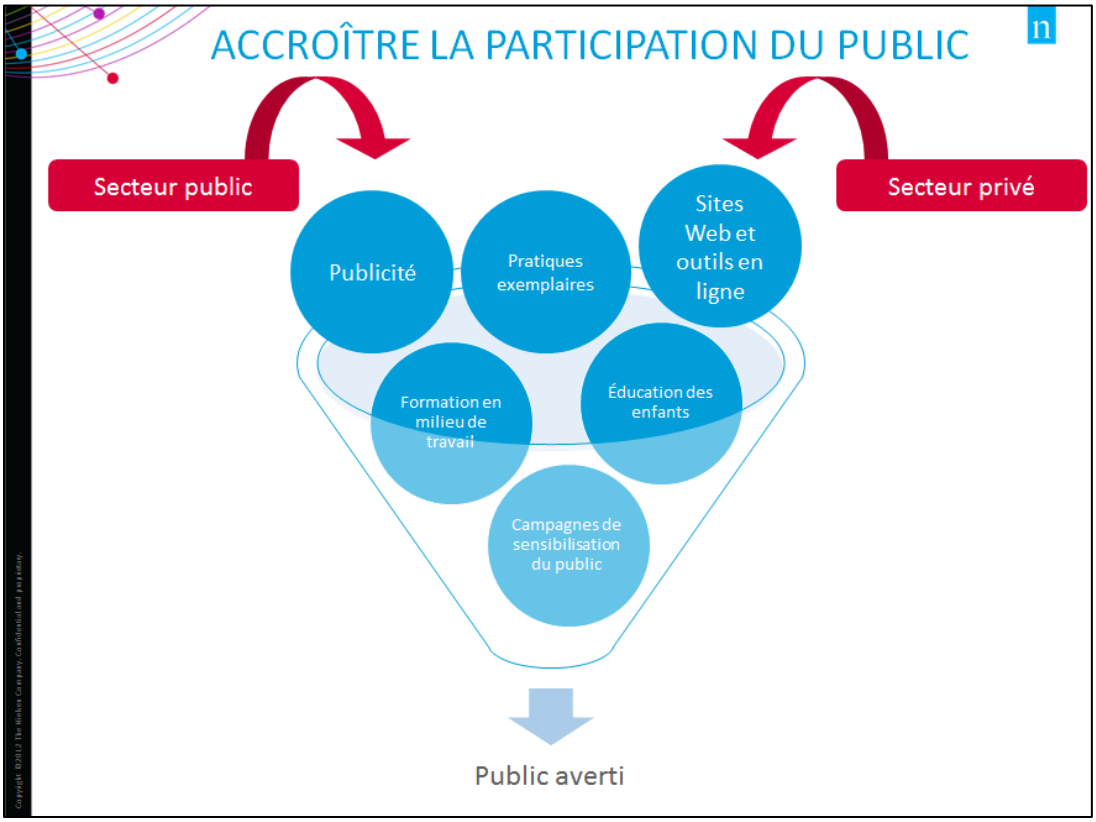
Les participants des autres industries étaient aussi moins susceptibles de citer une hausse des vulnérabilités découlant de l'échange de renseignements. Cependant, ils étaient plus susceptibles de croire que la sécurité de l'échange de renseignements dépend du niveau de formation et d'expertise d'une personne et de suggérer que cet échange donne aux autres un avantage concurrentiel.

Les citoyens mobilisés étaient plus susceptibles de dire que l'échange de renseignements pouvait enfreindre les droits à la vie privée et que toute intervention devrait être faite conformément à ces droits.

Accroître la participation du public

La préface aux questions posées aux participants sur l'augmentation de la participation du public énonce clairement que les Canadiens doivent savoir comment se protéger contre les cybermenaces et qu'un engagement approfondi en matière de cybersécurité est nécessaire de la part de toutes les couches de la société.

On a ensuite demandé aux participants comment les particuliers peuvent être mieux informés sur la façon de reconnaître un cybercrime et d'intervenir, et de quelles façons les secteurs public et privé peuvent accroître la sensibilisation du public quant aux questions de cybersécurité.



TRAVAILLER ENSEMBLE POUR ACCROÎTRE LA SENSIBILISATION ET INFORMER LE GRAND PUBLIC

Pour mobiliser le public, et au bout du compte accroître la sensibilisation et l'éducation à l'égard des questions de cybersécurité, les participants ont suggéré que le gouvernement et le secteur privé adoptent les stratégies suivantes :

- lancer des campagnes de sensibilisation pour le public;
- offrir une formation en milieu de travail;
- créer des publicités traditionnelles et dans les médias sociaux;
- élaborer et fournir des outils et des ressources en ligne;
- commencer par informer les enfants dans le système scolaire public;
- élaborer des pratiques exemplaires (claires et unifiées) et en faire la promotion;
- tenir des séances d'information et des ateliers;
- collaborer avec des partenaires stratégiques.

Bon nombre de participants estimaient que les membres du public devaient assumer un certain niveau de responsabilité pour s'assurer qu'ils sont bien informés, et certains ont mentionné que les utilisateurs des technologies numériques devaient faire preuve de bon sens.

Plutôt que de favoriser la mobilisation du public, certains participants croient que le secteur privé et le gouvernement devraient être le seul axe d'amélioration de la cybersécurité.

Les participants du gouvernement étaient plus susceptibles de suggérer l'utilisation de campagnes de sensibilisation du public et de reconnaître la nécessité de mettre à la disposition du public des renseignements clairs et concis. Les participants du gouvernement étaient moins susceptibles de suggérer l'utilisation de publicités ou la nécessité d'élaborer des pratiques exemplaires et d'en faire la promotion.

Les participants des autres industries étaient plus susceptibles de citer la nécessité d'élaborer des pratiques exemplaires et de suggérer l'utilisation de publicités pour informer le public. Les citoyens mobilisés étaient également plus susceptibles de suggérer l'utilisation de publicités.

Les participants de l'industrie de la cybersécurité étaient plus susceptibles de suggérer le renforcement de la mobilisation du gouvernement et la concentration des efforts sur le secteur privé (y compris la réalisation d'un plus grand nombre d'essais des systèmes). De même, les citoyens mobilisés étaient aussi plus susceptibles de mettre l'accent sur le secteur privé.

IMPORTANCE ÉCONOMIQUE CROISSANTE DE LA CYBERSÉCURITÉ

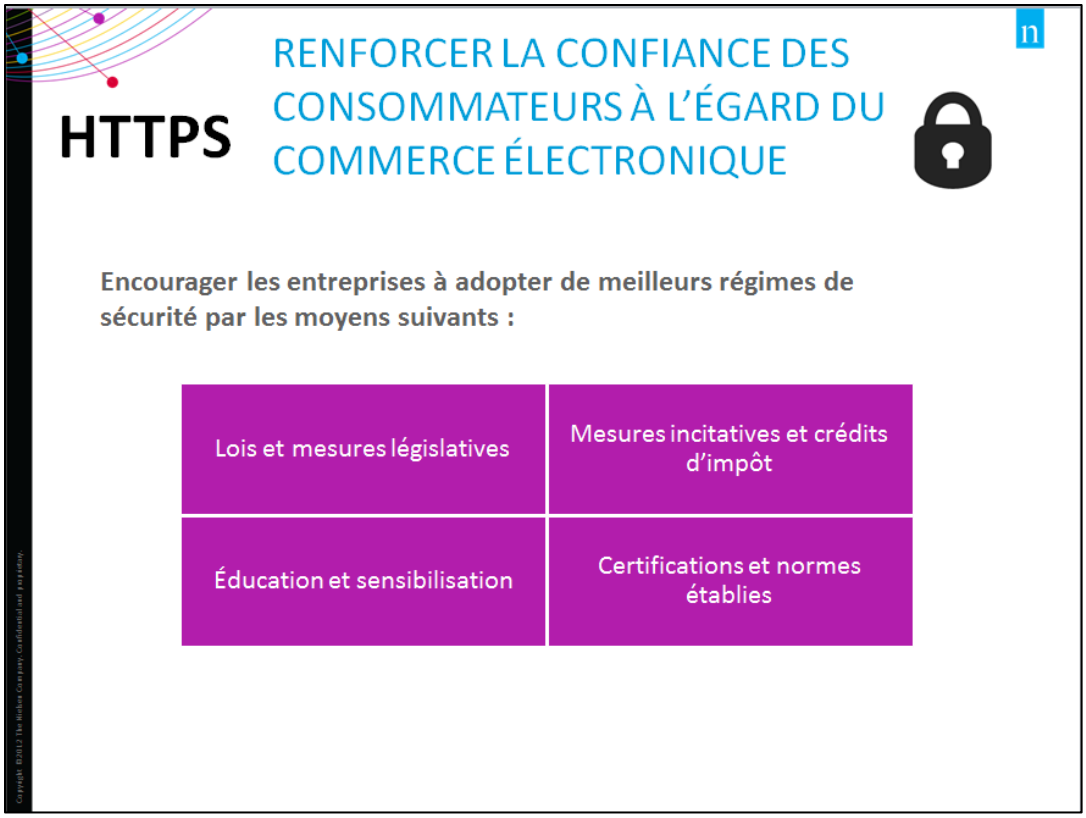
Les technologies numériques et Internet sont des moteurs d'innovation et de croissance économique de plus en plus importants.

Parallèlement, la cybersécurité peut améliorer la capacité concurrentielle, la stabilité économique et la prospérité à long terme du Canada. Le Canada a l'occasion de façonner un avantage concurrentiel dans le domaine de la cybersécurité et de créer une économie numérique robuste, sécurisée et à la fine pointe.

Renforcer la confiance des consommateurs à l'égard du commerce électronique

Le cahier de travail précisait que les Canadiens doivent pouvoir se fier à la sécurité des transactions en ligne pour protéger la confiance des consommateurs et stimuler l'économie par le biais d'un engagement continu sur le marché en ligne. Il soulignait également que bon nombre d'entreprises ne réalisent pas qu'elles pourraient être ciblées par des cybercriminels ou estiment qu'il est difficile de trouver des solutions abordables et efficaces pour protéger leurs renseignements.

On a demandé aux participants comment les entreprises pouvaient être encouragées à adopter de meilleurs régimes de cybersécurité et de quels facteurs il faut tenir compte lorsqu'il vient le temps d'évaluer le niveau de sécurité des entreprises en ligne.



ENCOURAGER L'ADOPTION DE MEILLEURS RÉGIMES DE CYBERSÉCURITÉ

« Il faut établir une certification facultative pour les entreprises et les particuliers. Selon le niveau, les membres participants pourraient devoir faire un examen sur la cybersécurité, mettre en œuvre des pratiques exemplaires, ou même déclarer leur trafic Internet à la police. » [traduction]

Lorsqu'on a demandé aux participants quelles mesures pouvaient être prises pour encourager les entreprises à adopter de meilleurs régimes de cybersécurité, la plupart de leurs réponses portaient sur quatre idées principales :

- établir des lois et des règlements;
- offrir des mesures incitatives ou des crédits d'impôt;
- promouvoir l'éducation et la sensibilisation;
- élaborer des certifications et des normes.

Selon certains participants, les entreprises devraient collaborer avec des partenaires stratégiques et effectuer des tests et des vérifications internes de sécurité.

Les participants de l'industrie de la cybersécurité étaient plus susceptibles de recommander des lois et des mesures législatives, et lorsqu'ils sont associés aux participants des autres industries, ils étaient également plus susceptibles de suggérer l'éducation et la sensibilisation ainsi que l'élaboration de certifications et de normes.

Alors que les participants du gouvernement étaient moins susceptibles de suggérer des mesures incitatives et des crédits d'impôt pour encourager les entreprises, ils étaient plus susceptibles de dire qu'une certification et des normes établies permettraient d'atteindre ce but.

Les citoyens mobilisés étaient moins susceptibles de citer les lois et les mesures législatives comme des façons d'encourager les entreprises.

FACTEURS IMPORTANTS À PRENDRE EN CONSIDÉRATION

De loin, le facteur le plus souvent cité par les participants dans l'évaluation de la sécurité d'un site Web concernait l'inclusion du protocole HTTPS au début des adresses Web.

De nombreux participants ont également mentionné la réputation de l'entreprise comme un important facteur. Cependant, peu de citoyens mobilisés ont fourni cette réponse.

Les participants ont également mentionné le chiffrement des données et l'utilisation de voies sécurisées comme stratégies pour évaluer les niveaux de sécurité, surtout pour les participants des autres industries. Peu de participants des autres industries et de citoyens mobilisés ont mentionné les logos de sécurité ou les timbres de certification, même s'il s'agit d'une réponse tout de même fréquente.

« Les logos sécurisés ne comptent guère, et le protocole SSL (HTTPS) pourrait tout de même être vulnérable aux attaques de l'intercepteur. Il est impossible d'être totalement en sécurité. » [traduction]

Certains participants estimaient que les gens doivent être plus sceptiques quant à la sécurité des sites Web. Par exemple, certains ont dit que certains sites Web peuvent sembler sécuritaires, même s'ils ne le sont pas. Les participants du gouvernement étaient particulièrement susceptibles de penser que les gens devraient faire preuve de prudence lors de l'évaluation des déclarations de sécurité d'un site Web.

De plus, les facteurs suivants ont été mentionnés dans quelques-unes des réponses des participants :

- des mots de passe forts;
- une certification SSL/TLS;
- une authentification multifactorielle;
- l'utilisation de données biométriques;
- des évaluations indépendantes du site Web;
- le numéro de téléphone et l'adresse de l'entreprise.

Adopter de nouvelles technologies cybersécuritaires

Pour présenter les questions aux participants, le cahier de travail précisait que même si les Canadiens continuent d'adopter des appareils réseautés intelligents, il n'existe aucune norme claire pour protéger ces appareils et assurer la confidentialité des données qu'ils recueillent. Il décrit également un obstacle potentiel voulant que la mise en œuvre de normes puisse miner la capacité des entreprises canadiennes de mettre en marché de nouveaux produits ou retarder le lancement de produits pour les consommateurs canadiens.

Dans cette optique, on a demandé aux participants quelles mesures devraient être prises pour s'assurer que les technologies réseautées et émergentes sont cybersécuritaires.

MESURES À PRENDRE POUR ASSURER LA CYBERSÉCURITÉ

Lorsque l'on a demandé aux participants quelles mesures devraient être prises pour assurer la cybersécurité des technologies nouvelles et émergentes, la réponse la plus souvent donnée par les participants concernait l'établissement de normes claires et de pratiques exemplaires. De nombreux participants ont parlé de la nécessité d'établir une réglementation et d'en assurer l'application pour tenir responsables les fabricants et les développeurs de produits et de services. Même si ces idées ont été souvent communiquées, les participants des autres industries étaient plus susceptibles de mentionner les deux.

De nombreux participants ont parlé de la nécessité d'accroître l'éducation du public, de respecter les protocoles de chiffrement, de vérifier les serveurs et la technologie, ainsi que d'exiger et d'élaborer des normes de certification pour protéger les nouvelles technologies.

Les participants de l'industrie de la cybersécurité étaient plus susceptibles de suggérer l'audit, la certification, la réglementation et l'application de la loi pour protéger les technologies réseautées et émergentes.

AUTRES POINTS DE VUE

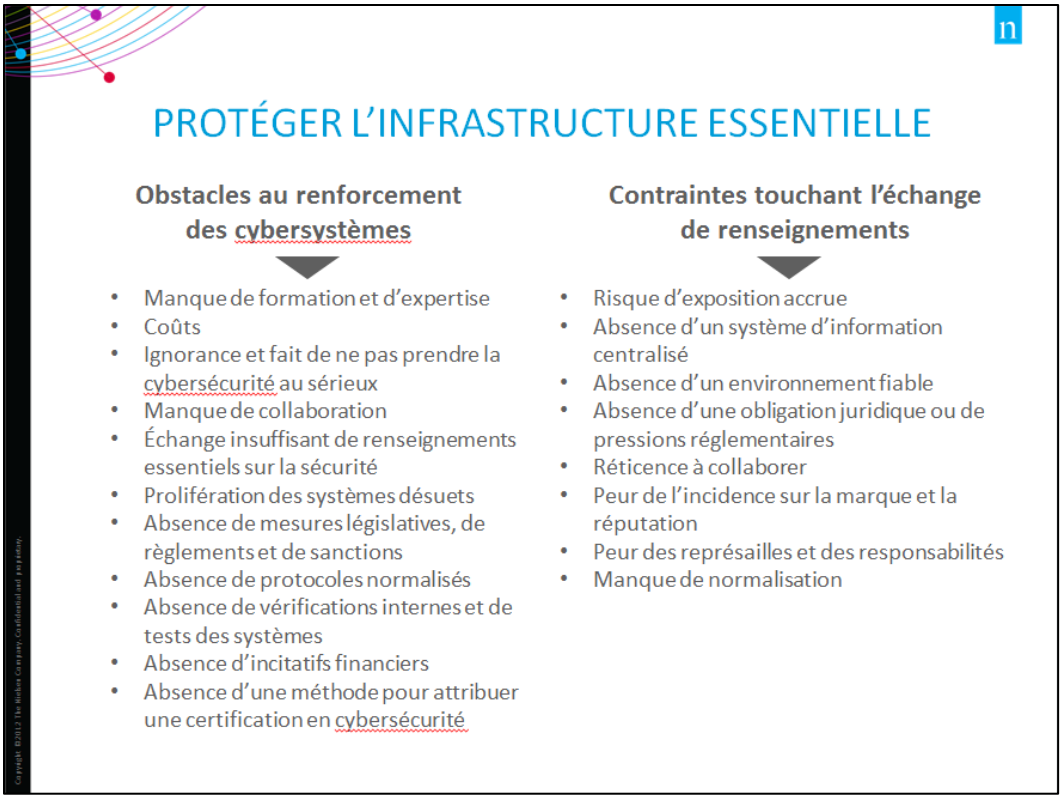
« Le particulier a une importante responsabilité, soit celle de s'assurer que les applications installées sont vérifiées au moyen d'un dépôt reconnu. » [traduction]

Certains participants estimaient que le public devait assurer sa propre protection et comprendre que des risques sont associés à l'utilisation de leurs appareils (surtout sur des réseaux ouverts et non sécurisés).
Quelques participants ont également suggéré d'éviter d'utiliser les paramètres par défaut sur leurs appareils.

Protéger les infrastructures essentielles

L'introduction aux questions concernant la protection des infrastructures essentielles soulignait comment les améliorations clés apportées aux infrastructures essentielles par le biais de l'adoption de technologies numériques et de systèmes réseautés ont créé une vulnérabilité qui peut être exploitée par ceux qui ont un faible pour le vol, l'espionnage et le sabotage. Selon l'introduction, même si la majeure partie des infrastructures essentielles du Canada appartient au secteur privé, le gouvernement du Canada devra trouver des façons de rassembler d'autres ordres de gouvernement et les propriétaires et les exploitants afin de lutter véritablement contre les menaces à l'égard des services essentiels.

On a ensuite demandé aux participants de donner leur avis sur la façon de protéger les infrastructures essentielles en recensant les obstacles au renforcement des cybersystèmes et les contraintes touchant l'échange de renseignements et la mobilisation.



OBSTACLES AU RENFORCEMENT DES CYBERSYSTÈMES

Les participants ont cerné des obstacles fréquents au renforcement des cybersystèmes, notamment :

- le manque de formation et d'expertise;
- les coûts (p. ex. *« Le manque de produits testés correctement et la course pour être les premiers sur le marché au plus bas coût causent ce problème. »* [traduction]);
- l'ignorance et le fait de ne pas prendre la cybersécurité au sérieux;
- le manque de collaboration;
- l'échange insuffisant de renseignements essentiels sur la sécurité;
- la prolifération des systèmes désuets;
- l'absence de mesures législatives, de règlements et de sanctions;
- l'absence de protocoles normalisés;
- l'absence de vérifications internes et de tests des systèmes;
- l'absence d'incitatifs financiers;
- l'absence d'une démarche pour attribuer une certification en cybersécurité.

CONTRAINTES TOUCHANT L'ÉCHANGE DE RENSEIGNEMENTS ET LA MOBILISATION

Les participants ont cerné des contraintes fréquentes à l'échange de renseignements et à la mobilisation, notamment :

- le risque d'exposition accrue (aux criminels et aux concurrents);

- l'absence d'un système d'information centralisé;
- l'absence d'un environnement fiable;
- l'absence d'une obligation juridique ou de pressions réglementaires;
- la réticence à collaborer;
- la peur de l'incidence sur la marque et la réputation (*« La politique, l'image publique, le mépris de l'importance. »* [traduction]);
- la peur des représailles et des responsabilités;
- le manque de normalisation.

ÉLARGISSEMENT DES FRONTIÈRES DE LA CYBERSÉCURITÉ

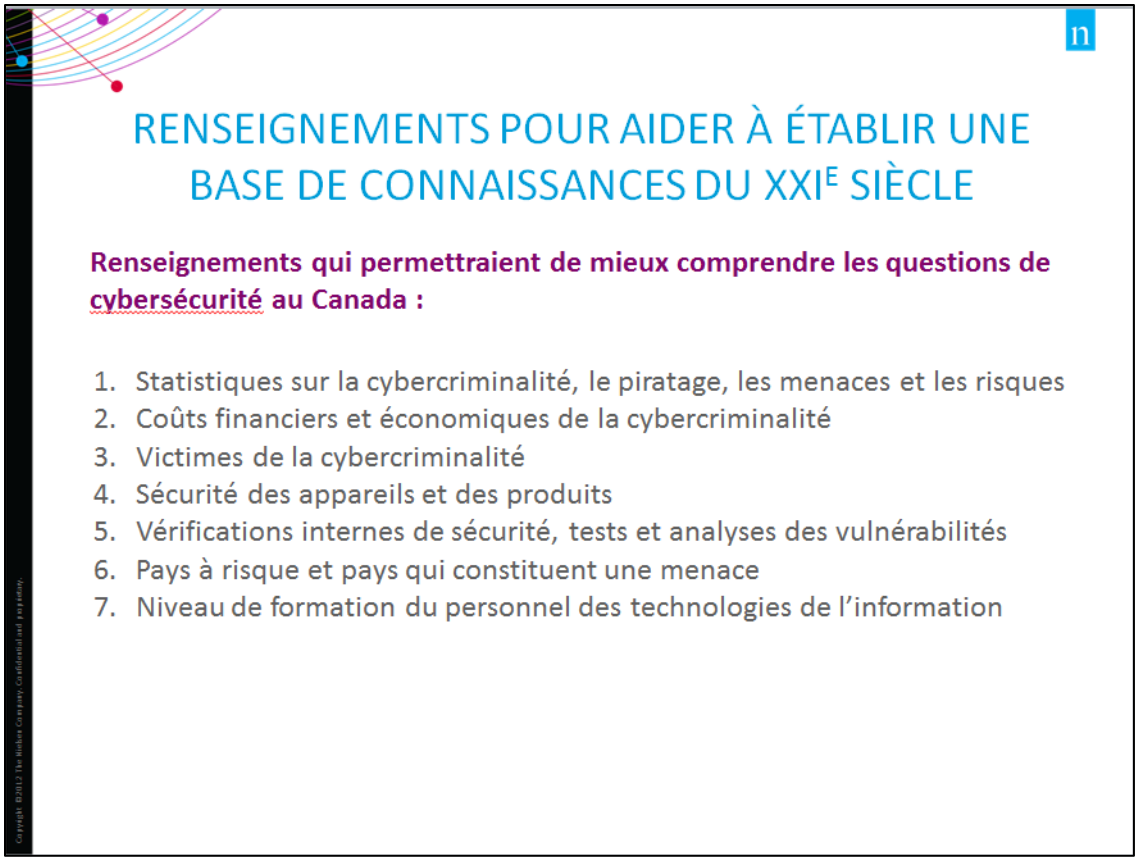
Depuis la mise en œuvre de la Stratégie de cybersécurité du Canada en 2010, les nouvelles technologies ont joué un rôle déterminant dans la transformation du paysage numérique. Compte tenu de cette nouvelle réalité, la cybersécurité doit évoluer au même rythme que les nouvelles technologies.

Le Canada doit être en mesure de maintenir une approche de cybersécurité agile et flexible pour exploiter de nouvelles possibilités ainsi que développer et adopter des capacités et des technologies clés.

Établir une base de connaissances du XXI^{e} siècle

Le cahier de travail précisait que le Canada avait besoin de meilleurs renseignements sur les questions de cybersécurité afin de fournir une vue plus exacte des questions de cybersécurité, d'affronter les menaces contre la cybersécurité, et de cerner des occasions relatives à la cybersécurité. Toujours selon le cahier de travail, ces renseignements pourraient ensuite être utilisés par le milieu universitaire, les chercheurs et les décideurs afin de comprendre les tendances et de guider l'élaboration de nouveaux programmes, services et politiques.

On a demandé aux participants de déterminer quels renseignements permettraient de mieux comprendre les questions de cybersécurité au Canada.



RENSEIGNEMENTS POUR APPUYER UNE MEILLEURE COMPRÉHENSION

« Peu de personnes apprécient la pertinence stratégique des renseignements sur la cybersécurité. Vous ne pouvez gérer ce que vous ne mesurez pas. » [traduction]

On a demandé aux participants quels renseignements permettraient de mieux comprendre les questions de cybersécurité au Canada. Leurs suggestions, présentées ci-après, ont été classées selon la fréquence de réponse :

- des statistiques sur la cybercriminalité, le piratage, les menaces et les risques (p. ex. fréquence et moment, lieu de l'incident, incidence);
- les coûts financiers et économiques de la cybercriminalité;
- les victimes de la cybercriminalité;
- la sécurité des appareils et des produits;
- les vérifications internes de sécurité, les essais et les analyses des vulnérabilités;
- les pays à risque et les pays qui constituent une menace;
- le niveau de formation du personnel des technologies de l'information.

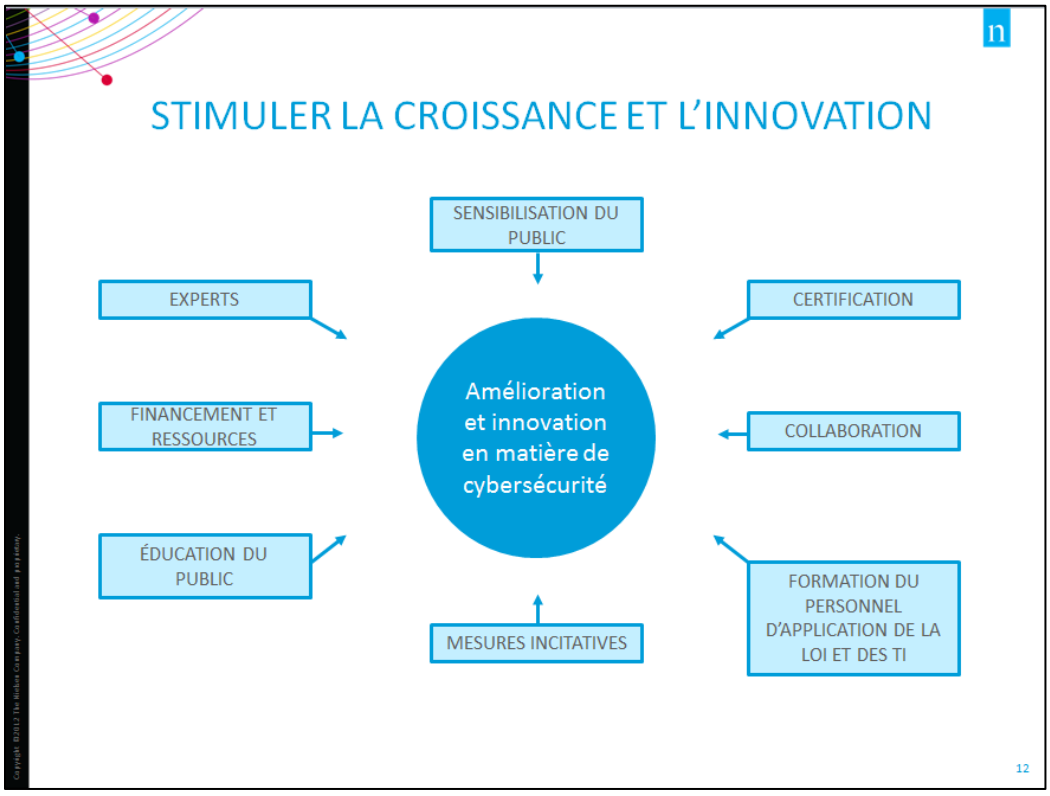
Même si la question n'a pas été expressément posée, l'avis général relatif à la collecte et à la publication de ce type de renseignements semblait être favorable.

Stimuler la croissance et l'innovation

Avant de présenter les questions de la consultation, on a informé les participants que le Canada doit favoriser la création d'une main-d'œuvre solide en cybersécurité, ainsi que l'établissement de centres de technologie de cybersécurité de pointe, afin de stimuler la croissance et l'innovation en matière de cybersécurité et de continuer de récolter les bénéfices de l'économie numérique mondiale.

Dans cet esprit, on a demandé aux participants quelles mesures pouvaient être prises pour améliorer la disponibilité, la pertinence et la qualité de la formation en cybersécurité et quelles conditions sont nécessaires pour accroître l'innovation du Canada en matière de cybersécurité.

Les participants ont mentionné bon nombre des mêmes idées pour les deux questions.



ACCROÎTRE L'INNOVATION DU CANADA EN MATIÈRE DE CYBERSÉCURITÉ

Selon les participants, l'amélioration des connaissances du public et de la cyberlittératie permettrait d'accroître l'innovation en matière de cybersécurité.

« La sensibilisation favorisera l'innovation. » [traduction]

Une autre solution fréquemment mentionnée était de collaborer avec des partenaires stratégiques, ainsi que disposer de suffisamment de fonds et de ressources.

Certains participants estimaient que d'offrir des mesures incitatives et des crédits d'impôt, de consulter et d'embaucher des experts, ou d'améliorer la formation du personnel des organismes d'application de la loi et des technologies de l'information favoriserait l'innovation.

« Il est surtout important de s'assurer que les chercheurs sont en mesure de faire leur travail sans s'inquiéter d'être poursuivis par des entreprises contrariées. Aux États-Unis, il existe de nombreux exemples de documents qui ne sont pas divulgués et de recherches qui ne sont pas effectuées parce que des fabricants d'appareils ou des propriétaires de contenu ont menacé d'engager des poursuites. Nous devons nous assurer que la situation juridique au Canada est très claire : les recherches sur les vulnérabilités sur le plan de la sécurité n'entraîneront pas de poursuites contre les chercheurs, même si (surtout si) ces recherches mènent à la découverte et à la médiatisation de vulnérabilités. » [traduction]

Dans le cadre de la consultation, quelques participants étaient d'avis que les menaces de poursuites et les lois rigoureuses sur le droit d'auteur restreignent la créativité et l'innovation.

AMÉLIORER LA DISPONIBILITÉ, LA PERTINENCE ET LA QUALITÉ DE LA FORMATION EN CYBERSÉCURITÉ

Bon nombre des mêmes idées énumérées ci-dessus pour aider à favoriser l'innovation canadienne dans le domaine de la cybersécurité ont été formulées afin d'améliorer la formation en cybersécurité et, dans une plus large mesure, la cybersécurité en général.

La réponse la plus fréquente concerne la création de programmes visant à améliorer la formation en cybersécurité.

Une autre réponse fréquente concerne l'amélioration de la formation du personnel des organismes d'application de la loi et des technologies de l'information.

Certains participants ont également formulé des suggestions pour améliorer la formation en cybersécurité, notamment :

- créer un programme de certification pour les professionnels de la cybersécurité;
- rendre la formation obligatoire en milieu de travail;
- fournir du financement pour les programmes de formation et d'éducation;
- travailler avec des spécialistes de la cybersécurité et les embaucher;
- commencer l'éducation en cybersécurité dès l'enfance;
- offrir des ressources et de la formation en ligne.

Certains participants ont mentionné la nécessité de mettre à jour la formation en cybersécurité actuellement disponible.

Aussi, certains participants ont indiqué que le problème n'était pas la formation, mais plutôt le manque de sensibilisation du public.

PROCHAINES ÉTAPES RELATIVES À LA CYBERSÉCURITÉ AU CANADA

La révolution numérique a fondamentalement changé le tissu social, économique et culturel du Canada. La participation du Canada à la vie numérique a offert de nombreux avantages, engendré une immense prospérité et ouvert une nouvelle porte sur le monde. Par ailleurs, les Canadiens se voient régulièrement offrir de nouveaux moyens d'accéder au monde, lesquels moyens présentent des défis et des menaces qui pourraient miner les nombreux avantages de l'ère numérique. La nouvelle approche du Canada en matière de cybersécurité doit tenir compte de ces questions complexes et intégrées.

Prochaines étapes au Canada

Le cahier de travail précisait de quelle façon le Canada disposera d'une stratégie renouvelée en matière de cybersécurité guidée par les cinq principes suivants :

- assurer la sûreté et la sécurité des Canadiens en ligne et des infrastructures essentielles du Canada;
- promouvoir et protéger les droits et les libertés en ligne;
- reconnaître et promouvoir l'importance de la cybersécurité pour les entreprises, la croissance économique et la prospérité;
- collaborer et assurer la coordination entre les administrations et les secteurs afin de renforcer collectivement la cybersécurité du Canada;
- s'adapter pour répondre aux technologies émergentes et aux conditions changeantes.

Trois domaines d'intervention potentiels ont également été suggérés pour examen, soit :

- **la résilience :** elle comprend la prévention et l'atténuation des cyberattaques évoluées contre les institutions et les systèmes canadiens, et l'intervention en cas de cyberattaque, ainsi qu'une plus grande mobilisation du public en matière de cybersécurité;
- **la collaboration et la capacité :** ce secteur serait axé sur la collaboration afin d'acquérir des compétences et de créer des ressources et des outils nécessaires pour assurer une cybersécurité efficace au Canada;
- **l'innovation cybernétique :** ce secteur serait axé sur des initiatives qui permettraient aux gouvernements, aux entreprises et aux citoyens canadiens de prévoir les tendances, de s'adapter à un environnement changeant et de demeurer à la fine pointe de l'innovation en matière de cybersécurité.

On a demandé aux participants de formuler des commentaires sur les champs d'action présentés et de cerner toute mesure potentielle qui, selon eux, améliorerait la cybersécurité au Canada.

Il est important de mentionner que les participants ont généralement accepté les champs d'action proposés. Un grand nombre de participants ont indiqué qu'ils en convenaient et ont ajouté leurs propres idées ou encore n'ont pas du tout mentionné les exemples fournis. Plutôt que d'être distinctement différente, cette partie a produit bon nombre des mêmes opinions et idées révélées dans les parties précédentes de la consultation. À ce titre, il s'agit d'un bon résumé de l'ensemble de la consultation sur la cybersécurité.

DOMAINES D'INTÉRÊT DES PARTICIPANTS

Ces domaines sur lesquels les participants se sont concentrés étaient des thèmes transversaux dans de nombreux cas. En effet, bon nombre de participants ont fourni des réponses larges, souvent une combinaison des 10 domaines décrits ci-dessus.

Protection de la vie privée

« Je veux bien que mon gouvernement s'assure que nous, les Canadiens, sommes en sécurité. Cependant, je ne sacrifierai pas ne serait-ce qu'un minuscule détail de ma vie privée ou de ma liberté pour obtenir un peu plus de sécurité. » [traduction]

La protection de la vie privée était une grande préoccupation des participants, surtout des citoyens mobilisés.

De nombreux participants ont très clairement indiqué que tous les champs d'action devaient être envisagés, mais que le maintien des droits à la vie privée des Canadiens devait être au premier rang des efforts du Canada pour améliorer la cybersécurité.

Certains participants ont mentionné que le respect de la procédure établie (p. ex. un soupçon raisonnable et des mandats sont exigés des organismes d'application de la loi en cours d'enquête) et le maintien de la confidentialité des renseignements personnels recueillis pendant l'enquête occupaient une place importante dans le maintien des droits à la vie privée.

Collaboration

« Promouvoir et cultiver les occasions de collaboration et de partenariat entre le milieu universitaire et les secteurs privés et publics au Canada et dans le monde entier. » [traduction]

De nombreux participants ont dit qu'une collaboration était nécessaire. Ils estimaient que la collaboration, la coordination et les relations avec des partenaires stratégiques étaient importantes pour améliorer la cybersécurité au Canada. Ces partenaires peuvent comprendre d'autres nations, le secteur privé, d'autres organismes gouvernementaux et le milieu universitaire.

D'autres participants ont parlé de l'importance de la collaboration dans le cadre de l'échange de renseignements et du signalement des vulnérabilités, des problèmes et des faiblesses. Les citoyens mobilisés étaient moins susceptibles que d'autres types de participants de parler de collaboration, alors que les participants du gouvernement étaient plus susceptibles de le faire.

Il faut noter que les participants ne croyaient pas tous que le gouvernement du Canada avait une responsabilité ou devait participer aux prochaines étapes du pays en matière de cybersécurité, mais cette opinion n'était pas très répandue.

Éducation

« L'éducation et la formation sont fondamentales. » [traduction]

Pour certains participants, l'éducation et la sensibilisation du public sont essentielles aux prochaines étapes que franchira le Canada en matière de cybersécurité, ce qui pourrait vouloir dire l'amélioration

de la base de connaissances ou de la cyberlittératie du public ou encore une meilleure compréhension de l'importance des questions de cybersécurité au sein de celui-ci. Les participants des autres industries étaient moins susceptibles de mentionner l'éducation du public.

Toutefois, l'éducation ne se limitait pas qu'au public. Bon nombre de participants ont dit qu'il était important que le personnel des organismes d'application de la loi et de la cybersécurité se voie offrir une meilleure éducation et une meilleure formation également.

Normalisation

« Application renforcée des règlements et utilisation de licences de production et de fabrication. » [traduction]

Un grand nombre de participants ont indiqué qu'il était nécessaire de normaliser les pratiques exemplaires et de s'assurer que les lignes directrices sont claires et faciles à suivre. L'idée générale des « normes » a été largement communiquée.

Certains participants de l'industrie de la cybersécurité ont parlé de la nécessité de normaliser les techniques utilisées pour protéger tous les appareils et estimaient que le Canada devait contribuer à ces normes à l'échelle internationale.

Application de la loi

« Créer un centre national de coordination de la lutte contre la cybercriminalité qui serait chargé du triage, de l'harmonisation et de la coordination relativement aux enquêtes sur la cybercriminalité des différentes administrations. » [traduction]

Certains participants estimaient que les organismes d'application de la loi doivent imposer des amendes et poursuivre les cybercriminels. Bien qu'aucun des participants du gouvernement ne l'ait mentionné, quelques participants ont indiqué que des mesures législatives et des mandats devraient être en place pour lutter contre la cybercriminalité. Pour d'autres, la loi s'appliquait en tenant responsables les entreprises ou les fabricants qui ne maintiennent pas des normes de sécurité suffisantes (p. ex. les gardiens des données personnelles devraient être tenus responsables lorsqu'ils ne réussissent pas à protéger efficacement ces renseignements).

Selon quelques participants, les organismes d'application de la loi devraient se concentrer sur les crimes majeurs, et non les infractions mineures. Cette opinion a été formulée presque exclusivement par les citoyens mobilisés.

Transparence

« Accorder de larges pouvoirs discrétionnaires sans procédures légitimes, procédures établies et transparence suffisantes compromet les valeurs essentielles à la démocratie et à la culture canadienne. » [traduction]

Liée à certains autres champs d'action, la transparence était un thème fréquent lors de cette consultation. Selon un grand nombre de participants, il doit y avoir une augmentation globale de la transparence et de la surveillance publique afin que les intervenants (p. ex. organismes d'application de la loi, gouvernement et secteur privé) puissent être tenus responsables des mesures qu'ils prennent

pour assurer la cybersécurité. Certains participants ont affirmé que le gouvernement devrait consulter le public alors qu'il va de l'avant pour améliorer la cybersécurité au Canada (une réponse principalement formulée par les participants du gouvernement). Quelques participants ont dit que la transparence et la sensibilisation du public permettraient au bout du compte d'accroître la sensibilisation aux problèmes posés.

Mesures rigoureuses en matière de cybersécurité

« En ce qui concerne la cybercriminalité, un facteur atténuant clé sera la solidité des méthodes de chiffrement et des systèmes de sécurité utilisés par les particuliers, les sociétés et le grand public, ce qui signifie n'avoir accès à AUCUN passe-partout, passage ou porte dissimulée dans les systèmes sécurisés même pour le gouvernement, les organismes gouvernementaux ou les parties qui y sont associées de quelque manière que ce soit. » [traduction]

Une autre réponse fréquente des participants ciblait l'élaboration ou l'utilisation de mesures rigoureuses en matière de cybersécurité, notamment utiliser des réseaux privés virtuels, une connexion Internet sécurisée et le chiffrement, s'abstenir d'utiliser des portes dissimulées et tenir les logiciels à jour. Certains participants ont dit que ces mesures devraient être obligatoires.

Expertise

« Toutes les organisations, qu'elles soient publiques, privées ou gouvernementales, devraient embaucher de véritables experts qui savent ce qu'ils font. » [traduction]

Un grand nombre de participants ont clairement indiqué que toute mesure prise en matière de cybersécurité devait être dirigée par des employés qualifiés qui sont des experts dans le domaine.

Investissement

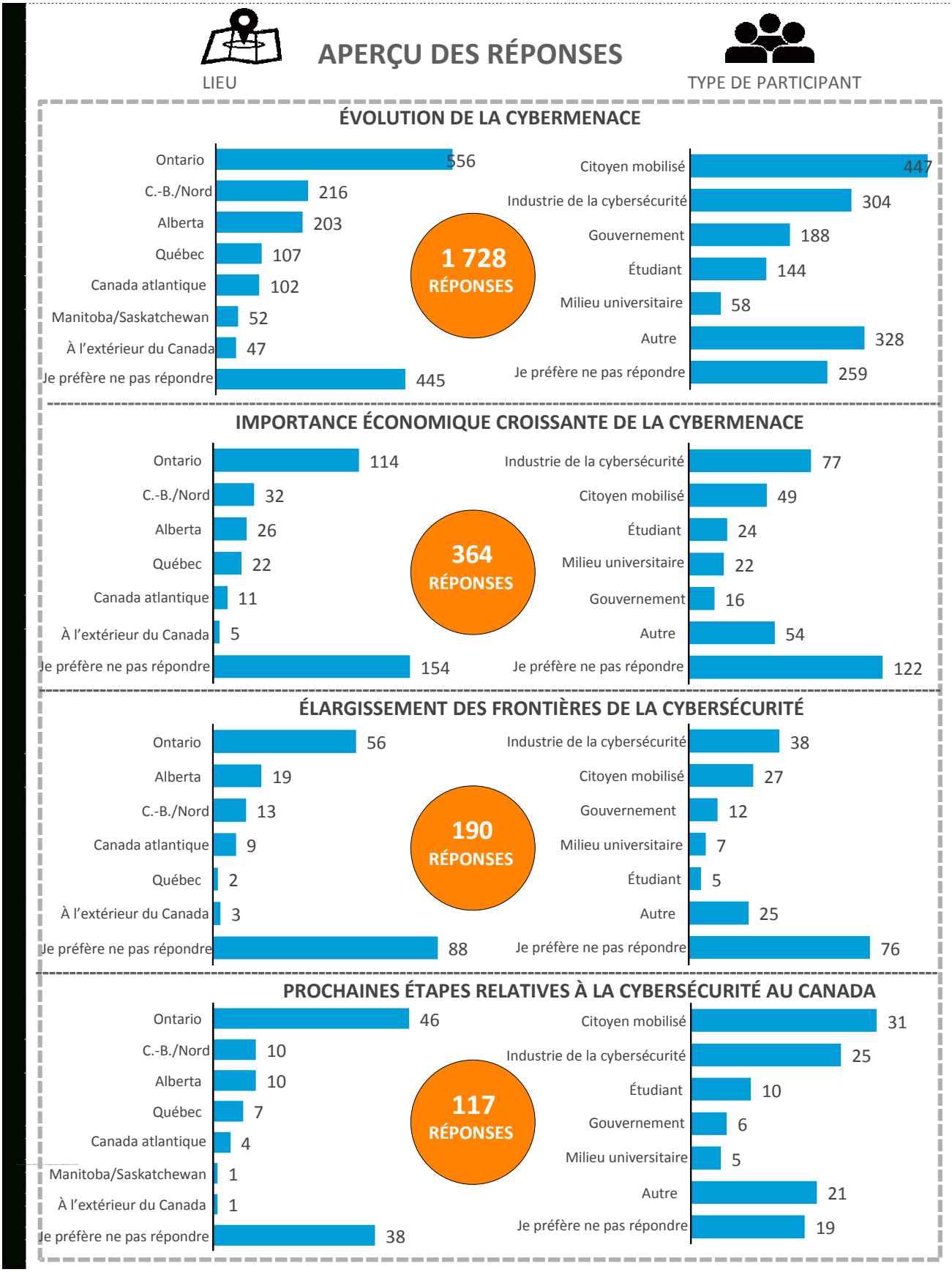
Une autre réponse fréquente parmi les participants concernait l'investissement, notamment des investissements accrus dans les programmes, la technologie, le personnel et l'éducation. En ce qui concerne le gouvernement, certains participants ont parlé de la nécessité d'établir des crédits budgétaires, à savoir mettre de côté des fonds pour les mesures de cybersécurité.

Être proactif

« Il semble qu'une importance excessive soit accordée à la résilience, à la gestion des urgences et à la reprise après catastrophe, présentant ainsi une politique d'échec comme point de départ d'une stratégie pour la protection des infrastructures essentielles et du cyberespace. Une cyberdéfense proactive devrait être ajoutée. » [traduction]

Selon certains participants, les mesures prises pour améliorer la cybersécurité au Canada devraient être proactives plutôt que réactives. En réalité, quelques participants ont expressément dit que les champs d'action présentés comme exemples dans le cahier de travail étaient trop défensifs et devraient plutôt être plus offensifs.

ANNEXE A – APERÇU DES RÉPONSES



ANNEXE B – PERSPECTIVES DES INTERVENANTS

Des intervenants clés du gouvernement, du secteur des infrastructures essentielles, du milieu universitaire et du secteur privé ont été invités à participer à la consultation. Des réponses particulières ont été compilées ci-après pour présenter un aperçu des perspectives reçues.

DOMAINES D'INTERVENTION

Les intervenants ont recommandé une gamme de mesures qui pourraient être prises pour améliorer la cybersécurité au Canada.

Lutter contre la cybercriminalité

- Pour lutter contre la cybercriminalité d'une façon qui respecte les droits à la vie privée des Canadiens, les solutions suivantes devraient être envisagées :
    - cibler les forums clandestins pour perturber l'échange d'outils cybercriminels puissants et faciles à utiliser;
    - perturber l'infrastructure des créateurs de codes malveillants et des hébergeurs Web spécialisés par le biais de l'identification active des groupes de développeurs ainsi que de la collaboration des organismes d'application de la loi, du gouvernement et de l'industrie des TIC pour démanteler les sociétés d'hébergement;
    - cibler les produits de la cybercriminalité en collaboration avec le secteur financier;
    - continuer d'accroître la compréhension des comportements des cybercriminels contemporains.
- Les stratégies de lutte contre la cybercriminalité devraient notamment mettre l'accent sur les services de soutien axés sur les victimes qui traitent des circonstances uniques de la victimisation facilitée par la technologie. Les victimes pourraient avoir besoin de différents services, comme des lignes directrices sur la façon de rétablir leur réputation financière ou personnelle.
- Il est nécessaire d'accroître la sensibilisation du public à l'égard de la victimisation cybernétique et de s'assurer que le personnel de la justice pénale reçoit une formation adéquate sur la victimisation cybernétique.
- Il serait utile de créer une méthode modèle pour signaler les cybercrimes. Cette méthode pourrait employer un principe de guichet unique qui permet à tous les incidents touchant la cybersécurité d'être signalés par l'intermédiaire d'une interface virtuelle simple, peu importe l'administration, la portée ou la nature.
- Un mécanisme exigeant que les secteurs public et privé téléchargent le détail du cybercrime présumé (p. ex. fichiers, captures d'écran, courriels) doit être en place.

Respecter la vie privée tout en améliorant la sécurité

- L'application de la loi dans le cyberespace devrait tenir compte des principes suivants :
  - permettre l'accès aux renseignements numériques en vertu d'un processus légitime seulement;
  - maintenir le droit des fournisseurs de technologie de contester les demandes au nom de leurs consommateurs;
  - exiger des formes plus rigoureuses de processus judiciaire pour les renseignements plus sensibles;
  - autoriser la divulgation en cas d'urgence seulement;
  - appuyer la transparence;
  - les particuliers et les organisations ont le droit de savoir à quel moment le gouvernement accède à leurs renseignements numériques (sauf dans de rares cas);
  - moderniser les règles qui régissent les cibles appropriées des demandes de données;
  - s'assurer que les réformes réglementaires ou juridiques dans ce domaine n'affaiblissent pas la sécurité, un élément essentiel de la confiance des utilisateurs dans la technologie.

Améliorer la gouvernance et les partenariats

- Au sein du paysage actuel de la cybersécurité, de nombreux organismes gouvernementaux fédéraux ont les mêmes buts. Il est possible de rationaliser tous les secteurs cruciaux en un seul organisme unique.
- Il est nécessaire d'établir un réseau de renseignements sur les menaces qui peut répondre aux besoins des secteurs public et privé. Les consommateurs seraient alors en mesure de s'abonner à un fil de nouvelles par différents moyens, comme les courriels, les messages textes ou les mises à jour sur le Web, afin de recevoir en temps opportun des comptes rendus sur les plus récentes questions ou attaques ainsi que des lignes directrices sur la façon de se protéger.
- La création d'un centre national d'innovation en matière de cybersécurité permettrait au gouvernement, à l'industrie et au milieu universitaire d'élaborer conjointement des programmes d'éducation, des programmes de gestion des talents, des politiques et des instruments de financement.

  « Si le Canada devait harmoniser ses ressources dans l'ensemble du gouvernement, de l'industrie, du milieu universitaire et du secteur de la recherche et offrir les forums et les mesures incitatives appropriés en vue d'investissements multinationaux, il serait alors probable d'observer une hausse considérable des investissements commerciaux dans l'innovation, l'élaboration de solutions et la recherche en matière de cybersécurité au Canada. » [traduction]
- Il faut créer une liste de sites de commerce électronique approuvés par le gouvernement du Canada ou le Conseil canadien des bureaux d'éthique commerciale.

Promouvoir la mesure

- La collecte de données sur la victimisation cybernétique au Canada doit être améliorée, régularisée et normalisée. Il faudrait envisager d'intégrer un nouveau sondage national ou une base de données centralisée des rapports sur les cybercrimes et la victimisation cybernétique.
- Les mesures recueillies et publiées devraient correspondre aux résultats. Les mesures actuelles ne correspondent pas aux interventions ou aux résultats. *« Les mesures devraient directement fournir des lignes directrices sur la façon d'améliorer la situation actuelle afin d'obtenir le résultat désiré. »* [traduction]
- *« Le gouvernement doit harmoniser les avantages des TIC (croissance du produit intérieur brut) avec les responsabilités en matière de TIC (perte de produit intérieur brut) afin de cerner des facteurs comme la dimension de l'économie, s'il y avait une diminution des cyberincidents. »* [traduction]

Accroître la sensibilisation et l'éducation du public

- *« Habiliter les filles à étudier en STIM (sciences, technologie, ingénierie et mathématiques) dès l'école primaire. Encourager, saisir et créer des occasions de croissance pour les femmes en technologies de l'information et cybersécurité, y compris des occasions à l'échelle du conseil. »* [traduction]
- Les écoles devraient intégrer des concepts de cybersécurité au programme afin de favoriser :
    - les interactions sécuritaires avec des étrangers dans les médias sociaux et les jeux virtuels;
    - la création d'une identité numérique et le partage de contenu en ligne d'une façon intelligente et sécuritaire;
    - les choix éclairés quant aux achats et aux ventes en ligne.
- Les conseils suivants devraient être offerts aux membres du public afin de les aider à se protéger.
    - Faites des recherches sur le site Web avant de vous engager.
    - Supprimez les courriels, les messages et les textos si vous doutez de leur source.
    - Protégez les renseignements personnels et les considérer comme de l'argent.
    - Utilisez des options de paiement sécuritaires, comme les cartes de crédit, lorsque vous faites des achats en ligne.
    - Fermez le système Bluetooth et Wi-Fi lorsque vous ne l'utilisez pas.
    - Limitez le type d'affaires que vous faites par le biais du service public ouvert Wi-Fi.
    - Exécutez toujours les versions les plus récentes des logiciels et des applications.
    - Renforcez la sécurité de vos comptes en ligne en utilisant les outils d'authentification les plus efficaces disponibles, comme les données biométriques, les clés de sécurité ou un code unique par le biais d'une application sur votre appareil mobile.
    - Créez une phrase comme mot de passe.
    - Choisissez un mot de passe unique pour chaque compte.

- Les campagnes publiques peuvent remédier au manque de sensibilisation à la cybercriminalité auprès de la population générale et encourager les victimes et les autres personnes concernées à faire un signalement.
- Un bulletin d'information cybernétique peut être créé pour les menaces nouvelles et émergentes contre la sécurité des Canadiens. Des bulletins brefs et à voies multiples peuvent être utilisés pour communiquer des nouvelles sur le cyberespace et d'autres renseignements de sécurité aux Canadiens.
- Les petites et moyennes entreprises ne croient pas qu'elles sont des cibles de grande valeur pour les cybercriminels. Cette croyance suggère une confiance excessive dans leur capacité de contrecarrer les attaques virtuelles évoluées d'aujourd'hui, ou plutôt que les attaques ne toucheront jamais leur entreprise.

Améliorer l'échange de renseignements

- Accroître l'échange de renseignements du gouvernement avec le secteur privé.
- Élaborer une stratégie globale pour l'échange de renseignements et la collaboration pour réduire la confusion et accroître le soutien des efforts d'échange de renseignements au sein d'une organisation et parmi les partenaires.
- Axer l'échange de renseignements sur les menaces passibles de poursuites, les vulnérabilités et l'atténuation.
- Établir un processus de gouvernance significatif qui comprend la gestion appropriée des données échangées, de leur création à leur diffusion, en passant par leur utilisation et leur destruction.
- Éliminer les obstacles législatifs et réglementaires qui gênent l'échange de renseignements parmi les sociétés privées, notamment l'inquiétude voulant que l'échange de renseignements crée des problèmes d'antitrust ou une responsabilité.
- S'assurer que les entités gouvernementales qui n'ont pas besoin des renseignements communiqués pour des raisons de cybersécurité n'y aient pas accès.
- Promouvoir des méthodes de gestion des vulnérabilités, lesquelles permettent de communiquer avec des tiers détecteurs, de valider et de classer les vulnérabilités, d'élaborer et de déployer une mise à jour pour atténuer les vulnérabilités, et d'appliquer des mises à jour aux systèmes opérationnels.
- Comprendre que la protection de la vie privée est un élément essentiel pour établir et maintenir une confiance numérique mondiale.

Former des professionnels en cybersécurité

- *« Il existe déjà une pénurie globale d'environ 1 million de professionnels en cybersécurité, et ce nombre continue d'augmenter. »* [traduction]
- Il faut s'assurer que les employés clés de la cybersécurité sont en mesure de participer aux activités de l'industrie et aux événements parrainés par le gouvernement dans l'ensemble des régions afin d'apprendre les uns des autres et de créer un réseau, lequel peut être utilisé pour élaborer un programme plus solide.

Adapter le cadre législatif

- Les dispositions du *Code criminel* doivent être renforcées pour refléter les actes criminels dans le cyberespace (sites Web frauduleux, matériel illégal protégé par des droits d'auteur en ligne, etc.).
- La *Loi sur la protection des renseignements personnels* pourrait être modifiée pour s'assurer que les données que détiennent les institutions gouvernementales sont protégées selon une norme rigoureuse (en transit et archivées, pendant leur utilisation, stockées, et au moment de leur destruction).
- Les institutions gouvernementales doivent signaler les infractions au-delà d'un seuil convenu et informer les personnes concernées en temps opportun. Le seuil de signalement obligatoire devrait être clairement défini dans la loi, d'une manière semblable aux récentes modifications apportées à la *Loi sur la protection des renseignements personnels et les documents électroniques*. Les institutions gouvernementales doivent conserver des dossiers de toutes les infractions à des fins d'examen potentiel par le Commissariat à la protection de la vie privée du Canada. Même si les infractions ne respectent pas le seuil de signalement obligatoire, les institutions devraient maintenir des dossiers et les fournir sur demande au Commissariat.
- *« Adopter une loi pour contraindre les organisations publiques et privées à déployer une authentification à deux facteurs pour tous les services accessibles au public, y compris les finances, l'éducation et les soins de santé. »* [traduction]

Établir des normes, des certifications et des règlements intelligents

- Les entreprises faisant des affaires à l'échelle mondiale doivent faire face à de multiples exigences réglementaires axées sur la cybersécurité. L'harmonisation des exigences pourrait atténuer le fardeau réglementaire tout en assurant des mesures de protection adéquates.
- Des normes plus rigoureuses en matière de cybersécurité peuvent poser des défis pour les innovateurs canadiens qui cherchent à créer des produits concurrentiels, et elles pourraient entraîner des retards dans l'intégration de produits extérieurs sur les marchés canadiens. Cependant, l'élaboration précoce de normes dans l'industrie peut également créer de la certitude et de la confiance chez le consommateur. Des mesures peuvent être prises pour s'assurer non seulement que des normes réglementaires sont en place, mais aussi que les innovateurs disposent des outils nécessaires pour respecter ces normes et en bénéficier également.
- Il existe de nombreux documents d'orientation et de normes dans l'industrie qui peuvent être exploités afin d'aider à élaborer un programme approprié pour traiter de ces appareils de l'Internet des objets, notamment :
    - NIST 800-53, 800-121, 800-171;
    - cadre de cybersécurité du NIST pour les infrastructures essentielles;
    - AAMI TIR57;
    - documents d'orientation préalables et postérieurs (ébauches) à la mise en marché de la Food and Drug Administration.

- Un sceau d'approbation devrait être attribué selon la mise en œuvre réussie des recommandations formulées dans le cadre d'une vérification interne de sécurité (pour les petites et moyennes entreprises).

Mettre en œuvre des pratiques rigoureuses en matière de cybersécurité

- Un programme efficace de cybersécurité utilise des outils comme la prévention des pertes de données, la sécurité des points d'accès, des pare-feu puissants, l'analytique de la sécurité et l'authentification à facteurs multiples.
- La modélisation des menaces devrait être effectuée pour évaluer les menaces contre un appareil et son environnement d'utilisation prévu. Des mesures de contrôle de la cybersécurité peuvent ensuite être utilisées pour atténuer les menaces, permettant ainsi de s'assurer que l'appareil est fabriqué d'une façon sécuritaire et sûre. Des tests de sécurité devraient être faits tout au long de l'élaboration. Une fois qu'un appareil est commercialisé, un plan doit être établi pour la gestion postérieure à la mise en marché également.
- La minimisation des données stockées aide à réduire la gravité des infractions potentielles en limitant la quantité de renseignements disponibles.

Participer à la collaboration internationale

- *« La collaboration internationale relative à l'établissement de normes de comportement en ce qui concerna la cybersécurité façonnera l'avenir du cyberespace dans l'ensemble des économies développées et émergentes, et nous espérons que le Canada jouera un rôle de premier plan dans cet espace. »* [traduction]
- Participer de façon proactive à l'établissement de normes internationales sur la gestion de l'identité.

Autres mesures potentielles

- Étendre la semaine des technophiles (« Geek Week ») sur la cybersécurité aux provinces (chacune pourrait avoir sa propre semaine à laquelle des collèges et des universités participeraient, par exemple).

ANNEXE C – QUESTIONS DE LA CONSULTATION

Tendance 1 : Évolution de la cybermenace

CONTRER LA CYBERCRIMINALITÉ

Q : Comment les organismes d'application de la loi peuvent-ils mieux relever les défis croissants que présente la cybercriminalité (p. ex. formation et renforcement des capacités, équipements, partenariats et initiatives novatrices)?
Q : Comment les organisations des secteurs public et privé peuvent-elles aider à se protéger elles-mêmes contre la cybercriminalité, notamment la menace d'attaques par rançongiciel, de fraudes et de vols d'identité, et de quels outils ont-elles besoin pour y parvenir?
Q : Y a-t-il des obstacles qui nuisent au signalement des cybercrimes (ou des cybercrimes présumés) aux organismes d'application de la loi? Dans l'affirmative, lesquels?

APPLIQUER LA LOI DANS LE CYBERESPACE

Q : Quelles sont vos attentes en matière d'application de la loi dans le cyberespace? Sont-elles différentes de vos attentes dans le monde réel?
Q : En cette ère numérique, la sécurité et la protection des renseignements personnels vont de pair. De quelle façon peut-on contrer la cybercriminalité tout en respectant les droits des Canadiens relatifs à la vie privée et en protégeant la sécurité du public?

SE PROTÉGER DES CYBERMENACES ÉVOLUÉES

Q : De quoi les organisations des secteurs public et privé ont-elles besoin pour se protéger contre les cybermenaces évoluées (p. ex. outils, capacités et renseignements)?
Q : Quelles sont les contraintes de l'échange de renseignements sur les cybermenaces évoluées et les vulnérabilités connexes?

ACCROÎTRE LA PARTICIPATION DU PUBLIC

Q : De quelle façon peut-on mieux informer les gens pour qu'ils sachent reconnaître un cybercrime (comme un hameçonnage ciblé) ou une vulnérabilité en matière de cybersécurité (p. ex. sécurité des voitures en réseau ou des dispositifs de santé branchés tels que les stimulateurs cardiaques)?
Q : De quelle façon les organisations des secteurs public et privé peuvent-elles travailler de concert pour sensibiliser les Canadiens à l'égard des questions de cybersécurité (p. ex. initiatives concertées de formation en ligne)?

Tendance 2 : Importance économique croissante de la cybersécurité

RENFORCER LA CONFIANCE DES CONSOMMATEURS À L'ÉGARD DU COMMERCE ÉLECTRONIQUE

Q : Comment peut-on encourager les entreprises canadiennes, tout particulièrement les petites et moyennes entreprises, à adopter de meilleurs systèmes de cybersécurité?
Q : De quels facteurs doit-on tenir compte avant d'échanger des renseignements personnels et financiers avec les entreprises en ligne (p. ex. sites Web affichant un logo sécurisé, adresses Web commençant par https)?

ADOPTER DE NOUVELLES TECHNOLOGIES CYBERSÉCURITAIRES

Q : Quelles mesures devraient être prises pour assurer la cybersécurité des nouvelles technologies et des technologies en réseau (comme l'Internet des objets et les applications)?

PROTÉGER LES INFRASTRUCTURES ESSENTIELLES

Q : Quels sont les obstacles au renforcement des cybersystèmes des infrastructures essentielles (au sein des secteurs et entre ceux-ci)?
Q : Quelles sont les contraintes liées à l'échange de renseignements et à la mobilisation pour la protection des cybersystèmes des infrastructures essentielles du Canada?

Tendance 3 : Élargissement des frontières de la cybersécurité

ÉTABLIR UNE BASE DE CONNAISSANCES DU XXI^{E} SIÈCLE

Q : Quels renseignements (p. ex. données et chiffres) permettraient de mieux comprendre les questions de cybersécurité au Canada? Veuillez expliquer votre réponse.

STIMULER LA CROISSANCE ET L'INNOVATION

Q : Quelles mesures pourraient être prises pour accroître la disponibilité, la pertinence et la qualité de la formation sur la cybersécurité?
Q : Que faut-il pour améliorer l'innovation dans le domaine de la cybersécurité au Canada?

Prochaines étapes relatives à la cybersécurité au Canada

PRINCIPAUX CHAMPS D'ACTION

Le Canada sera guidé par ses principes en matière de cybersécurité dans les trois champs d'action présentés ci-dessous. Des initiatives prospectives pour une intervention nationale en matière de cybersécurité sont décrites sous chaque champ d'action.

RÉSILIENCE

Ce champ d'action serait axé sur les éléments essentiels de la résilience cybernétique, ce qui comprend la prévention et l'atténuation des cyberattaques évoluées contre les institutions et les systèmes canadiens, et l'intervention en cas de cyberattaque, ainsi qu'une plus grande mobilisation du public en matière de cybersécurité.
Exemples

- Délivrer des attestations aux entreprises qui respectent des normes, des lignes directrices ou des cadres de pratiques exemplaires reconnus en matière de cybersécurité.
- Encourager les cadres supérieurs du secteur privé à présenter à leur conseil d'administration des bilans sur la cybersécurité au sein de leur organisation.
- Sensibiliser davantage la population à l'égard des cybermenaces et des mesures que peuvent prendre les Canadiens et les entreprises pour se protéger.

COOPÉRATION ET CAPACITÉ

Ce champ d'action serait axé sur la collaboration aux fins de l'acquisition des compétences, des ressources et des outils nécessaires pour assurer une cybersécurité efficace au Canada.

Exemples

- Donner la formation et le perfectionnement requis pour constituer les effectifs de cybersécurité de l'avenir grâce à une collaboration entre les gouvernements, le milieu universitaire et le secteur privé.
- Élaborer de nouveaux programmes d'études secondaires pour former une génération de Canadiens maîtrisant bien la technologie.
- Créer un centre national de coordination de la lutte contre la cybercriminalité qui serait chargé du triage, de l'établissement des priorités et de la coordination relativement aux enquêtes sur la cybercriminalité des différentes administrations.
- Soutenir l'échange de renseignements au sein du secteur privé.

CYBERINNOVATION

Ce champ d'action serait axé sur des initiatives qui permettraient aux gouvernements, aux entreprises et aux citoyens canadiens de prévoir les tendances, de s'adapter à un environnement changeant et de demeurer à la fine pointe de l'innovation en matière de cybersécurité.

Exemples

- Élaborer une stratégie de collecte et d'analyse de données pour générer de l'information sur les tendances en matière de cybersécurité et effectuer des analyses de données approfondies pour comprendre ces tendances et cerner les lacunes et les possibilités.

- Fournir un soutien collaboratif pour la recherche et le développement en cybersécurité, y compris des projets dans des domaines de pointe comme l'informatique quantique, l'impression 3D et la réalité virtuelle.
- Établir des partenariats public-privé pour créer des centres d'innovation en matière de cybersécurité.

Veuillez formuler vos commentaires sur ces champs d'action et les exemples d'initiatives connexes. Veuillez également proposer d'autres initiatives qui, selon vous, pourraient accroître la cybersécurité au Canada.