Une voie d'entrée à la cybersécurité pour le secteur d'aide à l'établissement des nouveaux arrivants

CENTRE CANADIEN POUR LA RÉSILIENCE NUMERIQUE DES ORGANISMES SANS BUT LUCRATIF

Nous travaillons pour créer un secteur à but non lucratif au diapason de l'ère numérique pour que les organismes canadiens puissent utiliser les données et la technologie pour réaliser leur mission et multiplier l'impact de leur travail. Joignez-vous à nous!

ccndr.ca

Crédits

Auteur :

Jason Shim

Responsable de production :

Émilie Pontbriand

Conception graphique :

Elaine Stam, Universe Design Studio

Traduction :

Cornelia Schrecker

Remercions

Nous remercions Mastercard Changeworks™ pour son soutien à la réalisation du projet.

ISBN: 978-1-55401-445-3

Publié en octobre 2024

Table des matières

Introduction 1

Cybersécurité : l'état actuel 3

- L'importance de la cybersécurité dans le secteur d'établissement 5
- Pourquoi une voie d'entrée à la cybersécurité? 6
- Ampleur et limites de l'initiative 7
- Cadre règlementaire et exigences de conformité 7

Évaluation des besoins 9

- Entrevues avec des parties prenantes et sondages 9
- Évaluation de la cybersécurité dans le cadre du processus d'établissement 9

Voie d'entrée à la cybersécurité 11

- 1re étape : Évaluer les risques 11
- 2e étape : Développer un plan de cybersécurité 12
- 3e étape : Obtenir l'approbation du conseil d'administration 12
- 4e étape : Mettre en œuvre le plan de cybersécurité 13
- 5e étape : Communauté et partage des connaissances 13

Prochaines étapes 14

- Résumé des principaux résultats et recommandations 14
- Perspectives et évolution de l'initiative La voie d'entrée à la cybersécurité 15

Annexes 16

- Annexe A : Participant.e.s au projet 16
- Annexe B : Analyse environnementale 18
- Annexe C : Autres normes 23

Introduction

Au début de 2023, le Centre canadien pour la résilience numérique des organismes sans but lucratif (CCNDR) a publié le rapport *Building the Cybersecurity and Resilience of Canada's Nonprofit Sector: A Vision and Strategy for the Sector* (*en anglais*). Ce rapport présente la synthèse de l'expertise et des expériences d'un groupe de travail formé dans le but de discuter de la cybersécurité dans le secteur des organismes à but non lucratif (OBNL) et de proposer des solutions aux défis cernés. Il propose la vision suivante : chaque OBNL canadien a les outils nécessaires pour réaliser sa mission en toute sécurité et pour protéger son organisation et ses bénéficiaires contre les cyberattaques. De plus, il recommande une stratégie pansectorielle pour relever les défis en matière de cybersécurité. Cette stratégie a entre autres objectifs celui d'offrir aux OBNL « une voie d'entrée accessible à la cybersécurité, à commencer par une évaluation des risques pertinente axée sur des mesures préventives et circonscrites, selon le niveau de maturité. » [*traduction libre*]

Le rapport propose de créer et de tester d'abord cette voie d'entrée pour le secteur d'aide à l'établissement des nouveaux arrivants. Ce dernier est composé d'organismes qui fournissent des services et du soutien aux populations immigrantes et réfugiées, notamment de l'interprétation; des cours de langue; de l'aide à la recherche d'emploi, à l'inscription aux services de garde et à la préparation de formulaires et de demandes; ainsi que de la réorientation vers d'autres programmes et services communautaires[1].

Chaque OBNL canadien a les outils nécessaires pour réaliser sa mission en toute sécurité et pour protéger son organisation et ses bénéficiaires contre les cyberattaques.

1 Etablissement.Org (2022), "Que sont les services d'établissement ?" https://etablissement.org/ontario/immigration-et-citoyennete/arrivee-et-etablissement/arriver/en-quoi-consistent-les-services-d-etablissement.

En raison de la nature de leur travail, les organismes d'établissement possèdent une quantité considérable de renseignements personnels et confidentiels. De plus, leurs bailleurs de fonds gouvernementaux leur imposent des normes minimales en matière de cybersécurité et de protection des données. Un cyberincident aurait des effets importants sur la prestation de services aux nouveaux.elles arrivant.e.s, compromettrait le financement de l'organisme et minerait la confiance des client.e.s envers l'organisme pendant une période particulièrement sensible de leur arrivée au pays.

La concrétisation de cette proposition a mené à l'initiative « Une voie d'entrée à la cybersécurité », puis à la mise sur pied d'un comité directeur. Ce dernier réunissait des participants provenant d'OBNL, des spécialistes en développement de capacités dans les OBNL, des expert.e.s et fournisseurs en matière de cybersécurité, en plus de chercheurs.euses[2]. Une analyse environnementale des normes et ressources en matière de cybersécurité a été réalisée pour orienter le développement initial du prototype de la voie d'entrée. S'y sont greffés des renseignements tirés d'entrevues avec les membres du comité directeur et des membres du milieu des OBNL et de la cybersécurité. Ces renseignements ont également été utilisés pour la préparation du présent rapport. Enfin, le comité directeur a fourni des commentaires au sujet du rapport et du prototype proposé.

En priorité, l'initiative « Une voie d'entrée à la cybersécurité » cherchait à répondre à la question suivante : « comment pouvons-nous éviter le sentiment de surcharge exprimé par les dirigeant.e.s d'OBNL et leur offrir une voie d'entrée à la cybersécurité des organismes? ». Bien que la voie d'entrée ait été développée pour le secteur d'établissement, nous croyons que tout organisme qui suit cette voie sera en meilleure position pour élaborer un plan de cybersécurité fondé sur les risques et pour gérer efficacement les plus importants parmi eux. Qui plus est, au fil du temps, la définition et l'adoption continues de mesures élémentaires amélioreront la cybersécurité collective du secteur.

2 L'annexe A comprend une liste des participant.e.s.

Cybersécurité : l'état actuel

Depuis quelque temps, la fréquence et la virulence accrues des cyberincidents attirent l'attention, et les institutions au cœur de la confiance du public n'y échappent pas. De nombreux OBNL[3] ont été la cible de cyberattaques, y compris des bibliothèques publiques[4,5], des établissements postsecondaires[6,7] et des hôpitaux[8]. Les reportages à ce sujet dans les médias, en plus des exigences de cybersécurité imposées par les bailleurs de fonds et les assureurs, ont fait de la cybersécurité et de la conformité des sujets de première préoccupation dans le secteur des OBNL.

Bien que les OBNL soient nombreux à se préoccuper des risques de cybersécurité, c'est loin d'être le cas pour tous. Selon l'*Enquête canadienne sur les entreprises*, au milieu de 2024, plus d'un quart (28 %) des OBNL affirmaient prévoir prendre des mesures de cybersécurité nouvelles ou supplémentaires au cours de la prochaine année[9]. Toutefois, près de la moitié d'entre eux (47 %) disaient ne pas en prévoir et un quart (25 %), ne pas savoir. Parmi les organismes n'ayant pas de plans en ce sens, 48 % pensaient que ce n'était pas nécessaire, 36 % avaient déjà adopté des mesures et 15 % nommaient les coûts comme obstacle.

3 Gandhi, S. (21 mars 2023, A "huge number" of non-profits have been victims of cyberattacks, risking the data of vulnerable groups, according to a new working group, Future of Good.
4 Radio Canada (7 novembre 2023), Un rançongiciel à l'origine de la paralysie de services à la Bibliothèque de Toronto.
5 CBC News (4 mars 2024), London library 'almost fully recovered' from ransomware attack, CEO says.
6 CBC News (1er juin 2023), University of Waterloo investigates suspected ransomware attack on email server.
7 Radio Canada (21 février 2024), L'Université Laurentienne se remet d'un incident touchant ses services informatiques
8 Radio Canada (7 novembre 2023), Cyberattaque : 270 000 patients et employés d'hôpitaux ontariens touchés
9 Statistique Canada, L'entreprise ou l'organisme prévoit prendre de nouvelles mesures de cybersécurité ou prendre des mesures supplémentaires au cours des 12 prochains mois, troisième trimestre de 2024.

*Le manque de connaissances parmi les OBNL contribue aux cyberrisques. **Selon l'Enquête canadienne sur la cybersécurité et le cybercrime 2021, seulement 10 % des OBNL avec 10 employé.e.s ou plus connaissent des normes de cybersécurité***

Le manque de connaissances parmi les OBNL contribue aux cyberrisques. Selon l'*Enquête canadienne sur la cybersécurité et le cybercrime 2021*, seulement 10 % des OBNL avec 10 employé.e.s ou plus connaissent des normes de cybersécurité[10]. Le *Sondage sur les compétences numériques 2023* de CanaDon révèlait que seulement 23 % des organismes utilisent un outil de gestion des mots de passe et qu'à peine 18 % d'entre eux exigent de suivre régulièrement des formations en cybersécurité[11]. De plus, 12 % des répondant.e.s affirmaient ne prendre aucune des mesures présentées dans le sondage pour protéger leur organisation contre les cyberattaques.

Lors d'un sondage réalisé dans le cadre d'un webinaire sur la cybersécurité co-organisé par CCNDR plus tôt cette année, nous avons posé la question suivante aux participant.e.s issu.e.s du milieu des OBNL : « quels défis votre organisation a-t-elle rencontrés dans le développement et la mise en œuvre d'une approche ou de normes de cybersécurité? ». Les répondant.e.s ont alors nommé le manque de ressources financières et humaines pour développer une approche en cybersécurité (58 %) et le manque d'information pour se lancer (49 %) comme principaux défis[12]. Ces résultats sont appuyés par des données de Statistique Canada, qui montrent que 39 % des OBNL n'ayant pas d'employés affectés régulièrement à des tâches liées à la cybersécurité indiquent que la principale raison est un manque de ressources[13].

10 Statistique Canada (2021), *Enquête canadienne sur la cybersécurité et le cybercrime*. Données sur les OBNL fournies à Imagine Canada. L'enquête ne tient compte que des organismes et entreprises avec 10 employé.e.s ou plus.

11 CanaDon (2023), How Digital Are Canadian Charities Now? Digital Skills Survey Results.

12 Institut Tamarack (19 janvier 2024), sondage à propos des stratégies de cybersécurité présentée durant le webinaire « Cybersecurity – Building a proactive approach. »

13 Statistique Canada (2021), *Enquête canadienne sur la cybersécurité et le cybercrime*.

Les obstacles relevés par les OBNL dans leurs efforts d'améliorer leur cybersécurité mettent en évidence la nécessité d'offrir des ressources qui les aident à définir leurs priorités et une approche systémique en matière de cybersécurité. Ces ressources leur permettraient d'avancer et d'éviter le sentiment de surcharge vécu par leurs dirigeant.e.s.

L'importance de la cybersécurité dans le secteur d'établissement

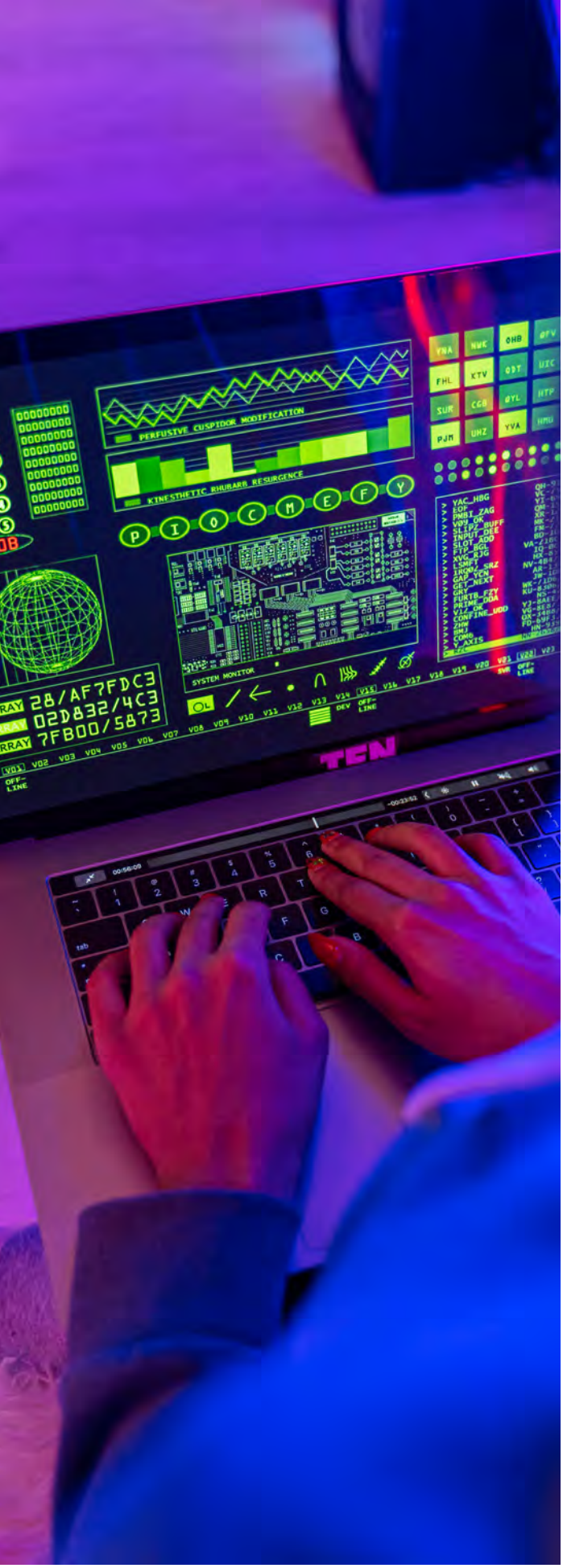
Les organismes d'établissement, tout comme les autres OBNL, rencontrent essentiellement les mêmes problèmes sur le plan de la cybersécurité que d'autres organisations canadiennes. Or, certains enjeux distinguent le secteur. Ainsi, les fonds assortis de conditions peuvent rendre difficile le financement de besoins opérationnels continus, comme ceux associés à la cybersécurité. Des fonds restreints liés à des projets particuliers et peu flexibles peuvent contribuer à des difficultés budgétaires et compromettre la viabilité d'efforts en matière de cybersécurité. En outre, la nature de leur travail amène beaucoup d'OBNL à acquérir et à traiter des renseignements personnels confidentiels et identifiables au sujet de leurs client.e.s.

La cybersécurité est aussi un sujet important pour les nouveaux.elles arrivant.e.s. Une analyse produite par des chercheurs.euses de l'Université métropolitaine de Toronto de données publiées par Statistique Canada a montré que « [l]es immigrant.e.s… qui utilisaient des médias sociaux étaient environ 2,3 fois plus susceptibles que les autres de trouver un emploi. Ceux.celles qui utilisaient l'Internet aux fins de formation ou de recherche d'emploi l'étaient deux fois plus[14]. » Pourtant, les membres de ce groupe sont nombreux à s'inquiéter de la cybersécurité. En 2018, 13 % de la population immigrante disaient ne pas utiliser les médias sociaux pour des raisons de sécurité ou de confidentialité. Parmi les personnes immigrantes ayant utilisé les médias sociaux dans les trois mois précédents, 26 % avaient reçu des communications frauduleuses et 7 % avaient été la cible d'une attaque par rançongiciel[15]. Cette réalité souligne l'importance pour les organismes d'établissement de limiter le plus possible la possibilité d'une brèche de cybersécurité.

[L]es immigrant.e.s… qui utilisaient des médias sociaux étaient environ 2,3 fois plus susceptibles que les autres de trouver un emploi. Ceux.celles qui utilisaient l'Internet aux fins de formation ou de recherche d'emploi l'étaient deux fois plus.

14 Monteriro, S. (2022), Social media and internet usage rates on employment outcomes among newcomers in Canada, p. 1.

15 Monteriro, S. (2022), Social media and internet usage rates on employment outcomes among newcomers in Canada, p. 7-8.



Pourquoi une voie d'entrée à la cybersécurité?

Le rapport sur la cybersécurité publié par le CCNDR en 2023 soulevait plusieurs défis liés à la cybersécurité dans les OBNL, dont le manque de connaissances sur les cyberrisques, et l'incertitude relativement aux responsabilités légales fondamentales et de conformité[16]. Toujours selon le rapport, peu d'organismes savent que la sécurité et la confidentialité des données comptent parmi les exigences opérationnelles de base. Les données de l'*Enquête canadienne sur la cybersécurité et le cybercrime* de Statistique Canada viennent confirmer ces constats en révélant que 89 % des OBNL avec 10 employé.e.s ou plus ne connaissent aucune norme de cybersécurité ni aucun programme de certification[17].

La voie d'entrée à la cybersécurité se veut un modèle et une ressource pour aider les dirigeant.e.s d'organismes d'établissement et d'OBNL d'autres sous-secteurs à gérer et à évaluer les mesures initiales à prendre. Ces mesures permettraient d'améliorer la cybersécurité de leur organisation et d'atténuer les principaux cyberrisques.

16 Centre canadien pour la résilience numérique des organismes sans but lucratif (2023), Building the Cybersecurity and Resilience of Canada's Nonprofit Sector.

17 Statistique Canada (2021), Enquête canadienne sur la cybersécurité et le cybercrime.

Ampleur et limites de l'initiative

L'initiative « La voie d'entrée à la cybersécurité » visait à développer une voie d'entrée à la cybersécurité pour les organismes d'établissement, qui offrirait un niveau élémentaire de connaissances, de formations et de préparation. Le public cible est composé de cadres et de leurs conseillers.ières dans des organismes ayant des capacités internes limitées ou un accès restreint à l'expertise en matière de cybersécurité, et qui cherchent un point de départ pour passer à l'action. D'éventuelles futures phases de l'initiative pourraient développer cette base en proposant d'autres mesures et des normes plus avancées en matière de cybersécurité.

L'initiative « La voie d'entrée à la cybersécurité » *visait à développer une voie d'entrée à la cybersécurité pour les organismes d'établissement, qui offrirait un niveau élémentaire de connaissances, de formations et de préparation.*

Cadre règlementaire et exigences de conformité

Dans le cas des organismes d'établissement, la conformité en matière de cybersécurité relève des ententes de contributions signées avec Immigration, Réfugiés et Citoyenneté Canada (IRCC). La *Loi sur la protection des renseignements personnels* du Canada impose des exigences légales à IRCC et, par extension, aux bénéficiaires de fonds par le biais des ententes de contribution. Ces exigences doivent garantir la mise en place de normes de sécurité et de confidentialité pour protéger les renseignements personnels des client.e.s.

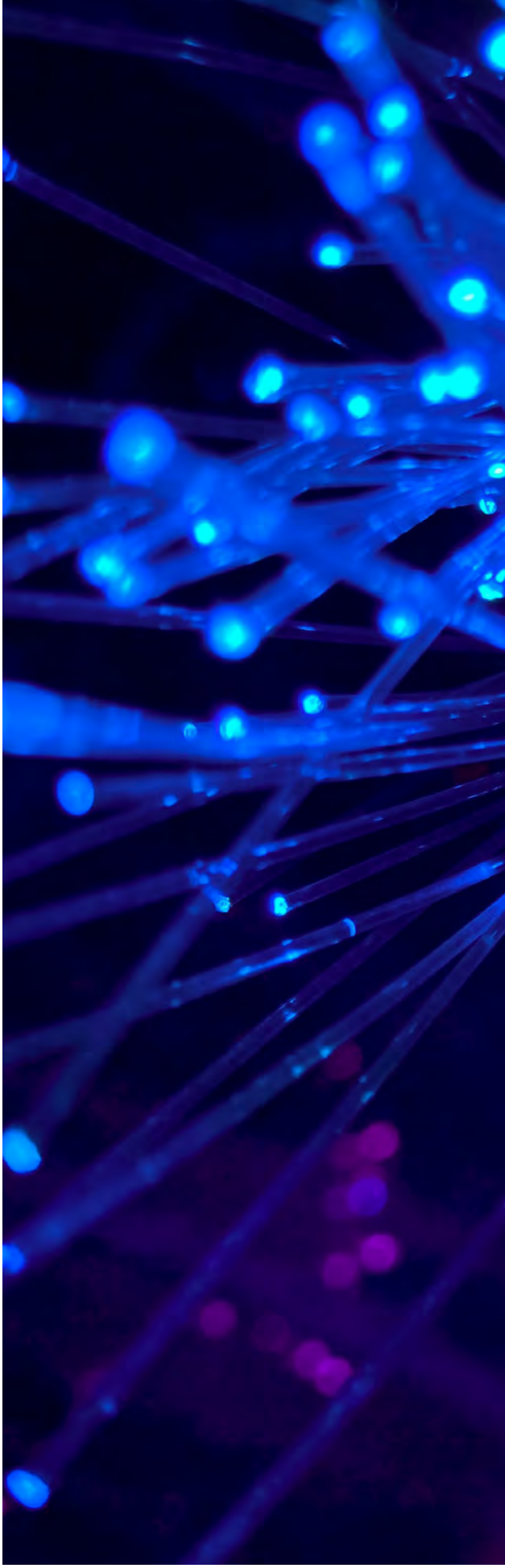
Les lignes directrices fournies par IRCC comprennent une liste de contrôle des exigences minimales relatives à la sécurité (EMS) à remplir par quiconque souhaite accéder à l'environnement de déclarations d'ententes de contribution (iEDEC). La liste de contrôle EMS est un élément incontournable du processus de déclaration. Les organismes qui ne répondent pas à toutes les exigences dès le début « doivent prendre les mesures requises pour améliorer les conditions de sécurité, et fournir des mises à jour à IRCC, afin de se conformer aux exigences non respectées… [et] doivent soumettre un formulaire EMS mis à jour lorsque les mesures auront été prises permettant de répondre à l'ensemble des exigences[18]. » *[traduction libre]*

18 Immigration, Réfugiés et Citoyenneté Canada (2020), Privacy and Security Requirements for Funding Recipients, p. 8.

La liste de contrôle EMS comprend des exigences de sécurité concernant les aspects suivants :

- Pare-feu
- Logiciels antivirus/antimaliciel
- Correctifs de sécurité
- Paramètres de sécurité
- Navigateurs Web
- Protection des mots de passe et verrouillage
- Clés USB et périphériques de stockage portables
- Services de stockage et serveurs infonuagiques
- Réseau sans fil
- Courriel
- Détection des intrusions
- Inspection du contenu

Outre IRCC, les compagnies d'assurance peuvent demander aux organismes de révéler les mesures prises en matière de cybersécurité. Leurs exigences varient en ampleur et complexité, à commencer par la confirmation de l'authentification multifacteur, les sauvegardes et la formation du personnel, jusqu'à des mesures plus exhaustives comme l'analyse des vulnérabilités, les tests d'intrusion et les cyberaudits[19].



19 Gandhi, S. et Oatley, G. (20 décembre 2023), Cybersecurity insurance growing in popularity after high-profile digital attacks. Does your organization need it?, *Future of Good*.

Évaluation des besoins

Entrevues avec des parties prenantes et sondages

Le comité directeur de la voie d'entrée à la cybersécurité a été formé en mai 2023. Il réunissait des représentant.e.s d'OBNL, des spécialistes en développement de capacités dans les OBNL, des expert.e.s et vendeurs en matière de cybersécurité, en plus de chercheurs.euses. Deux réunions du comité ont permis de rassembler des conseils et orientations qui, ensuite, ont contribué à la réalisation d'une analyse environnementale exhaustive des normes et ressources en matière de cybersécurité pour les organismes d'établissement[20].

L'analyse environnementale a contribué à la réflexion sur la possibilité pour le secteur d'adopter une norme ou un cadre en particulier. Dans la première moitié de 2024, des entrevues avec les membres du comité directeur et d'autres personnes ont été réalisées dans le cadre de la préparation du présent rapport.

Évaluation de la cybersécurité dans le cadre du processus d'établissement

L'analyse environnementale, combinée aux entrevues avec les membres du comité directeur et d'autres personnes, a permis de mettre au point les constats suivants :

- La plupart des normes et cadres de cybersécurité sont trop coûteux et trop complexes pour le personnel des OBNL, en plus de surcharger les organismes sans accès facile à de l'expertise en cybersécurité.
- Souvent, les organismes et les fournisseurs développent leurs propres cadres pour rendre les normes de cybersécurité complexes plus accessibles pour les OBNL.

20 Les résultats de l'analyse environnementale sont présentés dans l'annexe B.

- Le coût initial pour se conformer à des normes comme ISO 27001 (Organisation internationale de normalisation), CIS Critical Security Controls (Center for Internet Security), NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), ou SOC (Service and Organization Control) constitue une barrière pour beaucoup d'OBNL[21].
- Les OBNL ont besoin d'outils immédiats et accessibles qui les aident à réagir aux plus importants cyberrisques, tout en créant la base d'un plan à long terme pour une gestion efficace de tous les cyberrisques.

L'analyse s'est arrêtée sur deux ressources considérées comme des points de départ appropriés aux fins d'une voie d'entrée à la cybersécurité :

- Mesures de cybersécurité de base à l'intention des petites organisations (ITSAP.10.300)

  Le gouvernement canadien, par l'intermédiaire du Centre canadien pour la cybersécurité, publie ce guide dans la série de sensibilisation à la sécurité informatique (ITSAP). Le document ITSAP.30.100 propose une liste de mesures de cybersécurité recommandées pour aider à atténuer les principaux cyberrisques et servir de référence pour les OBNL.

- Contrôles de base de la cybersécurité pour les petites et moyennes organisations CAN/CIOSC 104:2021

  CAN/CIOSC104 est une norme nationale canadienne concernant les contrôles de base de la cybersécurité pour les petites et moyennes organisations. C'est le CIO Strategy Council, dorénavant connu comme Conseil de gouvernance numérique, qui a adopté la convention CAN/CIOSC. Cette norme en particulier peut servir de ressource d'entrée élémentaire et accessible pour les OBNL et les spécialistes en cybersécurité qui les accompagnent. Certain.e.s consultant.e.s en cybersécurité travaillent avec leurs propres cadres ou des normes comme CIS, NIST ou SOC, mais celles-ci dépassent généralement largement la norme CAN/CIOSC 104 élaborée pour les petites et moyennes organisations. Cette norme peut servir de point de départ de la voie d'entrée à la cybersécurité.

21 L'annexe C comprend plus d'information sur chacune de ces normes.

Voie d'entrée à la cybersécurité

La voie d'entrée à la cybersécurité comprend cinq étapes et utilise les normes ITSAP 30.100 et CAN/CIOSC 104 pour orienter l'évaluation et les étapes subséquentes.

1re étape : Évaluer les risques

Dans un premier temps, l'organisme réalise une évaluation des risques de base pour déterminer les lacunes et les aspects préoccupants. Idéalement, l'évaluation est entreprise par une personne se connaissant en cybersécurité, de concert avec les personnes connaissant bien l'organisme et son travail.

La première étape consiste à répondre au Questionnaire d'évaluation des risques de cybersécurité à l'annexe B de la norme Contrôles de base de la cybersécurité pour les petites et moyennes organisations CAN/CIOSC 104:2021. Si de l'expertise supplémentaire en cybersécurité est disponible à ce stade-ci, on recommande un examen complet de la norme CAN/CIOSC 104 pour évaluer l'existence de lacunes potentielles.

La norme Mesures de cybersécurité de base à l'intention des petites organisations (ITSAP.10.300) peut également servir de ressource.

Résultat de la 1re étape :
Une meilleure compréhension des principaux cyberrisques qui guettent l'organisme, et une liste des mesures de cybersécurité de base permettant d'atténuer ces risques.

2e étape : Développer un plan de cybersécurité

La prochaine étape de la voie d'entrée à la cybersécurité consiste à faire appel à un.e spécialiste en gestion de la cybersécurité pour réviser l'évaluation initiale et développer un plan et un échéancier pour la mise en œuvre des exigences de niveau 1 de la norme CAN/CIOSC 104[22]. Certains organismes peuvent compter sur l'expertise et les ressources disponibles à l'interne afin d'accomplir ce travail, tandis que d'autres doivent demander l'aide d'un.e consultant.e externe.

Résultat de la 2e étape :
Le développement d'un plan de cybersécurité, y compris des cibles et échéanciers, qui permettra d'atténuer les principaux cyberrisques et mettra l'organisme sur la voie d'améliorations continues de sa cybersécurité.

3e étape : Obtenir l'approbation du conseil d'administration

L'étape suivante consiste à obtenir l'adhésion du conseil d'administration de l'organisme par la présentation des cyberrisques mis en évidence par l'évaluation et du plan de cybersécurité proposé. La présentation doit se pencher sur les ressources requises pour la mise en œuvre du plan. Le conseil d'administration peut alors présenter, et approuver, une motion ou des politiques en lien avec le plan de cybersécurité. À cette étape, il est également opportun pour l'organisme de considérer l'ajout de connaissances en cybersécurité à la grille de compétences utilisée pour le recrutement d'administrateurs. trices.

Résultat de la 3e étape :
Adoption d'une motion ou d'une proposition budgétaire par le conseil d'administration pour la mise en œuvre du plan de cybersécurité.

22 Les exigences de niveau 1 s'adressent aux petites organisations qui font leurs débuts en cybersécurité. Généralement, ces organisations n'ont pas de ressources à investir dans les technologies d'information ou dans des services externes. Leurs connaissances de la cybersécurité sont considérées comme de base.

4e étape : Mettre en œuvre le plan de cybersécurité

Après l'approbation du plan de cybersécurité par le conseil d'administration, l'organisme entame la mise en œuvre du plan et son intégration aux cycles de planification. Si l'organisme manque de personnel ayant l'expertise nécessaire en cybersécurité pour voir à la mise en œuvre du plan, il devra collaborer avec un fournisseur de service crédible et fiable.

Résultat de la 4e étape :
Mise en œuvre du plan de cybersécurité de l'organisme, se traduisant par une cybersécurité améliorée.

5e étape : Communauté et partage des connaissances

La dernière étape implique la participation constante de l'organisme aux activités liées à la cybersécurité dans le milieu des OBNL, notamment sa participation à des formations continues et conférences ou séminaires, ainsi que le partage de connaissances avec d'autres organismes. L'engagement actif auprès de la communauté sur des questions de cybersécurité permet à l'organisme de rester à jour et de faire un travail de sensibilisation collectif quant à l'importance de maintenir une position forte en matière de cybersécurité.

Résultat de la 5e étape :
L'organisme participe activement à l'apprentissage et à l'échange de connaissances sur les tendances et développements en matière de cybersécurité qu'il pourra intégrer dans ses programmes pour maintenir une cybersécurité solide à mesure que l'environnement évolue.

Prochaines étapes

Résumé des principaux résultats et recommandations

Le présent rapport met en lumière certaines des difficultés vécues par les OBNL en matière de gestion des cyberrisques. Entre autres, il permet de comprendre que les normes existantes sont souvent trop complexes pour beaucoup d'organismes qui commencent tout juste à évaluer leur cybersécurité. Cette situation amène les dirigeant.e.s à se sentir surchargé.e.s et incertain.e.s quant à la marche à suivre.

Le rapport propose d'utiliser deux ressources accessibles comme points de départ : ITSAP.30.100 et CAN/CIOSC 104. Sur la base de ces ressources, le rapport présente une voie d'entrée à la cybersécurité en cinq étapes. Il recommande d'utiliser les exigences de niveau 1 de la norme CAN/CIOSC 104:2021 pour orienter l'évaluation initiale des organismes. À mesure que ces derniers augmentent leurs capacités et ressources, ils pourront renforcer davantage leur cybersécurité par l'adoption d'autres normes ou cadres, dont le *NIST Cybersecurity Framework*, les *CIS Critical Security Controls*, les rapports SOC, la norme ISO 27001 ou d'autres programmes, en fonction des besoins particuliers de leur organisation.

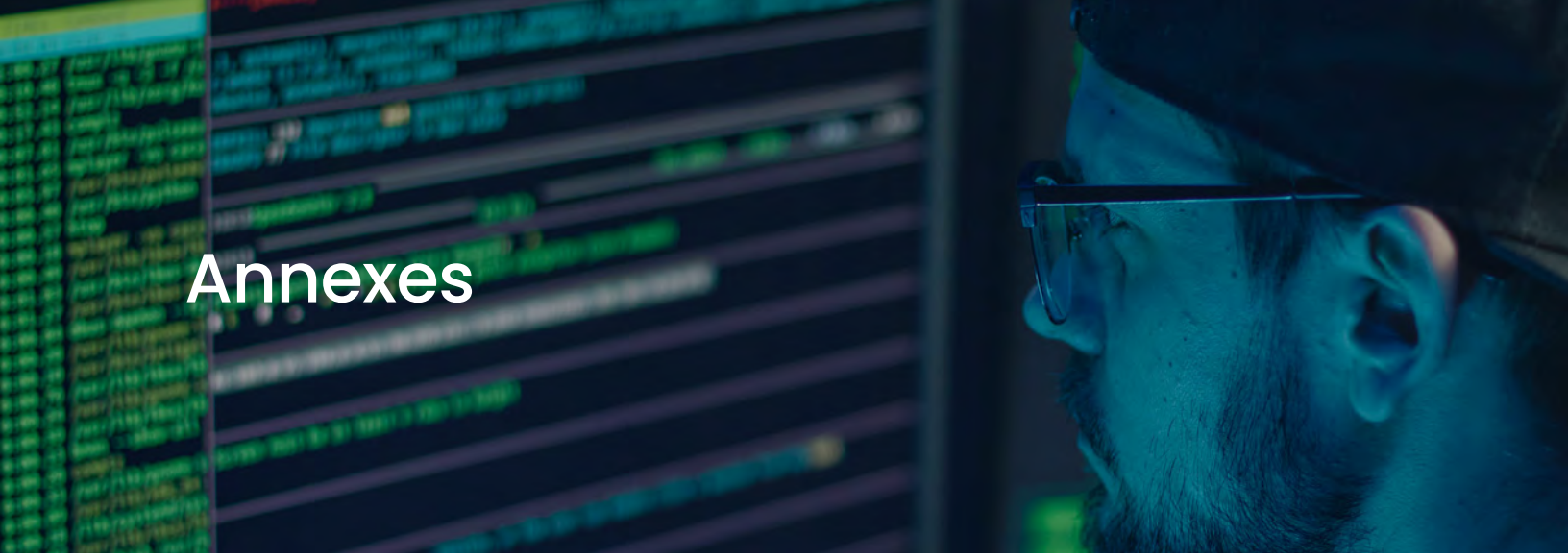
À mesure que ces derniers augmentent leurs capacités et ressources, ils pourront ***renforcer davantage leur cybersécurité par l'adoption d'autres normes ou cadres, dont le NIST Cybersecurity Framework, les CIS Critical Security Controls, les rapports SOC, la norme ISO 27001 ou d'autres programmes,*** *en fonction des besoins particuliers de leur organisation.*

Perspectives et évolution de l'initiative La voie d'entrée à la cybersécurité

Pour que la voie d'entrée à la cybersécurité devienne un succès à long terme, un écosystème de fournisseurs de services de cybersécurité sera nécessaire pour offrir aux OBNL un accès immédiat à une expertise fiable qui les guidera dans leurs efforts d'amélioration. Cet écosystème peut prendre la forme d'un marché de fournisseurs fiables, adapté aux besoins des OBNL, ou l'identification de fournisseurs présents dans le secteur qui ont une expertise en certification en cybersécurité.

Recommandations pour les dirigeant.e.s dans le secteur, les responsables politiques et les bailleurs de fonds :

- Continuer à travailler avec les parties prenantes pour les sensibiliser aux cyberrisques et promouvoir l'adoption d'une norme de cybersécurité de base commune.
- Explorer diverses possibilités pour faire évoluer et grandir la voie d'entrée à la cybersécurité, notamment par l'ajout d'information et de ressources offrant des pratiques et des renseignements pertinents en matière de cybersécurité.
- Fournir des ressources financières et un soutien constants, y compris des incitatifs, pour aider les organismes à mettre en place des mesures de cybersécurité efficaces.



Annexes

Annexe A : Participant.e.s au projet

Nous remercions les personnes suivantes de leur participation à l'initiative « La voie d'entrée à la cybersécurité » :

- Anthony Caldwell, Association des agences au service des immigrants de la région atlantique (ARAISA)
- Baijul Parikh, Ontario 211
- Cathy Barr, Imagine Canada
- Charles Buchanan, Technology Helps
- Chimene Emejuru, Lowase Management Consulting (USA)
- Darryl Kingston, Institut des normes de gouvernance numérique
- Hernan Popper, POPP3R Cybersecurity
- John Gilliam, Ontario Council of Agencies Serving Immigrants (OCASI)
- Karen Milligan, Ontario 211
- Kate Karn, Mastercard Canada
- Katie Gibson, Katie Gibson Consulting
- Kayode Olabisi, BDC
- Keith Jansa, Conseil de gouvernance numérique
- Liz Weaver, Institut Tamarack pour l'engagement communautaire
- Lyn Brooks, dHub Group
- Marco Campana, consultant indépendant
- Monika Freunek, Lighthouse Science Consulting and Technologies Inc.

- Nidhi Khanna, Skills for Change
- Nikki Hera, Office ontarien de réglementation de la gestion des condominiums
- Omar Yaqub, IslamicFamily
- Raj Rajakumar, IslamicFamily
- Randy Purse, conseiller principal, Formation et éducation en cybersécurité, Rogers Cybersecure Catalyst à l'Université métropolitaine de Toronto et consultant, Quantum Safe Canada
- Rashmi Sheth, North York Community House
- Victor Beitner, Cyber Security Canada
- Victor Cordon, Okta
- Wonders Pibowei, Lowase Management Consulting (Nigeria)

Annexe B : Analyse environnementale

Normes existantes pertinentes

- Conseil de gouvernance numérique et Institut de normes de gouvernance numérique :
  - Contrôles de base de la cybersécurité pour les petites et moyennes organisations
  - Sécurité centrée sur les données
- Centre canadien pour la cybersécurité :
  - Mesures de cybersécurité de base à l'intention des petites organisations
  - Utilisation de la gestion des biens de la technologie de l'information pour renforcer la cybersécurité
  - Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels
  - Choisir la solution de cybersécurité qui convient le mieux à votre organisation
  - Le Cadre des compétences en matière de cybersécurité du Canada (ITSM.00.039)
- Organisation internationale de normalisation - ISO
  - ISO/IEC 27001:2022 – Systèmes de management de la sécurité de l'information
  - ISO/IEC TS 27110:2021 – Lignes directrices relatives à l'élaboration d'un cadre en matière de cybersécurité
  - ISO 27701:2019 – Management de la protection de la vie privée
  - ISO 29100:2024 Technologies de l'information – Techniques de sécurité – Cadre privé
- Cadre de confiance pancanadien – Conseil canadien de l'identité et de l'authentification numériques (CCIAN)
- Rapport sur l'identité numérique - Conseil canadien de l'identité et de l'authentification numériques (CCIAN)
- Cybersecurity for Startups
- The National Institute of Standards and Technology (NIST) CSF v1.1 Cybersecurity Framework | NIST (Cadre des programmes et contrôles pour la sécurité de l'information. La version 2.0 du cadre est actuellement à l'étude et vaut la lecture)
  - Getting Started with NIST Cybersecurity Framework
- CIS Security Controls v8 CIS Center for Internet Security (Ressources, références et guides de mise en œuvre de contrôles de sécurité gratuits)
- CSA Cloud Control Matrix (CCM v4) (Guides et questionnaires gratuits pour les applications infonuagiques – applications SaaS)

Législation

- Règlement général sur la protection des données (RGPD)
- Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) (Canada)
- Parlement du Canada Projet de loi C-27 pour édicter la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données
- Parlement du Canada Projet de loi C-26 modifiant la Loi sur les télécommunications et édictant la Loi sur la protection des cybersystèmes essentiels
- PCI Data Security Standards (PCI DSS) – Normes de sécurité des données pour les paiements

Outils d'évaluation des risques existants

- Critical Security Controls Self Assessment Tool - Center for Internet Security CIS Controls Self Assessment Tool (CIS CSAT)
- Ransomware Business Impact Analysis CIS CSAT BIA Tool
- Guide de solutions en matière de cybersécurité pour votre organisation, Centre canadien pour la cybersécurité
- Cybersecurity Maturity Assessment for Small and Medium Enterprises, European Union Agency for Cybersecurity (ENISA)
- Tech Impact SecCheck
- D'autres offres de services de Tech Impact
- Global Cyber Alliance Sélection d'outils
- Ford Foundation Cybersecurity Assessment Tool (créé expressément pour des subventionnaires, partenaires subventionnés, organisations de la société civile et OBNL)
- « Normes » existantes imposées par des bailleurs de fonds, le gouvernement (IRCC), etc.
- IRCC's Privacy and Security Requirements for Funding Recipients - Immigration Contribution Agreement Reporting Environment
- Référence aux exigences de sécurité minimales iEDEC
- Droit à la vie privée et la transparence dans l'écosystème d'identité numérique au Canada, 2022 – Commissariat à la protection de la vie privée du Canada
- Sondage obligatoire sur la cybersécurité auquel les organismes prestataires de service doivent répondre – Enquête canadienne sur la cybersécurité et le cybercrime, 2022

- Les exigences canadiennes en matière de notification d'atteintes à la vie privée en un coup d'œil – Un résumé global des exigences respectives en matière de notification d'atteintes à la vie privée en vertu de la LPRPDE, la loi au Québec et la loi albertaine.

Formation et webinaires d'introduction

- Cybersecurity Training by Nonprofit Technology Enterprise Network (NTEN)
- Campagne de sensibilisation « Pensez cybersécurité » par le Centre canadien pour la cybersécurité
- Cours en cybersécurité offert gratuitement aux nouveaux.elles arrivant.e.s par Skills for Change (cohorte de juillet 2023)

Ressources de planification en matière cybersécurité

- Offres de Mastercard – créées pour les petites entreprises, mais avec une certaine pertinence pour les OBNL
  - Mastercard Trust Centre
  - Cybersecurity Assessment Quiz
- Centre canadien pour la cybersécurité :
  - Ressources de cybersécurité pour les petites et moyennes organisations
  - Guide sur les rançongiciels (ITSM.00.099)
  - Facteurs à considérer par les clients de services gérés en matière de cybersécurité
- Cyber Security Toolkit for Boards - La boîte à outils du NCSC aide les conseils d'administration à s'assurer que la cyberrésilience et la gestion des risques sont intégrées à l'échelle de l'organisation, y compris le personnel, les systèmes, le processus et les technologies.
- Cyber Readiness Institute - The Cyber Readiness Program

Formations et ressources en matière de cybersécurité offertes par des associations et réseaux professionnels

- Cyber Peace Builders - https://cyberpeaceinstitute.org/cyberpeace-builders/ - Aide gratuite en matière de cybersécurité, détection et analyse des menaces
- Canadian Institute for Cybersecurity, University of New Brunswick – Atelier de 4 jours sur la cybersécurité - https://www.unb.ca/cic/cybersecurity-101.html
- Secure and Responsible Tech Policy Foundations, Université métropolitaine de Toronto - https://www.cybersecurepolicy.ca/micro-credential-srtp
- Plateforme de formation en cybersécurité, CIRA - https://www.cira.ca/fr/cybersecurite/cybersecurity-awareness-training
- Analyste junior en cybersécurité, CISCO Skills for All https://www.netacad.com/fr/career-paths/cybersecurity?courseLang=fr-FR
- Formation en cybersécurité, CISCO Networking Academy https://www.netacad.com/fr/cybersecurity
- Formations en cybersécurité, Global Cyber Alliance (GCA) https://edu.globalcyberalliance.org/collections
- Cyber Readiness Program, The Cyber Readiness Institute https://programs.cyberreadinessinstitute.org/courses/cyber-readiness-program-change-behavior-be-cyber-ready
- Cyber Leader Program, The Cyber Readiness Institute https://programs.cyberreadinessinstitute.org/courses/cyber-leader-program
- Keep It Real Online, campagne de sensibilisation à la cybersécurité et au numérique, ministère des Affaires internes, gouvernement de la Nouvelle-Zélande - https://www.keepitrealonline.govt.nz/about-us/
- Simply Secure Knowledge Base - https://simplysecure.org/knowledge-base/
- (ISC)2 Certified in Cybersecurity preparation training (conçu pour se préparer à l'examen de certification, mais offre également une formation de base en cybersécurité autonome à toute autre personne)

Logiciel de formation en cybersécurité

- KnowBe4.com
- Mimecast Security Awareness Training | Awareness Training | Mimecast
- Cofense Knowledge Center | Cofense

Politiques, processus, guides et modèles en matière de sécurité de l'information

- Cadre de cybersécurité pour les OBNL
- 6 New Policy Templates to Help You Enact CIS Controls IG1
- Information Security Policy Templates | SANS Institute

Assurance cyberrisques

- Exemple de formulaire d'assurance cyberrisques
- Future of Good - Cybersecurity insurance growing in popularity after high-profile digital attacks. Does your organization need it?

Autres ressources

- UNESCO Un Internet de confiance
- Innovation concernant les bacs à sable, Institut des normes de gouvernance numérique
- Bias in Resilience, THINK Digital Partners England
- Ressources en cybersécurité, Autorité canadienne pour les enregistrements Internet
- Starter Kit, The Cyber Readiness Institute (Protégez votre organisation, vos client.e.s et votre bilan)
- GCA Cybersecurity Toolkit for Small Business, The Global Cyber Alliance
- Building the Cybersecurity and Resilience of Canada's Nonprofit Sector, Centre canadien pour la résilience numérique des organismes sans but lucratif
- Cybersécurité et nouvelles technologies, Bureau de lutte contre le terrorisme, Nations Unies

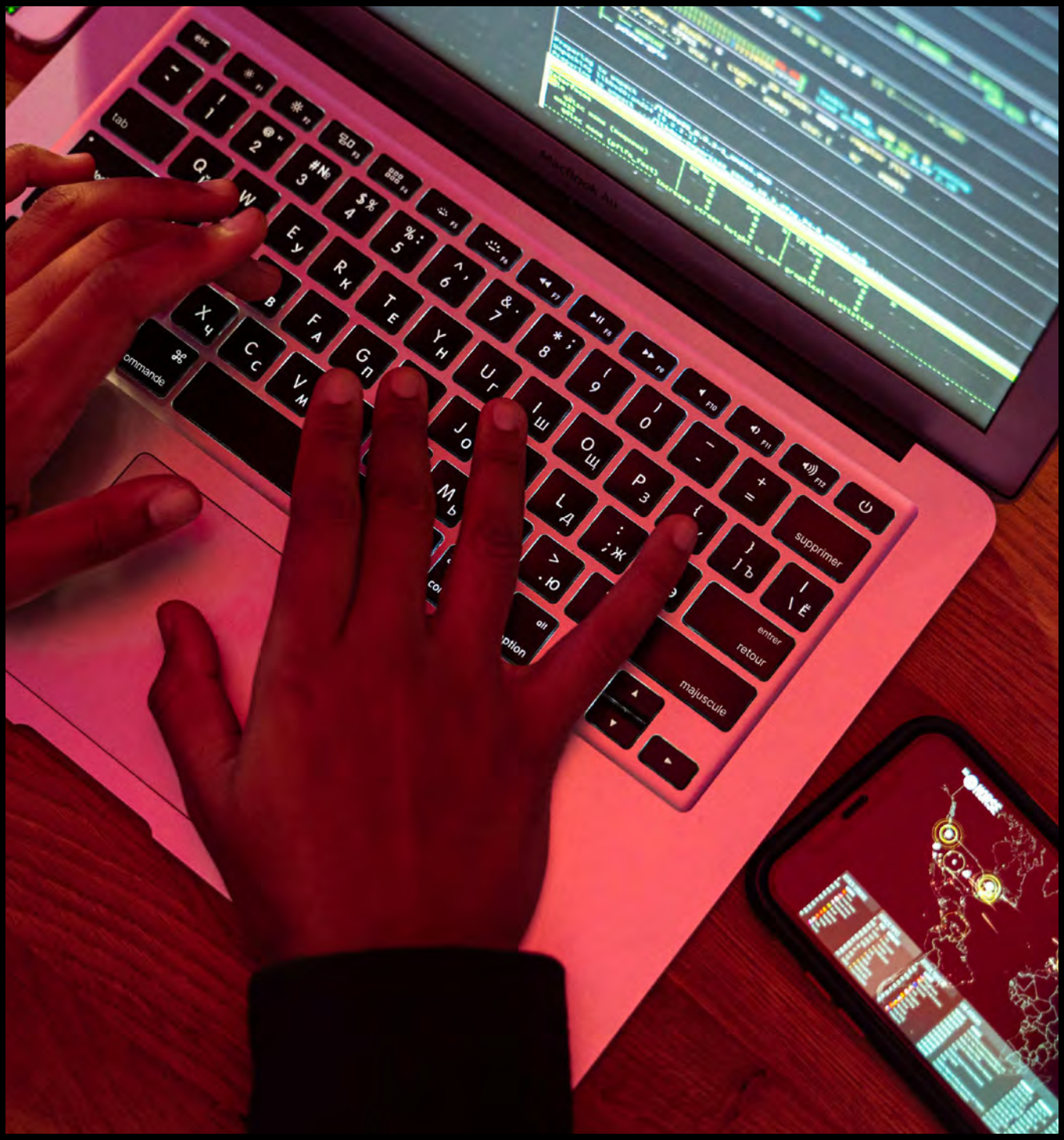
Annexe C : Autres normes

- **ISO 27001 :**
  Une norme internationale pour les systèmes de gestion de la sécurité de l'information, publiée par l'Organisation internationale de normalisation. La certification ISO 27001 requiert un audit par une entité de certification indépendante reconnue.

- **CIS Critical Security Controls :**
  Le Center for Internet Security (CIS) est un organisme à but non lucratif qui développe des contrôles de sécurité. Les *CIS Critical Security Controls* (CIS Controls) sont un ensemble de pratiques exemplaires prescriptives, simplifiées et présentées en ordre de priorité.

- **NIST Cybersecurity Framework :**
  Le National Institute of Standards and Technology (NIST) est une agence du ministère du Commerce des États-Unis. Le *NIST Cybersecurity Framework* (CSF) fournit de l'orientation aux organisations quant à la gestion de leurs cyberrisques et offre une taxonomie des résultats de haut niveau en matière de cybersécurité.

- **SOC :**
  Les *Systems and organization controls* (SOC) sont des rapports sur des contrôles dans les organisations, y compris la sécurité, la disponibilité et le traitement de données, ainsi que la confidentialité des systèmes. Le cadre de déclaration SOC a été développé par le American Institute of Certified Public Accountants (AICPA). Les rapports SOC sont préparés suivant une évaluation réalisée par un.e auditeur.trice indépendant.e.



CENTRE CANADIEN POUR LA RÉSILIENCE NUMERIQUE DES ORGANISMES SANS BUT LUCRATIF