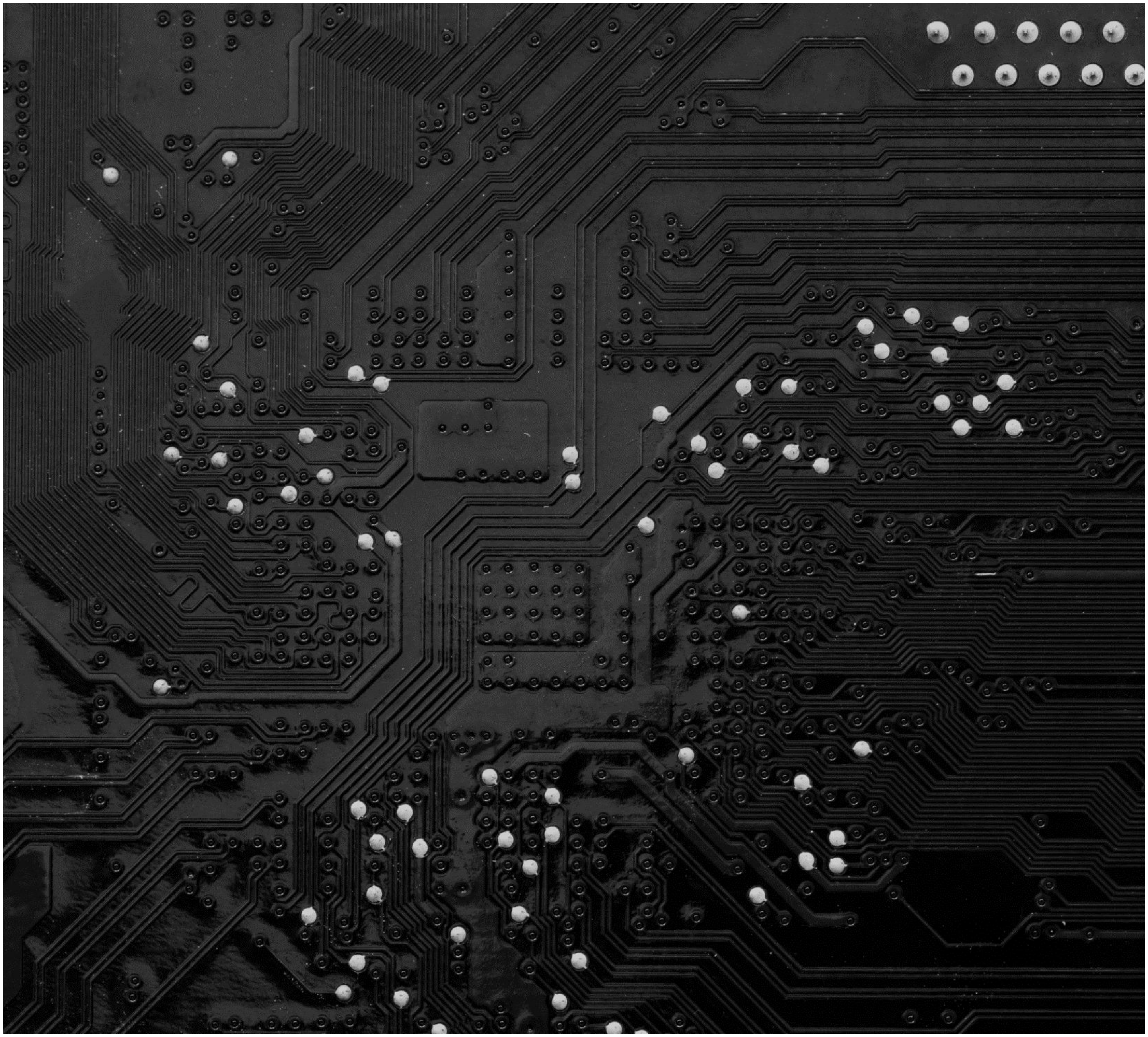
BUILDING THE CYBERSECURITY AND RESILIENCE OF CANADA'S NONPROFIT SECTOR

A VISION AND STRATEGY FOR THE SECTOR

February 2023

CANADIAN
CENTRE FOR
NONPROFIT
DIGITAL
RESILIENCE



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!

https://ccndr.ca/

Table of Contents

I. INTRODUCTION

The Canadian Centre for Nonprofit Digital Resilience convened a Working Group focused on **Building the Cybersecurity and Resilience of Canada's Nonprofit Sector**. The following document captures the knowledge and insights of the working group participants as well as the many sector stakeholders who offered feedback on drafts.

Problem Exploration

The Working Group met on May 5, 2022, with 47 participants including representatives from large and small nonprofits, nonprofit capacity-builders, nonprofit funders, policymakers, academics, cybersecurity experts, and cybersecurity vendors.

Katie Gibson (CIO Strategy Council) and Charles Buchanan (Technology Helps) co-chaired the initial meeting. They proposed employing a "double diamond" design process. This first meeting focused on exploring the problem.

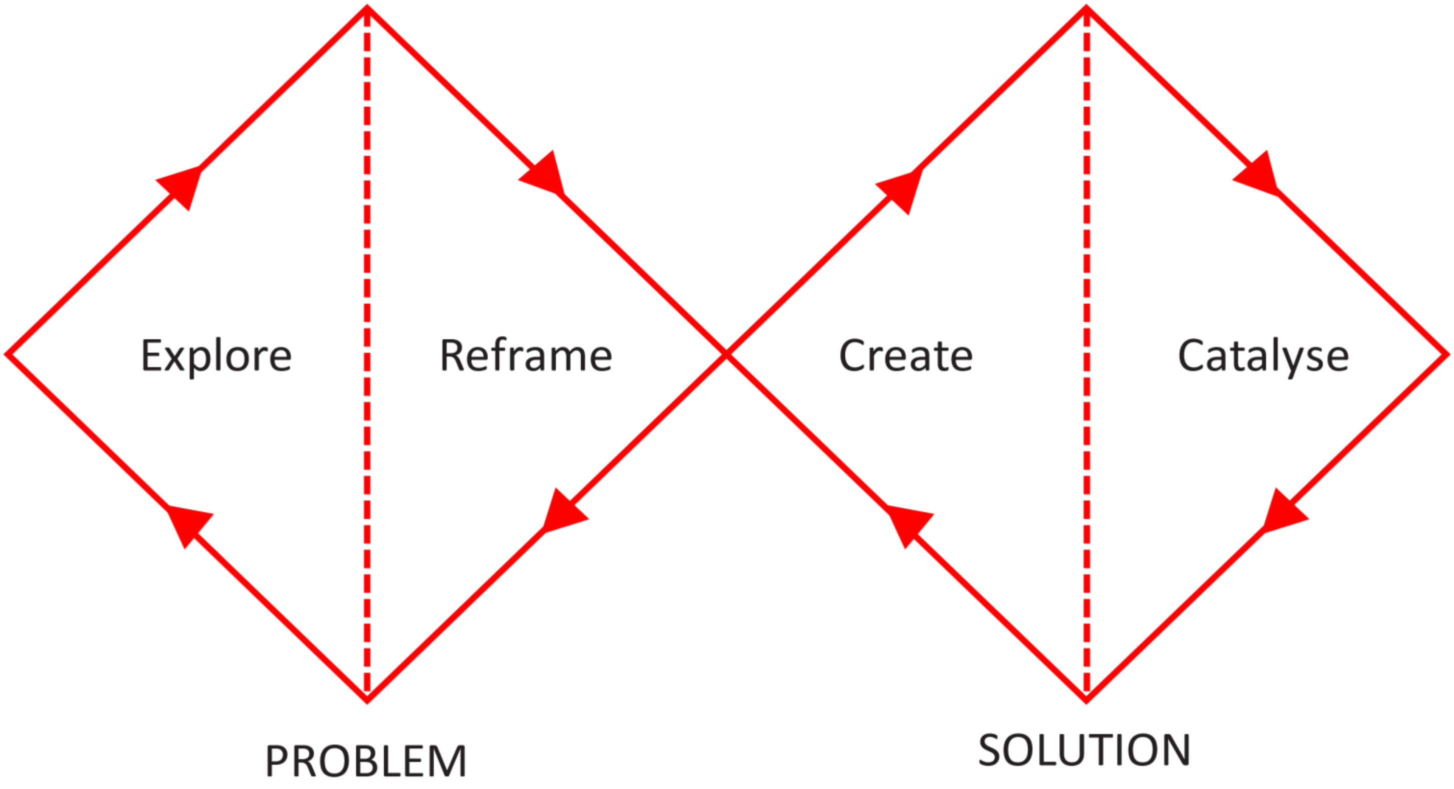


Fig 1: Double Diamond Design Process[1]

After the meeting, a draft report focused on defining the problem was posted for public comment. Fifty-nine comments were received and reviewed by a smaller expert committee, leading to an updated report.

[1] See updated double diamond framework by the Design Council in "Beyond Net Zero – A Systemic Design Approach."

Solution Creation

The Working Group met again on October 18, 2022, with 27 attendees representing the full spectrum of interests. This meeting focused on setting the vision and identifying a path forward. A draft report focused on solutions was then posted for public comment. Thirty-one comments were received as inputs into this final report.

II. CYBERSECURITY THREATS AND CHALLENGES FACING NONPROFITS

In nonprofit organizations, skillful use of technology combined with strong digital leadership can multiply impact. Nonprofits use technology to improve reach and accessibility, provide higher quality services, engage more effectively with donors and supporters, and achieve better outcomes from better data.

Technology adoption brings real benefits, but also risks. These are real risks that can hinder an organization's ability to serve its community. They include operational, financial, legal, and reputational risks with devastating outcomes.

Nonprofits face many of the same cybersecurity threats as other Canadian organizations. Attacks from malicious actors take multiple forms, including ransomware attacks, phishing attacks, and data breaches. Other threats, including accidental or natural hazards (e.g. fires, floods), can put digital information and systems at risk.

Nonprofits often adopt systems, software, and automated processes without fully understanding the risks. And an organization's ability to identify, assess and mitigate risks is often hindered by other constraints including time, expertise, and funding.

> *"A lot of nonprofit staff were working from home during COVID where they shared a computer with multiple family members. In this case, it's a huge risk from data perspective if that computer is not protected properly. The organization rarely has an internal IT team to do the work necessary to make sure data is entered and stored securely. So, the challenge is tech literacy and the capacity for nonprofits to understand how to protect systems and data."*

The following expands on the constraints faced by nonprofits that limit their ability to adopt effective cybersecurity controls and implement security requirements that keep their systems and data safe.

Awareness and Attention

Few nonprofits have data security and privacy on their radar as a basic operational requirement. Most nonprofits are lean and mission focused and tend to lack a strong culture of digital awareness and security.

Many nonprofit organizations lack awareness of cyber risk. One working group participant noted, "Many don't even know that they might be a victim." Another shared, "it's the literacy piece that's foundational", observing that many nonprofits do not have a comprehensive view of the data they collect and the accompanying risks. Many nonprofit leaders believe they are not big enough or rich enough to be targets for cyber threats, nor do they consider the cyber risks associated with accidental or natural events.

Furthermore, many nonprofits are unsure of their basic legal and compliance responsibilities. These regulatory requirements vary based on geography, data type, and activity being undertaken. It is incorrect to assume, however, that nonprofits are exempt from privacy laws. As these legislative requirements continue to increase, so too does compliance risk.

Even with awareness, cybersecurity may not make the organization's priority list: one participant noted, "there's a weird denial that we have a problem". Other psychological barriers to acceptance may arise from pressures nonprofits are under, such as funding challenges.

> *"Technology is already a topic a lot of organizations are afraid of, so when we talk about security and compliance, it becomes too overwhelming for organizations to even think about when they have so many other fires to put out."*

Funding Restrictions

Nonprofits often face challenges investing in an effective cybersecurity program. Funders rarely fully appreciate cybersecurity as a standard program cost, so nonprofits frequently lack funding for even the most basic cybersecurity measures.

Traditional funders have demonstrated little interest in funding technology infrastructure and all that entails – including training and implementation. Some may invest in technology innovation, such as new functionality. Few, however, will fund a technology infrastructure overhaul, even if data protection and security are at risk.

This makes it difficult for nonprofits to acquire even basic cybersecurity products/services. And future planning is difficult when nonprofits are already burdened by legacy systems.

Nonprofits are also challenged to build internal capacity. Most do not have a CIO (chief information officer), many do not have even an internal IT resource, and it is very rare for a nonprofit to have a CISO (chief information security officer). Senior leaders, managers, and staff all play an important role in cybersecurity. This requires training, which needs to be funded.

In the absence of sustained, sufficient funding for cybersecurity, organizations leverage free software, donated hardware, volunteer IT support, and, when needed, consultant security services to fill the gap.

> *"Cybersecurity and IT expertise is needed at all levels of decision making - governance boards, executive teams, staff, volunteers, etc."*

Even if funding is available, there is another challenge: scale.

Scale

Smaller organizations – which comprise the majority of Canada's nonprofits – are typically at a disadvantage relative to their larger peers, but nonprofits tend to struggle regardless of size.

Small nonprofits tend to have limited capacity and expertise to create custom policies and other interventions to ensure cybersecurity. Expanding operations without a strong cybersecurity foundation can be disastrous.

Larger organizations may be able to dedicate more resources to cybersecurity. They may have more skills, money, knowledge and support for safeguarding the organization. However, they too struggle, particularly if they have more complex data collection systems. And with more data and greater complexity, the risks increase.

> *"Smaller organizations often do not have the resources and critical mass to implement and manage the required controls to protect against information and cyber security risks. Anything we can do to help ensure those controls are understood, implemented, and managed will be essential."*

It is not only the size and scale of the organization that can present challenges. Despite the clear urgency to implement effective cybersecurity, nonprofits face timing constraints that impede their ability to sustain a cybersecurity program.

Time Horizon

Cyber risk is a challenge that must be continuously managed. One participant called it a "constant burning issue". This demands vigilance and keeping one eye on the future.

Risks change as new applications and technologies are introduced, digital interconnections increase, and access types expand. For example, cybersecurity needs will grow with the increasing reliance on virtualized work environments, cloud computing, and artificial intelligence. The shift to remote work and growing reliance on mobile devices has introduced new risks.

Nonprofits' planning and budgeting cycles impose a barrier to building and maintaining a cybersecurity program. Most nonprofits operate with a three to five-year business planning cycle and an annual budgeting process. Investments in their cybersecurity programs are often similarly constrained. Without sustained attention and funding, organizations leave themselves vulnerable to emerging threats.

Outdated Hardware and Software

The use of donated or low-cost/no-cost hardware and software solutions can also increase cybersecurity risk. Secondhand devices sometimes contain viruses, malware, or the previous owners' data.

Hardware, software and operating systems may be used well beyond their end-of-support date. This opens the organization up to a host of issues, as the manufacturer no longer provides security upgrades to protect from new risks. This is called technical debt. It accrues over time and amplifies an organization's risk.

> *"The nonprofit that is working from the position of 'beggars can't be choosers' is under tremendous risks simply due to the legacy systems that they are using."*

A related concern is the improper disposal of technology. Many organizations do not safely decommission their technology and sell, donate, or dispose of materials without realizing they contain sensitive data.

Awareness and attention, funding restrictions, scale, time horizon and outdated systems are key challenges faced by nonprofits. Several other issues are also important to consider.

Other Issues

Federations and associations: Several participants noted the specific challenge of operating in a federation or association context. "It's difficult to figure out, establish, and maintain the boundaries" and determine what should be accomplished centrally versus managed locally. There is additional complexity related to responsibility for, and prescriptive powers over, shared systems and the data they manage. Questions about who owns, manages, and is liable for each part of a technology ecosystem can hamper the implementation of robust cybersecurity measures. Failure to properly address these questions can leave unaddressed risk and liability to spread, uncontrolled, across federated or associated organizations. This risk is particularly acute where nonprofits are working with vulnerable populations and their data.

Funder requirements: Nonprofits are often mandated to collect certain information to meet their funding obligations. They may even be mandated to use a particular system to collect the data. This significantly constrains their flexibility and increases risk (especially if cybersecurity funding is not provided). It also raises the question of liability for a breach: when the funder demands that the organization collect certain data or use a particular system, who then is responsible for the protection of that data and system? This introduces additional risk.

Rights and values: The implementation of some cybersecurity measures may engage employee privacy rights. The nonprofit sector is particularly protective of employee privacy rights, and some organizations have advocated for stronger employee privacy and digital rights protection. The deployment of cybersecurity solutions must achieve a balance, weighing risk and reward.

Connectivity: Limited access to the internet, especially in rural areas, can push cybersecurity even further down the priority list. Rural locations may also have limited access to cybersecurity resources and expertise, increasing the potential likelihood and severity of a cybersecurity incident.

III. IMPACT OF CYBERSECURITY RISKS AND CHALLENGES ON NONPROFITS AND COMMUNITIES

Cyber risks are risks to operations (e.g. inability to access applications needed for service delivery) and risks to data (e.g. client and donor data getting into the wrong hands). These risks translate into real financial, reputational, operational, and strategic impacts. Cyber incidents – particularly data breaches – erode hard-earned community trust and the organization's reputation. They can impact program delivery and service capacity. They can also affect fundraising, volunteer engagement, and staff morale.

Nonprofits collect a good deal of data from clients, donors, staff, and others, including sensitive data such as personal health information and financial information. The biggest impact of a data breach can be on clients who may already be uncomfortable with technology, have limited knowledge of their data exposure, and/or face language barriers. Where clients are vulnerable for these reasons, their personal risk of experiencing fraud increases.

> *"How do we discharge the responsibility of what's required of us that honours the trust of our data depositors?"*

Most nonprofits have limited (if any) contingency funding to respond to a breach– including ransomware payments, fines, legal fees, and damages related to non-compliance actions and litigation. As a result of the dramatic rise in cybercrime-related claims, cyber insurance with relevant coverage limits has become prohibitively costly for many organizations. Even if they could afford cyber insurance, most nonprofits would not meet the stringent eligibility requirements.

IV. AVAILABLE SOLUTIONS AND THEIR SUFFICIENCY

Many cybersecurity resources available today do not require significant investment, and many good cybersecurity practices can be adopted at low-cost.

> *"Many of the tools and applications organizations use come with cybersecurity features and settings that the organizations are not aware of. There are multiple things they can do to improve their security posture without investing in new cybersecurity solutions."*

Several existing resources focused on small-medium enterprises could support nonprofits:

- Innovation, Science and Economic Development Canada's Cybersecure Canada certification program; Canadian Centre for Cyber Security's Baseline Cybersecurity Controls for Small & Medium Organizations; and CIO Strategy Council's National Standard of Canada on Baseline Cyber Security Controls for Small and Medium Organizations;
- Rogers Cybersecure Catalyst Simply Secure program;
- The University of Montreal's Clinique de Cyber-Criminology, which is a resource to support the victims of cybercrime.
- Other standards include NIST Cybersecurity Framework and the Center for Internet Security Controls Self Assessment Tool (CIS CAST)

Some organizations have developed resources specifically for nonprofits:

- NTEN's cybersecurity bundle of courses for nonprofit staff;
- Technology Helps' Ever Secure Enterprise Risk Management Program;
- Cybersecurity resource compilation by the National Council of Nonprofits in the United States.

However, resources are only as good as organizations' awareness of them, understanding of how to apply them, and motivation to use them.

V. VISION FOR THE SECTOR

The Working Group agreed on a vision for the sector:

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

This vision includes several components:

Knowledge

- Nonprofit boards, executives, staff, and members understand their risks and obligations and prioritize cybersecurity.

Tools

- Nonprofits have an easy on-ramp to cybersecurity, beginning with a relevant risk assessment that prioritizes preventive, focused action at different maturity levels;
- Nonprofits have access to a standard against which they can compare themselves and that is accepted by funders.

Resources

- Nonprofits have funding to implement required cybersecurity practices;
- Nonprofits have access to a marketplace of vendors providing quality, cost-effective solutions to nonprofits.

> *Nonprofits need to know how to manage the overwhelm, do a relevant threat assessment, and take focused action.*

VI.A SECTOR-WIDE STRATEGY

The Working Group recommends a holistic, sector-wide strategy to meet this challenge. It consists of five strategic objectives, each with a range of potential interventions for future exploration.

Objective 1: Nonprofit boards, executives, and staff understand their risks and obligations and prioritize cybersecurity

Potential interventions:

- A “myth-busting” or educational campaign to raise awareness of both the risks and organizations’ foundational responsibilities. This could form the foundation of a cybersecurity culture within the nonprofit sector. It could leverage rising insurance costs as the burning platform. It could also feature a “State of Cybersecurity in the Nonprofit Sector” report;
- Low-cost, readily accessible training and education solutions for key nonprofit decision-making and technical roles;

- An IT community of practice;
- A train-the-trainer program to improve nonprofit staff members' understanding of data management and security. This intervention could also support community partnerships to develop training plans;
- Encouraging more senior technology and cybersecurity leaders to join nonprofit governance boards, sharing their expertise and demystifying business and technical risk remediation.

Objective 2: Nonprofits have an easy on-ramp to cybersecurity, beginning with a relevant risk assessment that prioritizes preventive, focused action at different maturity levels

Potential interventions:

- A common risk assessment tool for nonprofit organizations that includes benchmarking against peers;
- A resource hub with some basic information and steps to be implemented that do not require technical knowledge.

Objective 3: Nonprofits have access to a standard against which they can compare themselves and that is accepted by funders

Potential interventions:

- A process to develop consensus among key stakeholders (nonprofits, funders, etc.) on the agreed standard and implementation guidelines in a specific sub-sector (e.g. settlement services). Standards include those listed above from CIO Strategy Council, NIST, and Center for Internet Security.

Objective 4: Nonprofits have funding to implement required cybersecurity practices

Potential interventions:

- An advocacy campaign for the expansion of operating funds to include cybersecurity and data management as well as organizational training and policy development;
- Educating funders on the importance of and requirements for cybersecurity funding.

Objective 5: Nonprofits have access to a marketplace of vendors providing quality, cost-effective solutions

Potential interventions:

- A shared services model that could help achieve economies of scale, lower unit costs, and lighten staff workloads;
- A roster or "vendor of record" of trusted IT/cybersecurity experts;
- A "carrier" model (i.e. an entity that makes it possible to deliver the cybersecurity service);
- An ecosystem portal embedding state-of-the-art cybersecurity with forward updates, identity, data security, privacy and trust attributes (e.g. Canada Health Infoway ACCESS2022 model).

"There are a lot of actions that can be taken that don't require a lot of investment to significantly mitigate risks."

VII.THE PATH FORWARD

To realize the vision and objectives above, the Working Group agreed to develop and test several prototypes.

A cybersecurity on-ramp in the settlement sector

We will prototype an on-ramp, including a risk assessment, with the immigrant and refugee-serving sector. The strategic approach is to go deep into the needs of one sector, develop a successful intervention, and then scale it to other sectors.

This pilot will focus on answering the following question: “How can we remove the overwhelm nonprofit leaders feel and provide an on-ramp to cybersecurity for organizations?”

A model cybersecurity policy for social services

In partnership with Islamic Family and Social Services Association, we will develop a model cybersecurity policy that can be adopted by other social service organizations.

“It's a complicated challenge. However, if we can work to make a meaningful difference, we will reduce technical barriers to mission and really multiply not-for-profit impact.”

PARTICIPANTS

Tremendous gratitude to the following individuals who provided invaluable insights and feedback throughout the process.

1. Adam Rosenzweig
2. Adrian Kaats
3. Alberta Johnson
4. Alexandru Lazar
5. Alina Turner
6. Amy Sample Ward
7. Andre Cote
8. Anthony Caldwell
9. Ayesha Zamudio
10. Benjamin Miller
11. Brock Warner
12. Cathy Barr
13. Chantal Edwards
14. Chantal Robitaille
15. Char San Pedro
16. Charles Buchanan
17. Chris Semanciw
18. Clint Kimchand
19. Courtney Baker
20. Darryl Kingston
21. Derek Johnstone
22. Donny Truong
23. Elie Saykali
24. Eric Jacksch
25. Erle Higgins
26. Francesca Bosco
27. Gwyneth Dalzell
28. Heather Simpson
29. Helen Knight
30. Hernan Popper
31. Hovman Javden
32. Jane Zhang
33. Jen Crowe
34. Jennifer Tran-Smith
35. Jerry Koh
36. Jessica Alcock
37. Jody Wolf
38. Joshua Peskay
39. Karen Chase
40. Karen Milligan
41. Katie Gibson
42. Kelly McKean
43. Kendra Fincaryk
44. Leonardo Soto
45. Lyn Brooks

46. Marco Campana
47. Marilee D'Arceuil
48. Mary Catalfo
49. Michelle Baldwin
50. Mina Demian
51. Moayad Aiash
52. Nancy Birungi
53. Natasha Vincent
54. Neemarie Alam
55. Nidhi Khanna
56. Nikki Hera
57. Pablo Zacarias
58. Paul Vallée
59. Racheal Khan
60. Raj Rajakumar
61. Raine Liliefeldt
62. Randy Purse
63. Rashmi Sheth
64. Renee Black
65. Robert Martin
66. Saif Azwar
67. Sandra Lapointe
68. Sarah Juma
69. Stacey Dakin
70. Stephanie Guico
71. Sumit Bhatia
72. Sundeep Virdi
73. Surranna Sandy
74. Tennyson Yang
75. Tim Lockie
76. Tracy Luca-Huger
77. Tuhin Mathur
78. Ushnish Sengupta
79. Vafa Adib
80. Wanda Brascoupe
81. Yasin Kokarca