A Cybersecurity On-Ramp for the Settlement Sector

CANADIAN CENTRE FOR NONPROFIT DIGITAL RESILIENCE

We're for a digitally enabled nonprofit sector, where Canada's diverse nonprofits use data and tech to advance their mission and multiply their impact. Join us!

ccndr.ca

Credits

Author:
Jason Shim

Production Manager:
Émilie Pontbriand

Design:
Elaine Stam, Universe Design Studio

French Translation:
Cornelia Schrecker

Acknowledgements

We are grateful to Mastercard Changeworks™ for their support of this work.

ISBN: 978-1-55401-445-3

Date published: October 2024

Contents

Introduction

In early 2023, the Canadian Centre for Nonprofit Digital Resilience released a report entitled *Building the Cybersecurity and Resilience of Canada's Nonprofit Sector: A Vision and Strategy for the Sector.* The report captured the knowledge and insights of a working group convened to discuss cybersecurity in the nonprofit sector and propose solutions to identified challenges. It presented the following vision: Every Canadian nonprofit is empowered to securely meet its mission and protect the organization and its beneficiaries from cyber threats. The report recommended a sector-wide strategy to address cybersecurity challenges. One of the strategy's objectives was that nonprofits have "an easy on-ramp to cybersecurity, beginning with a relevant risk assessment that prioritizes preventive, focused action at different maturity levels."

The report proposed prototyping the on-ramp with the settlement sector. This sector consists of organizations that provide services and support to immigrants and refugees. Services may include interpretation, language classes, help finding a job, help registering children for school, assistance filling out forms or applications, and referrals to other community programs and services.[1]

Every Canadian nonprofit is empowered to securely meet its mission and protect the organization and its beneficiaries from cyber threats.

1 Settlement.Org. (2022). "What are settlement services?" https://settlement.org/ontario/immigration-citizenship/landing-and-leaving/living-in-ontario/what-are-settlement-services/.

Given the nature of their work, settlement organizations possess a considerable amount of sensitive, personal information. In addition, their government funders require them to meet minimum cybersecurity and protection standards. A cybersecurity incident would significantly disrupt the delivery of services to newcomers, put the organization's funding at risk, and erode trust with clients during the sensitive period of settlement and integration.

The Cybersecurity On-Ramp Initiative was created to move this work forward. A Steering Committee was formed that included participants from nonprofits and nonprofit capacity-builders, cybersecurity experts, cybersecurity vendors, and academics.[2] A landscape scan of cybersecurity standards and resources was conducted to inform the initial development of the on-ramp prototype. Interviews with Steering Committee members and others in the nonprofit and cybersecurity communities were undertaken to further inform the development of the prototype and this report. The Steering Committee also provided feedback on this report and the proposed prototype.

The main goal of the Cybersecurity On-Ramp Initiative was to address the following question: "How can we remove the 'overwhelm' nonprofit leaders experience and provide an on-ramp to cybersecurity for organizations?" While the on-ramp was developed to meet the needs of the settlement sector, we believe that any organization that follows the on-ramp will be better positioned to develop a risk-informed cybersecurity plan and effectively manage critical cyber risks. Furthermore, over time, the ongoing identification and adoption of foundational cybersecurity actions will improve the collective cybersecurity of the sector.

2 A list of participants is presented in Appendix A.

Current Cybersecurity Landscape

Cybersecurity incidents have received more public attention recently due to their increasing frequency and severity. Institutions central to public trust and welfare have not been spared. Cyberattacks have impacted many nonprofits[3], including public library systems[4,5], post-secondary institutions[6,7], and hospitals[8]. Media reports of cyber incidents, along with increasing cybersecurity requirements from funders and insurance providers, have brought cybersecurity and compliance needs to the forefront in the nonprofit sector.

While many nonprofits are actively addressing cybersecurity risks, many are not. The Canadian Survey on Business Conditions found that, in mid-2024, over a quarter of nonprofits (28%) said they planned to take new or additional cybersecurity measures over the next year.[9] However, almost half (47%) said they didn't, and a quarter (25%) didn't know. Among those who didn't have plans to implement new or additional cybersecurity measures, 48% felt there was no need, 36% had already implemented measures, and 15% said cost was a barrier.

3 Gandhi, S. (2023, March 21). 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 CBC News. (2023, November 7). Ransomware attack behind Toronto Public Library service interruption, library says.

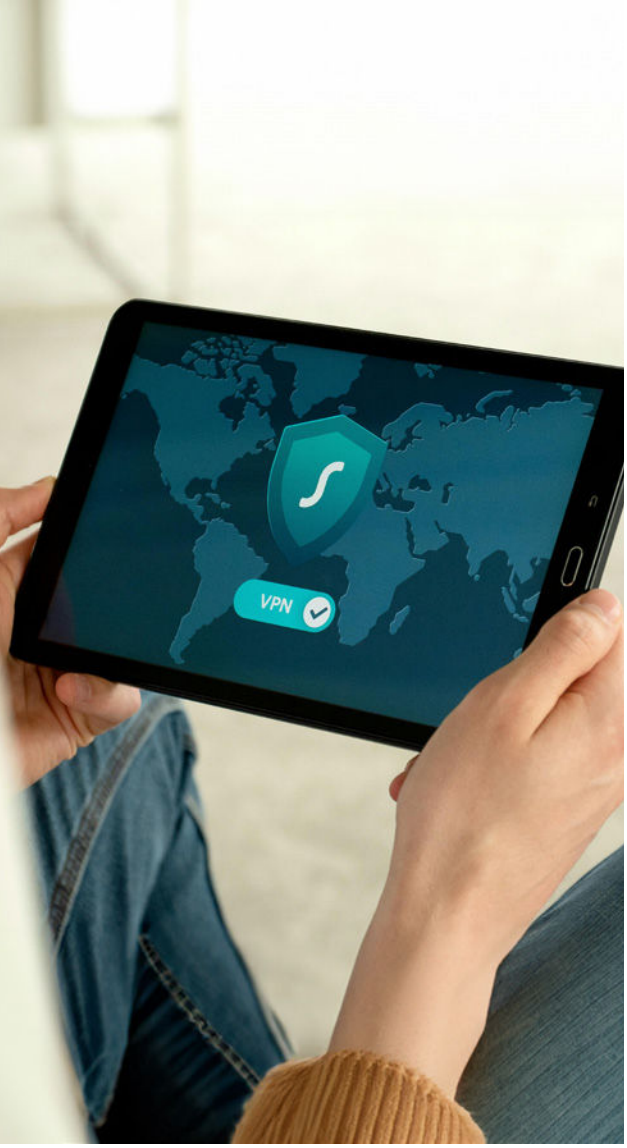
5 CBC News. (2024, March 4). London library 'almost fully recovered' from ransomware attack, CEO says.

6 CBC News. (2023, June 1). University of Waterloo investigates suspected ransomware attack on email server.

7 CBC News. (2024, February 22). Cyber incident shuts down Laurentian University's website, WiFi and email access.

8 CBC News. (2023, November 8). Southwestern Ontario hospitals will rebuild network from scratch amid fallout from cyberattack.

9 Statistics Canada. Table 33-10-0874-01. Business' or organization's plans to take any new or additional cybersecurity actions over the next 12 months, third quarter of 2024.



Lack of awareness among nonprofit organizations contributes to cyber risk. According to the 2021 Canadian Survey of Cyber Security and Cybercrime, ***only 10% of nonprofit organizations with ten or more staff are aware of cybersecurity standards.***

Lack of awareness among nonprofit organizations contributes to cyber risk. According to the 2021 Canadian Survey of Cyber Security and Cybercrime, only 10% of nonprofit organizations with ten or more staff are aware of cybersecurity standards.[10] CanadaHelps' 2023 Digital Skills survey found that just 23% of organizations are using a password management tool, and only 18% require regular participation in cybersecurity training.[11] Twelve percent of respondents reported taking none of the steps listed in the survey to protect their organizations from cyber threats.

In a poll conducted in a cybersecurity webinar co-hosted by CCNDR earlier this year, we asked participants from the nonprofit community, "What are the challenges that your organization has faced in developing and implementing a cybersecurity approach or standards?" The key challenges identified were a lack of financial or human resources to build a cybersecurity approach (58%) and a lack of information about where to begin" (49%).[12] These findings are supported by Statistics Canada data showing that 39% of nonprofits that have no employees with regular cybersecurity-related tasks report that the main reason is a lack of resources.[13]

10 Statistics Canada. (2021). Canadian Survey of Cyber Security and Cybercrime. Data for nonprofits provided to Imagine Canada. The survey only includes organizations and businesses with ten or more staff.

11 CanadaHelps. (2023). How Digital Are Canadian Charities Now? *Digital Skills Survey Results*.

12 Tamarack Institute. (2024, January 19). Poll on cybersecurity strategies presented during the webinar "Cybersecurity – Building a proactive approach."

13 Statistics Canada. (2021). Canadian Survey of Cyber Security and Cybercrime.

The challenges nonprofits face in improving their cybersecurity highlight the need for resources to help them identify key cybersecurity priorities and a systematic approach to move organizations forward and reduce the sense of 'overwhelm' that nonprofit leaders experience.

Importance of Cybersecurity in the Settlement Sector

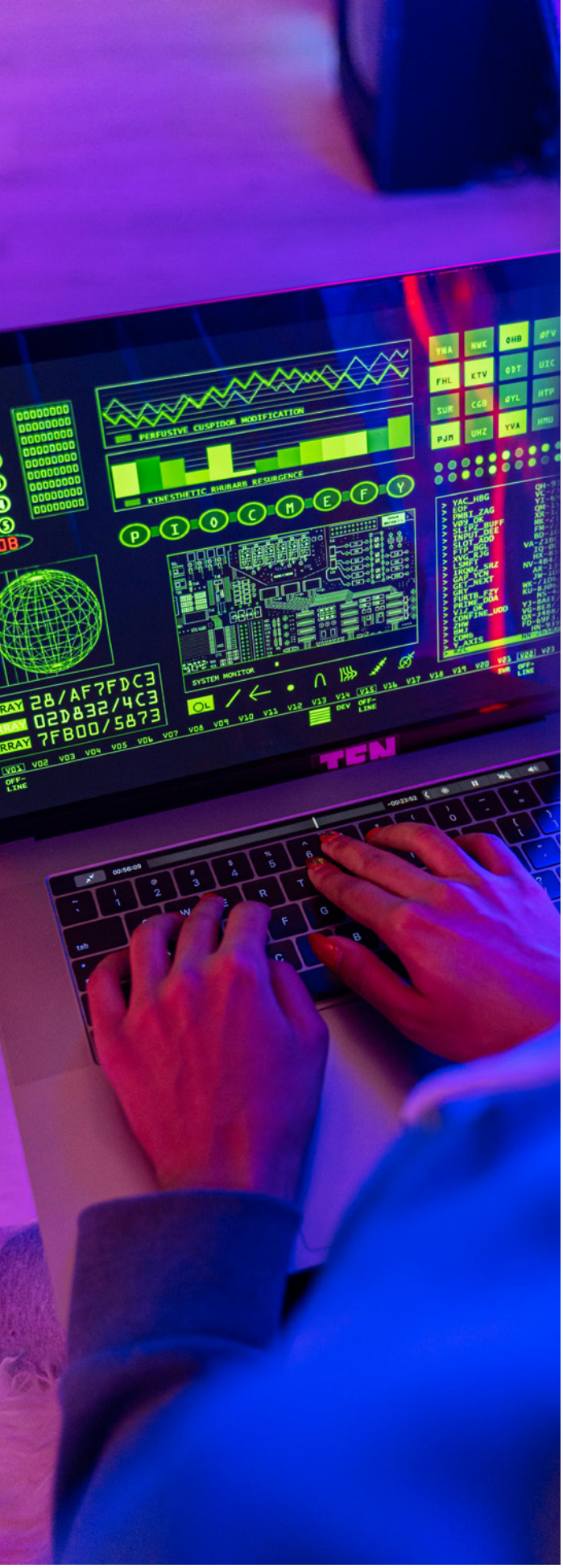
Many of the challenges related to cybersecurity encountered by settlement organizations—and other nonprofits—are similar to those experienced by other Canadian businesses. There are, however, issues unique to the nonprofit sector. For example, restricted funding can make resourcing ongoing operational needs, such as cybersecurity, challenging. Restricted funds tied to specific projects with little flexibility can create budgetary challenges and hinder the sustainability of long-term cybersecurity efforts. Due to the nature of their operations, many nonprofits also acquire and handle sensitive and personally identifiable information about their clients.

Cybersecurity is also important to newcomers. Analysis carried out by Toronto Metropolitan University researchers using Statistics Canada data found that "Immigrants . . . that used social media were about 2.3 times more likely to find employment, and those that used the internet for training purposes or to search for employment were about two times more likely to find employment."[14] Yet many newcomers are concerned about cybersecurity. In 2018, 13% of immigrants reported not using social media due to concerns about security or privacy. Among immigrants who had used social media regularly in the preceding three months, 26% had received fraudulent communications, and 7% had experienced a cyber-ransom attack.[15] This makes it especially important for settlement organizations to minimize the chance that they will experience a cybersecurity breach.

Immigrants that used social media were about 2.3 times more likely to find employment, *and those that used the internet for training purposes or to search for employment were about two times more likely to find employment.*

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, pp. 7-8.



Why a Cybersecurity On-Ramp?

CCNDR's 2023 cybersecurity report identified several challenges relating to cybersecurity and nonprofits, including the lack of awareness among many organizations of cyber risk, as well as uncertainty around basic legal and compliance responsibilities.[16] The report also noted that few nonprofits have data security and privacy on their radar as a basic operational requirement. These observations are supported by data from Statistics Canada's Survey of Cyber Security and Cybercrime, which found that 89% of nonprofits with 10 or more staff are not aware of any cybersecurity standards or certification programs.[17]

The cybersecurity on-ramp is intended to be a model and a resource for how leaders of settlement organizations, and other types of nonprofits, can manage and assess the initial actions needed to improve their organization's cybersecurity and mitigate critical cyber risks.

16 Canadian Centre for Nonprofit Digital Reslience. (2023). Building the Cybersecurity and Resilience of Canada's Nonprofit Sector.

17 Statistics Canada. (2021). Canadian Survey of Cyber Security and Cybercrime.

Scope and Limitations of the Initiative

The Cybersecurity On-Ramp Initiative focused on developing a basic cybersecurity on-ramp for settlement organizations that provides a foundational level of awareness, training and preparedness. The intended audience is senior decision-makers and their advisors in organizations with limited internal capacity or access to cybersecurity expertise, who need a starting point to move forward. Future phases of the initiative may build on this foundation by exploring additional cybersecurity measures and more advanced standards.

The Cybersecurity On-Ramp Initiative *focused on developing a basic cybersecurity on-ramp for settlement organizations that provides a foundational level of awareness, training and preparedness.*

Regulatory Framework and Compliance Requirements

For many settlement organizations, cybersecurity compliance is tied to contribution agreements with Immigration, Refugees and Citizenship Canada (IRCC). Canada's *Privacy Act* places legal requirements upon IRCC, which extend to funding recipients through their contribution agreements. These requirements ensure that security and privacy standards are put in place to protect personal client information.

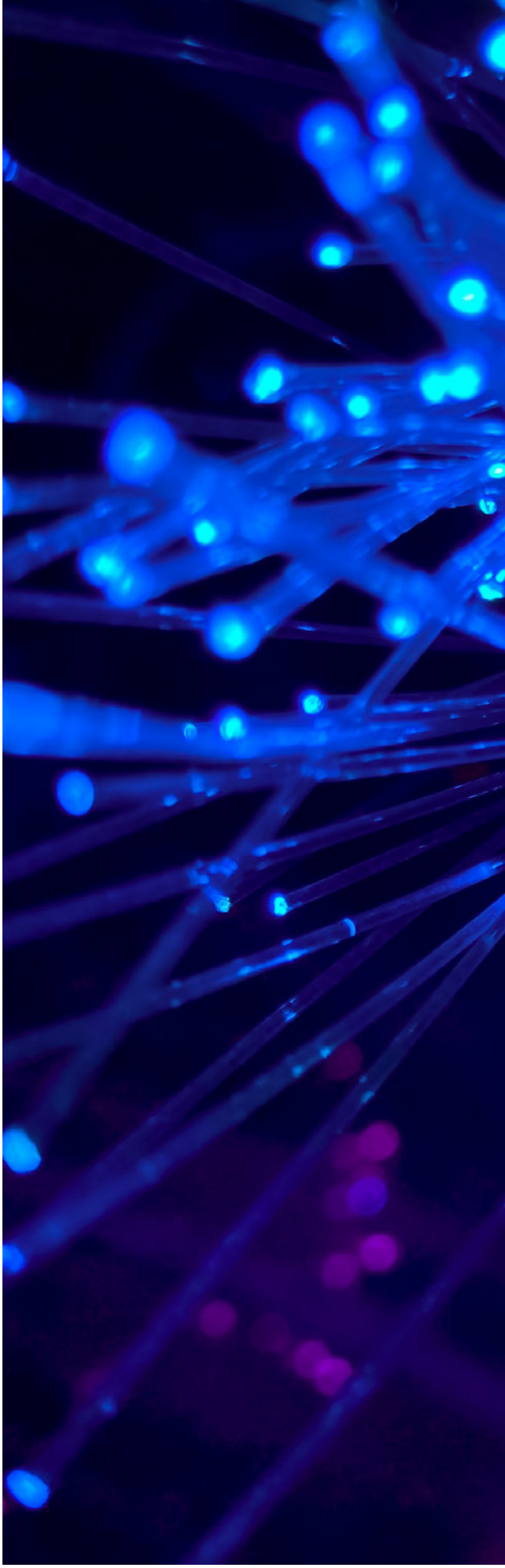
The guidelines provided by IRCC include a Minimum Security Requirements (MSR) Checklist that must be completed to access the Immigration Contribution Agreement Management Environment (iCARE). The MSR checklist is a mandatory component of the reporting process. Organizations that do not initially meet all security requirements are "required to take necessary actions to improve security conditions, as well as provide IRCC with updates, to address all outstanding security requirements . . . . [and] must submit an updated MSR when steps have been taken to meet all requirements."[18]

18 Immigration, Refugees and Citizenship Canada. (2020). Privacy and Security Requirements for Funding Recipients, p. 8.

The MSR checklist identifies security requirements in the following areas:

- Firewalls
- Anti-virus/anti-malware software
- Networks and networked computers
- Security patches
- Security settings
- Web browsers
- Password protection and lock
- USB keys and portable storage devices
- Cloud storage services and servers
- WiFi
- Email
- Intrusion detection
- Content inspection

In addition to the cybersecurity requirements of IRCC, insurance companies may also ask organizations to identify the cybersecurity measures they have taken. The cybersecurity requirements of insurance companies vary in comprehensiveness and complexity, from confirmation of multifactor authentication, backups, and employee training to more extensive measures that may include vulnerability scans, penetration tests, and cyber audits.[19]



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

Needs Assessment

Stakeholder Interviews and Surveys

The Cybersecurity On-Ramp Steering Committee was formed in May 2023 and included representatives from nonprofits and nonprofit capacity-builders, cybersecurity experts, cybersecurity vendors, and academics. Two meetings were held to gather advice, and guidance, which resulted in the development of a thorough landscape scan of cybersecurity standards and resources for settlement organizations.[20]

The landscape scan informed considerations of whether the sector could adopt a specific standard or framework. Interviews with Steering Committee members and others in the nonprofit and cybersecurity communities were undertaken in the first part of 2024 to further inform the development of this report.

Cybersecurity Assessment for Settlement Processes

The landscape scan, combined with interviews with Steering Committee members and others, produced the following key insights:

- Most existing cybersecurity standards and frameworks are too extensive and complex for nonprofit staff, and are often overwhelming to organizations that don't have ready access to cybersecurity expertise.
- Organizations and vendors often develop their own frameworks to make complex cybersecurity standards more accessible to nonprofits.

20 The results of the landscape scan are presented in Appendix B.

- The upfront costs to comply with standards such as ISO 27001 (International Organization for Standardization), CIS Critical Security Controls (The Center for Internet Security), NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), or SOC (Service and Organization Control) are a barrier for many nonprofits.[21]
- Nonprofits need something immediate and accessible that helps them address critical cyber risks while simultaneously providing the foundation for a longer-term plan that effectively manages all cyber risks.

Two resources were identified as useful starting points for the purposes of a cybersecurity on-ramp:

- Foundational cyber security actions for small organizations baseline cybersecurity controls for small organizations (ITSAP 30.100)

  The Canadian government, through the Canadian Centre for Cyber Security, publishes this guideline as an IT security awareness product (ITSAP). ITSAP30.100 provides a list of recommended cybersecurity actions intended to help to reduce key cyber risks and serve as an effective reference for nonprofit organizations.

- Baseline Cyber Security Controls for Small and Medium Organizations CAN/CIOSC 104:2021

  CAN/CIOSC104 is a Canadian national standard for baseline cybersecurity controls for small and medium organizations. The CAN/CIOSC convention was used by the CIO Strategy Council, now known as the Digital Governance Council. This standard may serve as a basic and accessible on-ramp resource for nonprofits and the cybersecurity experts with whom they work. Although there are cybersecurity consultants who employ their own custom frameworks, or other standards such as CIS, NIST, or SOC, these standards generally far exceed those of CAN/CIOSC 104, which is intended for small and medium organizations. The CAN/CIOSC 104 standard can serve as a basic starting point for the purposes of a cybersecurity on-ramp.

21 Further details about these standards are available in Appendix C

Cybersecurity On-Ramp

The Cybersecurity On-Ramp includes five steps and uses ITSAP 30.100 and CAN/CIOSC 104 to guide the assessment and subsequent actions.

Step 1: Risk Assessment

First, the organization will carry out a basic risk assessment to identify any gaps and areas of concern. Ideally, this will be conducted by someone familiar with cybersecurity in concert with those who are well informed about the business of the nonprofit.

The first step is to complete the Cyber Security Risk Assessment Questionnaire found in Annex of Baseline Cyber Security Controls for Small and Medium Organizations CAN/CIOSC 104:2021. If additional cybersecurity expertise is available at this stage, it is recommended that the full CAN/CIOSC 104 standard be reviewed in greater detail to assess where potential gaps may exist.

The Foundational cyber security actions for small organizations baseline cybersecurity controls for small organizations (ITSAP 30.100) may also be consulted as a resource.

Outcome of Step 1:
A clearer understanding of the organization's critical cyber risks and a list of basic cybersecurity actions that can be taken to mitigate the risks.

Step 2: Cybersecurity Plan Development

The next step in the cybersecurity on-ramp involves engaging a cybersecurity management expert to review the initial assessment and develop a plan and timeline for implementing the Level 1 requirements of CAN/CIOSC 104.[22] Some organizations may have internal expertise or resources to do this work internally; others may require the assistance of an external consultant.

Outcome of Step 2:
The development of a cybersecurity plan with targets and timelines that will reduce critical cyber risk and put the organization on the path of continuous cybersecurity improvement.

Step 3: Board Approval

The next step is to secure buy-in from the organization's board. This involves a presentation that outlines the cybersecurity risks identified in the assessment along with the proposed cybersecurity plan. The presentation should also outline the resources that are needed to implement the plan. Motions and/or policies related to the cybersecurity plan may be presented to, and approved by, the board at this step. The organization may also consider adding relevant cybersecurity knowledge to the skills matrix used for board member recruitment.

Outcome of Step 3:
A board resolution or budget proposal is passed, allowing the implementation of the cybersecurity plan.

22 Level 1 requirements are intended for smaller organizations that are just starting their cybersecurity journey. These organizations typically do not have the resources to invest in or outsource IT resources and their knowledge of cybersecurity would be considered entry-level.

Step 4: Cybersecurity Plan Implementation

Following the approval of the cybersecurity plan by the board, the organization will commence implementation of the plan and integration with their planning cycles. If the organization does not have staff with sufficient cybersecurity expertise to implement the plan, the organization will need to work with a credible, trustworthy cybersecurity vendor.

Outcome of Step 4:
The cybersecurity plan is successfully implemented, leading to improved cybersecurity for the organization.

Step 5: Community and Knowledge Sharing

The final step involves ongoing participation in broader cybersecurity activities within the nonprofit community. This may involve participating in ongoing training, engagement in conferences or seminars, and/or knowledge sharing with other organizations. By actively engaging with the broader community around cybersecurity issues and themes, organizations can stay up-to-date and collectively raise awareness of the importance of maintaining a strong cybersecurity posture.

Outcome of Step 5:
The organization is active in learning and sharing knowledge around ongoing cybersecurity trends and developments that they can integrate into their program, allowing them to sustain effective cybersecurity as the landscape changes.

Next Steps

Summary of Key Findings and Recommendations

This report highlights some of the key challenges that nonprofit organizations face when it comes to addressing cybersecurity risks. A key finding is that many existing standards are too complex for many organizations that are just beginning to assess their cybersecurity, leading leaders to feel overwhelmed and uncertain of where to begin.

This report identifies two accessible resources as starting points: ITSAP 30.100 and CAN/CIOSC 104. Using these resources, it presents a five-step Cybersecurity On-Ramp. It is recommended that the Level 1 requirements of CAN/CIOSC 104:2021 be used to guide the organization's initial assessment. As organizations continue to grow in their capabilities and resourcing, they may explore further strengthening their cybersecurity posture through the adoption of additional standards or frameworks such as the NIST Cybersecurity Framework, CIS Critical Security Controls, SOC, ISO 27001, or programs based on their unique organizational needs.

*As organizations continue to grow in their capabilities and resourcing, they may explore **further strengthening their cybersecurity posture through the adoption of additional standards, frameworks or programs** based on their unique organizational needs.*

Future Outlook and Evolution of the Cybersecurity On-Ramp Initiative

For the Cybersecurity On-Ramp to be successful on an ongoing basis, an ecosystem of cybersecurity vendors will be needed to ensure that nonprofit organizations have ready access to trusted expertise to help guide improvements. This may take the form of a trusted vendor marketplace specific to nonprofits and/or identification of vendors in the sector with expertise or certifications in cybersecurity.

Recommendations for sector leaders, policymakers, and funders:

- Continue to engage with stakeholders to raise awareness of cybersecurity risks and promote adoption of a shared baseline cybersecurity standard.
- Explore opportunities to further scale and expand the Cybersecurity On-Ramp, including adding information and training resources that provide relevant cybersecurity insights and practices.
- Provide ongoing support and financial resources, including incentives, to assist organizations in implementing cybersecurity measures effectively.

Appendices

Appendix A: Project Participants

We would like to thank the following individuals for their participation in the Cybersecurity On-Ramp Initiative:

- **Anthony Caldwell,** Atlantic Region Association of Immigrant Serving Agencies (ARAISA)
- **Baijul Parikh,** Ontario 211 Services
- **Cathy Barr,** Imagine Canada
- **Charles Buchanan,** Technology Helps
- **Chimene Emejuru,** Lowase Management Consulting (USA)
- **Darryl Kingston,** Digital Governance Standards Institute
- **Hernan Popper,** POPP3R Cybersecurity
- **John Gilliam,** Ontario Council of Agencies Serving Immigrants (OCASI)
- **Karen Milligan,** Ontario 211 Services
- **Kate Karn,** Mastercard Canada
- **Katie Gibson,** Katie Gibson Consulting
- **Kayode Olabisi,** BDC
- **Keith Jansa,** Digital Governance Council
- **Liz Weaver,** Tamarack Institute for Community Engagement
- **Lyn Brooks,** dHub Group

- **Marco Campana,** Freelance Consultant
- **Monika Freunek,** Lighthouse Science Consulting and Technologies Inc.
- **Nidhi Khanna,** Skills for Change
- **Nikki Hera,** Condominium Management Regulatory Authority of Ontario
- **Omar Yaqub,** IslamicFamily
- **Raj Rajakumar,** IslamicFamily
- **Randy Purse,** Senior Advisor, Cybersecurity Training and Education, Rogers Cybersecure Catalyst at Toronto Metropolitan University and Consultant, Quantum Safe Canada
- **Rashmi Sheth,** North York Community House
- **Victor Beitner,** Cyber Security Canada
- **Victor Cordon,** Okta
- **Wonders Pibowei,** Lowase Management Consulting (Nigeria)

Appendix B: Landscape Scan

Existing Relevant Standards

- Digital Governance Council and Digital Governance Standards Institute:
  - Baseline Cyber Security Controls for Small and Medium Organizations
  - Data Centric Security
- Canadian Centre for Cyber Security:
  - Foundational Cyber Security Actions for Small Organizations
  - Using IT Asset Management to Enhance Cyber Security
  - Protecting Your Organization from Software Supply Chain Threats
  - Choosing the Best Cyber Secyurity Solution for your Organization
  - The Canadian Cyber Security Skills Framework (ITSM.00.039)
- The International Organization for Standardization - ISO:
  - Information security management systems (ISO/IEC 27001:2022)
  - Cybersecurity framework development guidelines (ISO/IEC TS 27110:2021)
  - Privacy Information Management (ISO 27701:2019)
  - Information technology - Security techniques - Privacy framework (ISO 29100:2024)
- Pan-Canadian Trust Framework - Digital ID and Authentication Council of Canada - DIACC
- Digital Identity report - Digital ID and Authentication Council of Canada (DIACC)
- Cybersecurity for Startups
- The National Institute of Standards and Technology (NIST) CSF v1.1 Cybersecurity Framework (Information security program and controls Framework. CSF v2.0 is under review and worth reviewing)
  - Getting Started with NIST Cybersecurity Framework
- CIS Security Controls v8 CIS Center for Internet Security (Free resources, benchmarks, security control implementation guides)
- CSA Cloud Control Matrix (CCM v4) (Free guides and questionnaires targeting cloud based applications (i.e. SaaS Applications)

Legislation

- European Union General Data Protection Regulation (GDPR)
- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
- Parliament of Canada Bill C-27 to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act
- Parliament of Canada Bill C-26 amended the Telecommunications Act, and enacted Critical Cyber Systems Protection Act in 2024
- PCI Data Security Standards (PCI DSS) – Data Security Standards for Payments

Existing Risk Assessment Tools

- Critical Security Controls Self Assessment Tool - Center for Internet Security (CIS CSAT)
- Ransomware Business Impact Analysis CIS CSAT BIA Tool
- Cyber-Security Solution guide for your Organization Canadian Centre for Cyber Security
- Cybersecurity Maturity Assessment for Small and Medium Enterprises, European Union Agency for Cybersecurity (ENISA)
- Tech Impact SecCheck
- Additional Tech Impact Security offerings
- Global Cyber Alliance Tools Overview
- Ford Foundation Cybersecurity Assessment Tool (created with nontechnical grant makers, grantee partners, civil society organizations, and nonprofits in mind)

Existing "standards" imposed by funders, government (IRCC), etc.

- IRCC's Privacy and Security Requirements for Funding Recipients - Immigration Contribution Agreement Reporting Environment
  - Reference to iCare Minimum Security Requirements
- Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada, 2022 - Office of the Privacy Commissioner of Canada
- Mandatory survey for cybersecurity that service providing organizations must complete - Canadian Survey of Cyber Security and Cybercrime - 2022
- Canadian privacy breach notification requirements: An overview - a high-level overview of the specific breach notification requirements under PIPEDA, the Québec Act and PIPA AB.

Trainings and introductory webinars

- Cybersecurity Training by Nonprofit Technology Enterprise Network (NTEN)
- Get Cyber Safe guidance by the Canadian Centre for Cyber Security
- Skills for Change free Cybersecurity course for Newcomers (July 2023 cohort)

Cybersecurity planning resources

- Offerings from Mastercard - created for small businesses, some transferability for nonprofit
  - Mastercard Trust Centre
  - Cybersecurity Assessment Quiz
- Canadian Centre for Cyber Security:
  - Cybersecurity Resources for Small and and Medium Organizations
  - Ransomware Playbook (ITSM.00.099)
  - Cyber Security Considerations for Consumers of Managed Services
- Cyber Security Toolkit for Boards - The NCSC's Board Toolkit helps boards to ensure that cyber resilience and risk management are embedded throughout an organisation, including its people, systems, processes and technologies.
- Cyber Readiness Institute - The Cyber Readiness Program

Cybersecurity trainings and/or resources offered by professional associations and networks

- Cyber Peace Builders - Offers volunteer free cybersecurity assistance, threat detection and analysis
- Canadian Institute for Cybersecurity, University of New Brunswick - 4-Day Cybersecurity Workshop Training
- Secure and Responsible Tech Policy Foundations, Toronto Metropolitan University
- Cybersecurity Awareness Training Platform, CIRA
- Junior Cybersecurity Analyst, CISCO Skills for All
- Cybersecurity Training, CISCO Networking Academy
- Cybersecurity Training, Global Cyber Alliance (GCA)
- Cyber Readiness Program, The Cyber Readiness Institute
- Cyber Leader Program, The Cyber Readiness Institute
- Keep It Real Online, public cybersecurity and digital awareness campaign, Department of Internal Affairs, Government of New Zealand
- Simply Secure Knowledge Base
- (ISC)2 Certified in Cybersecurity preparation training (intended to be preparation for writing the CC exam, but provides a free self-directed basic cyber security training course that is useful even if not preparing for the exam)

Cybersecurity Training Software

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

Information Security Policies, Processes, Guidelines Templates

- Cybersecurity Framework for Nonprofits
- 6 New Policy Templates to Help You Enact CIS Controls IG1
- Information Security Policy Templates, SANS Institute

Cyber Insurance

- Example Cyber Insurance Application Form
- Cybersecurity insurance growing in popularity after high-profile digital attacks - Does your organization need it? Future of Good

Other resources

- UNESCO Internet for Trust
- Sandbox Innovation, The Digital Governance Standards Institute (DGSI)
- Bias in Resilience, THINK Digital Partners England.
- Cybersecurity resources, Canadian Internet Registration Agency (CIRA)
- Starter Kit, The Cyber Readiness Institute (Protecting your business, customers, and bottom line)
- GCA Cybersecurity Toolkit for Small Business, The Global Cyber Alliance
- Building the Cybersecurity and Resilience of Canada's Nonprofit Sector, Canadian Centre for Nonprofit Digital Resilience
- Cybersecurity and New Technologies, Office of Counter-Terrorism, United Nations

Appendix C: Additional Standards

- **ISO 27001:**
  An international standard for information security management systems (ISMS) published by the International Organization for Standardization. Achieving ISO 27001 certification requires an audit by an accredited third-party certification body.

- **CIS Critical Security Controls:**
  The Center for Internet Security (CIS) is a nonprofit organization that develops security controls. The CIS Critical Security Controls, also known as CIS Controls, are a prescriptive, prioritized, and simplified set of best practices.

- **NIST Cybersecurity Framework:**
  The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce. The NIST Cybersecurity Framework (CSF) provides guidance to organizations on managing cybersecurity risks and offers a taxonomy of high-level cybersecurity outcomes.

- **SOC:**
  System and organization controls (SOC) are reports on organizational controls, including the security, availability, and processing of data, as well as the confidentiality and privacy of systems. The SOC reporting framework is developed by the American Institute of Certified Public Accountants (AICPA). SOC reports are produced following an assessment performed by a third-party auditor.

CANADIAN CENTRE FOR NONPROFIT DIGITAL RESILIENCE