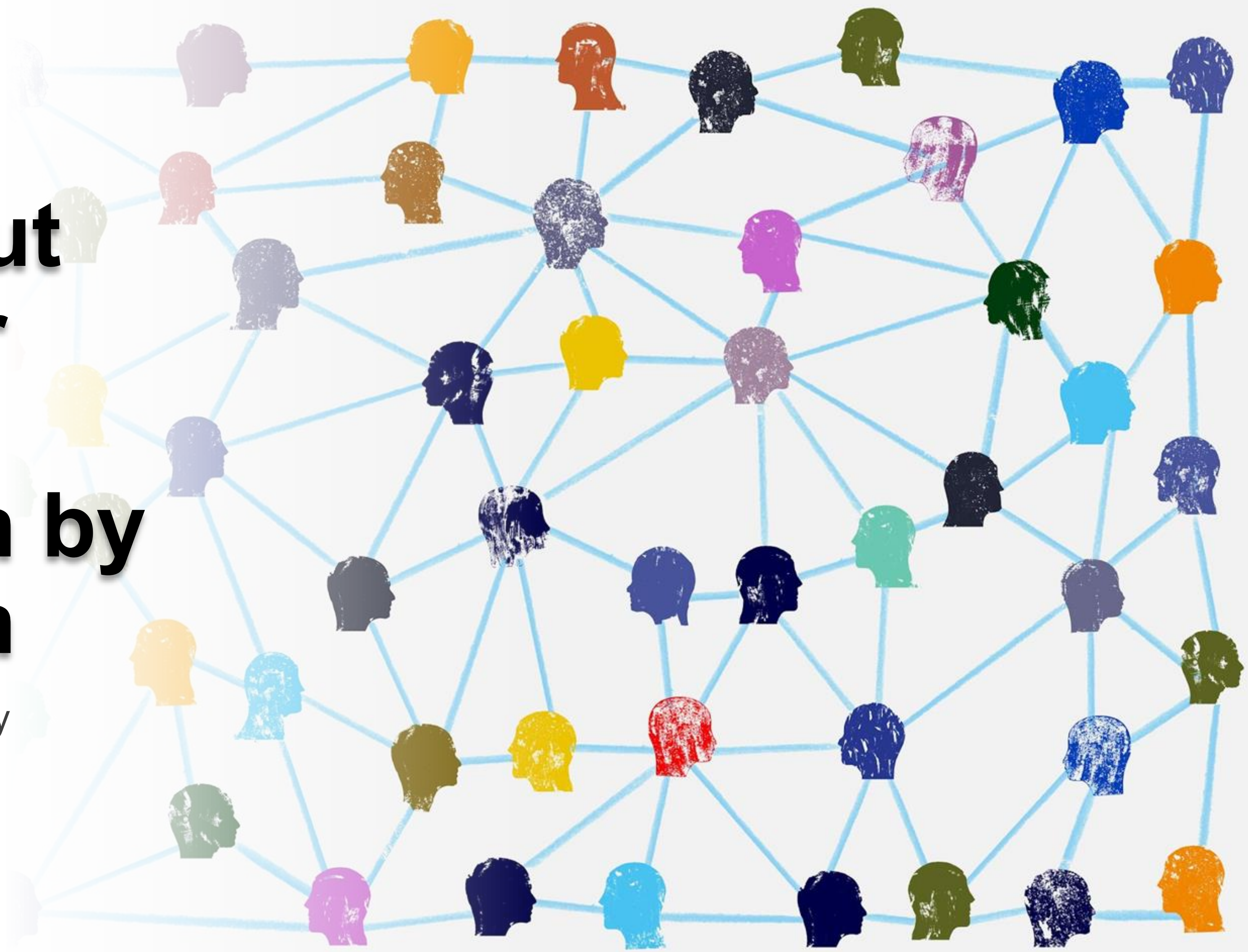
Building out BC's cyber safety net, connection by connection

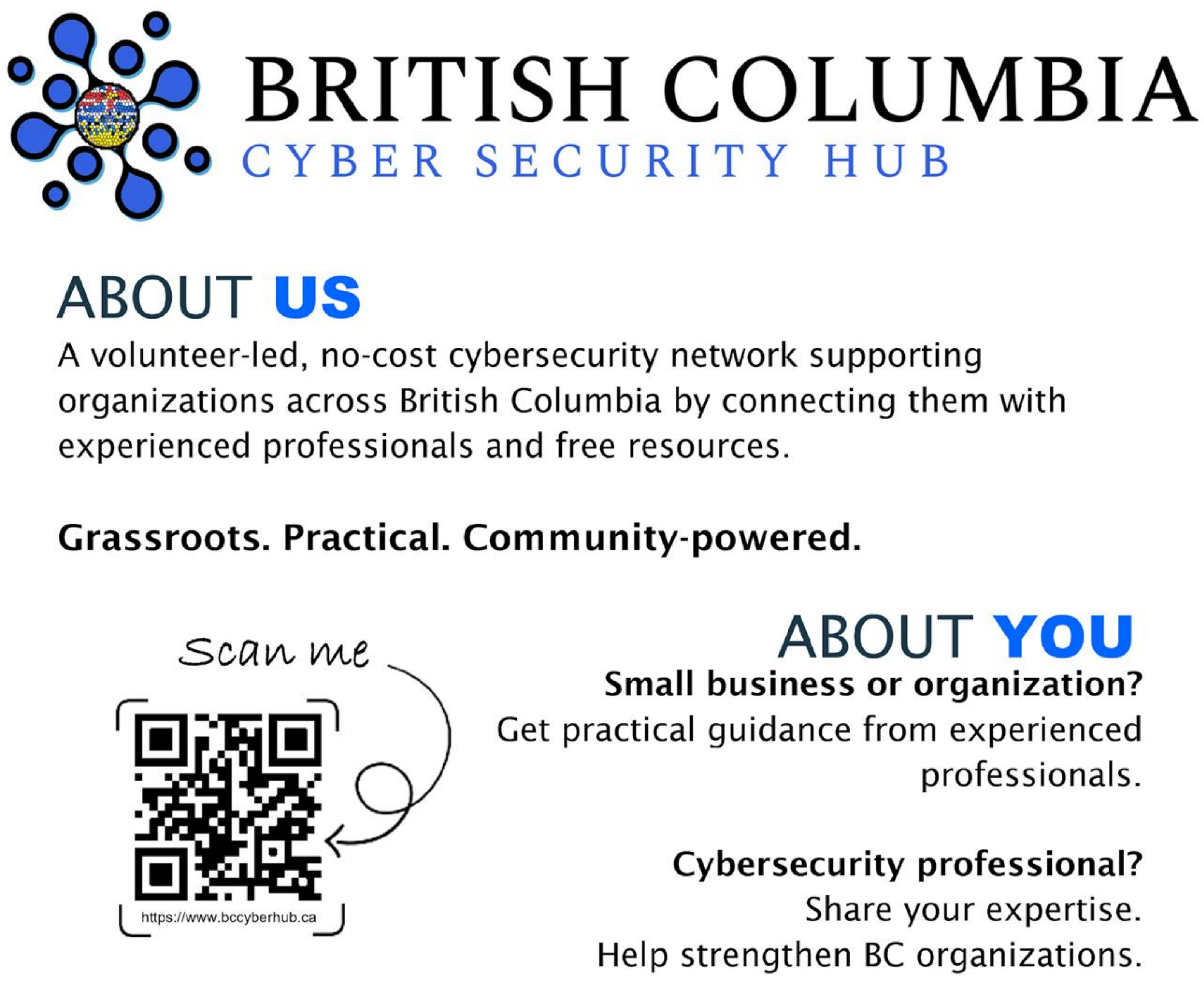
Victoria International Privacy
and Security Summit

3 March 2026



VIPSS 2025

"Helping the most vulnerable small organisations and businesses in BC practice better cybersecurity"



BRITISH COLUMBIA
CYBER SECURITY HUB

ABOUT US

A volunteer-led, no-cost cybersecurity network supporting organizations across British Columbia by connecting them with experienced professionals and free resources.

Grassroots. Practical. Community-powered.

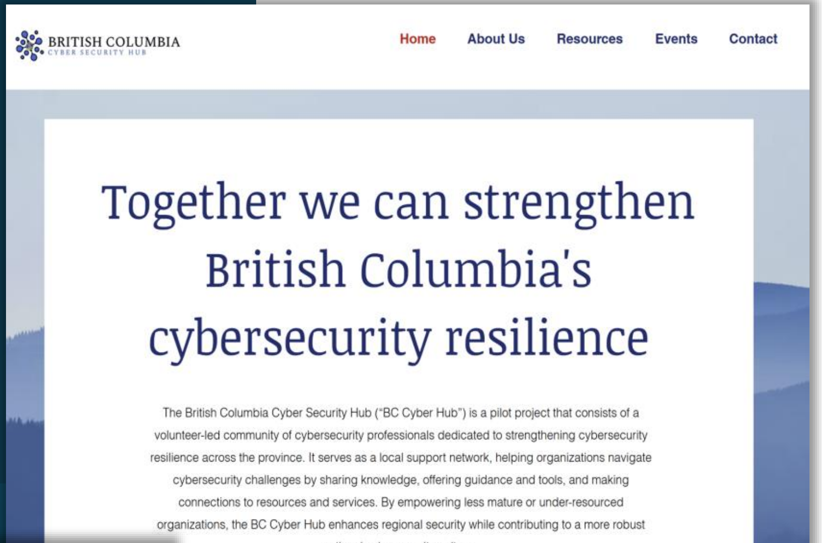
Scan me
https://www.bccyberhub.ca

ABOUT YOU

Small business or organization?
Get practical guidance from experienced professionals.

Cybersecurity professional?
Share your expertise.
Help strengthen BC organizations.

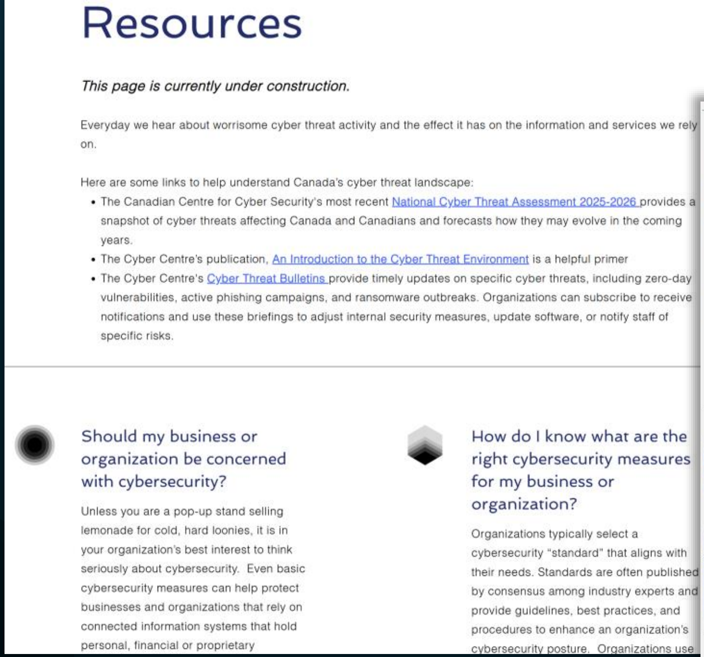
Since last year's VIPSS launch



Together we can strengthen British Columbia's cybersecurity resilience

The British Columbia Cyber Security Hub ("BC Cyber Hub") is a pilot project that consists of a volunteer-led community of cybersecurity professionals dedicated to strengthening cybersecurity resilience across the province. It serves as a local support network, helping organizations navigate cybersecurity challenges by sharing knowledge, offering guidance and tools, and making connections to resources and services. By empowering less mature or under-resourced organizations, the BC Cyber Hub enhances regional security while contributing to a more robust national cybersecurity culture.

We acknowledge the homelands of the Indigenous Peoples of this place we now call British Columbia, and honour the many territorial keepers of the Lands on which we work.



Resources

This page is currently under construction.

Everyday we hear about worrisome cyber threat activity and the effect it has on the information and services we rely on.

Here are some links to help understand Canada's cyber threat landscape:

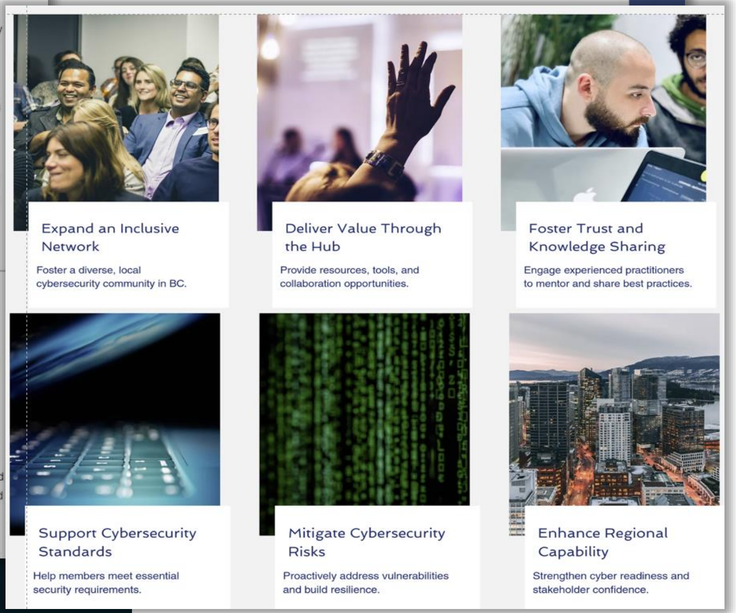
- The Canadian Centre for Cyber Security's most recent National Cyber Threat Assessment 2025-2026 provides a snapshot of cyber threats affecting Canada and Canadians and forecasts how they may evolve in the coming years.
- The Cyber Centre's publication, An Introduction to the Cyber Threat Environment is a helpful primer
- The Cyber Centre's Cyber Threat Bulletins provide timely updates on specific cyber threats, including zero-day vulnerabilities, active phishing campaigns, and ransomware outbreaks. Organizations can subscribe to receive notifications and use these briefings to adjust internal security measures, update software, or notify staff of specific risks.

Should my business or organization be concerned with cybersecurity?

Unless you are a pop-up stand selling lemonade for cold, hard loonies, it is in your organization's best interest to think seriously about cybersecurity. Even basic cybersecurity measures can help protect businesses and organizations that rely on connected information systems that hold personal, financial or proprietary

How do I know what are the right cybersecurity measures for my business or organization?

Organizations typically select a cybersecurity "standard" that aligns with their needs. Standards are often published by consensus among industry experts and provide guidelines, best practices, and procedures to enhance an organization's cybersecurity posture. Organizations use



Expand an Inclusive Network

Foster a diverse, local cybersecurity community in BC.

Deliver Value Through the Hub

Provide resources, tools, and collaboration opportunities.

Foster Trust and Knowledge Sharing

Engage experienced practitioners to mentor and share best practices.

Support Cybersecurity Standards

Help members meet essential security requirements.

Mitigate Cybersecurity Risks

Proactively address vulnerabilities and build resilience.

Enhance Regional Capability

Strengthen cyber readiness and stakeholder confidence.

BC Cyber Hub Pilot checklist

- ✓ Mission, vision, principles
- ✓ Steering group, TORs
- ✓ Inventory of key initiatives
- ✓ Threat assessment
- ✓ Website
- ✓ Registration and questionnaire
- ✓ Experts (!), advice, guidance
- ✓ Engagement and events

Tool Pilot: AI Cyber Security Assistant

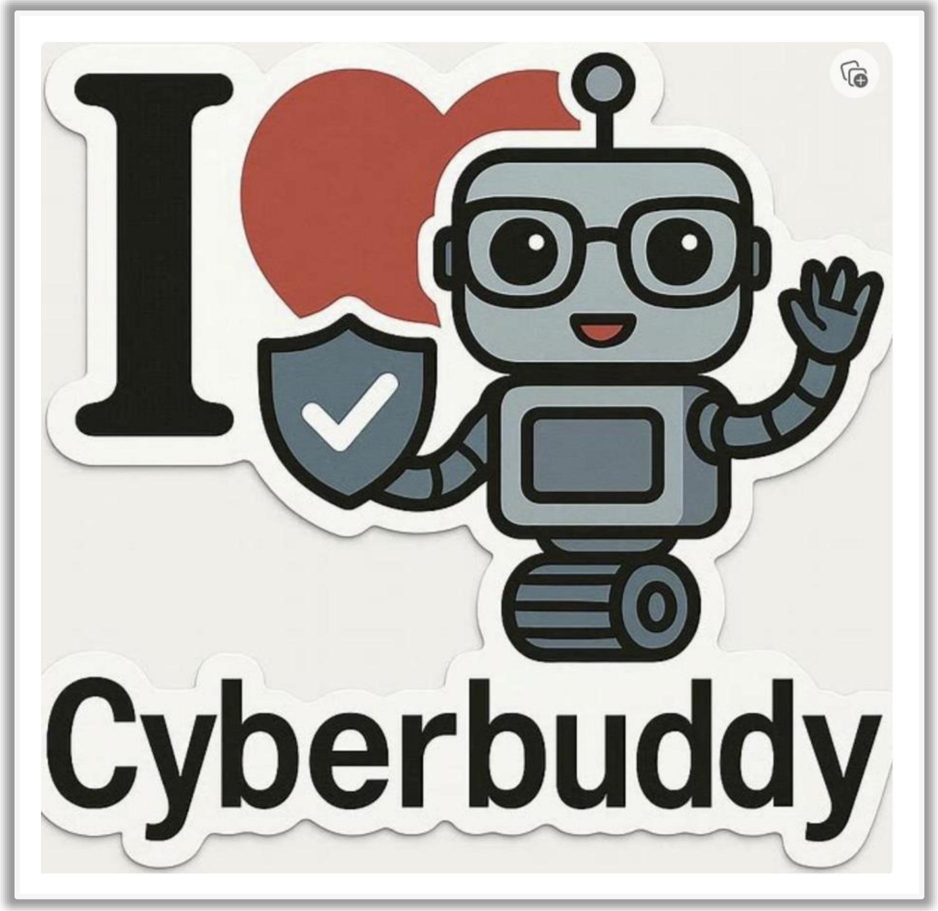
❑ Onboards users through a simple questionnaire to assess their people, technology.

❑ Allows them to ask unlimited plain-language questions in a safe and “no shame” space and receive tailored, implementable guidance in return.

❑ Translates universal cybersecurity standards into simple, implementable, step-by-step instructions.

❑ Generates cybersecurity policies, guidelines and training options appropriate for small organisations.

❑ Keeps each organization’s data isolated and secure.



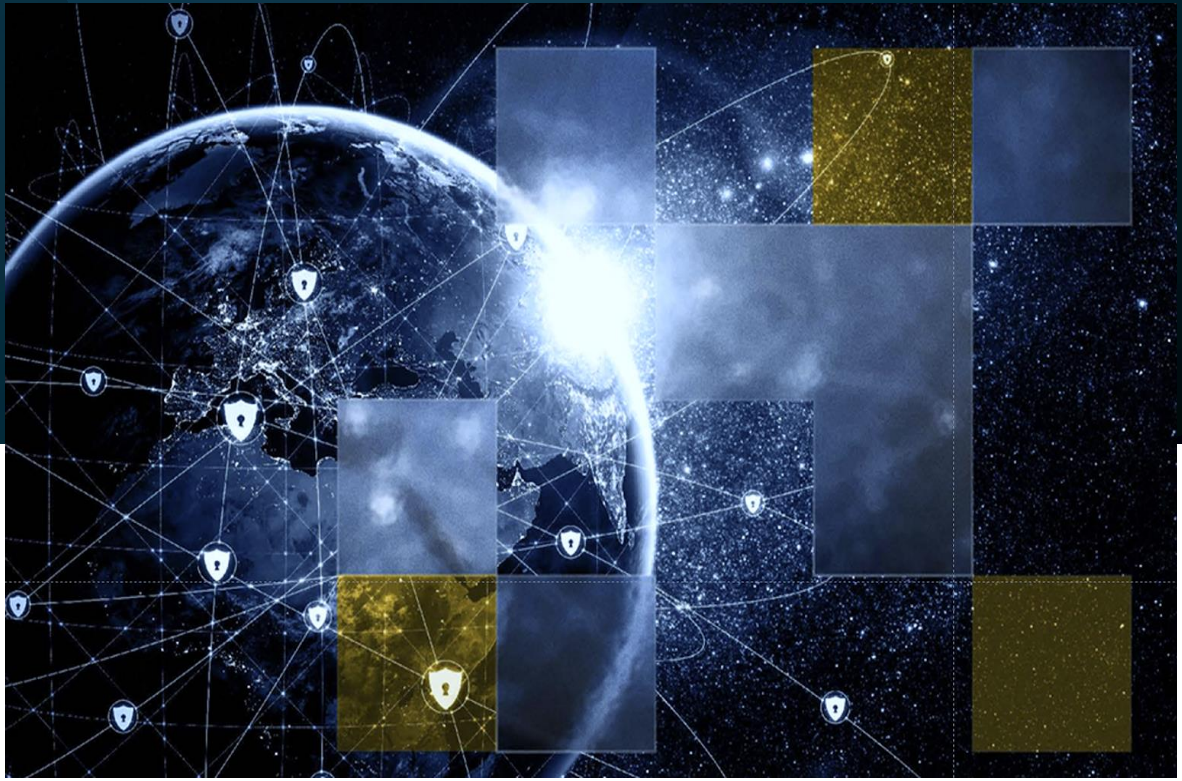
Challenges!

- Already stretched experts
- Hesitant target audience

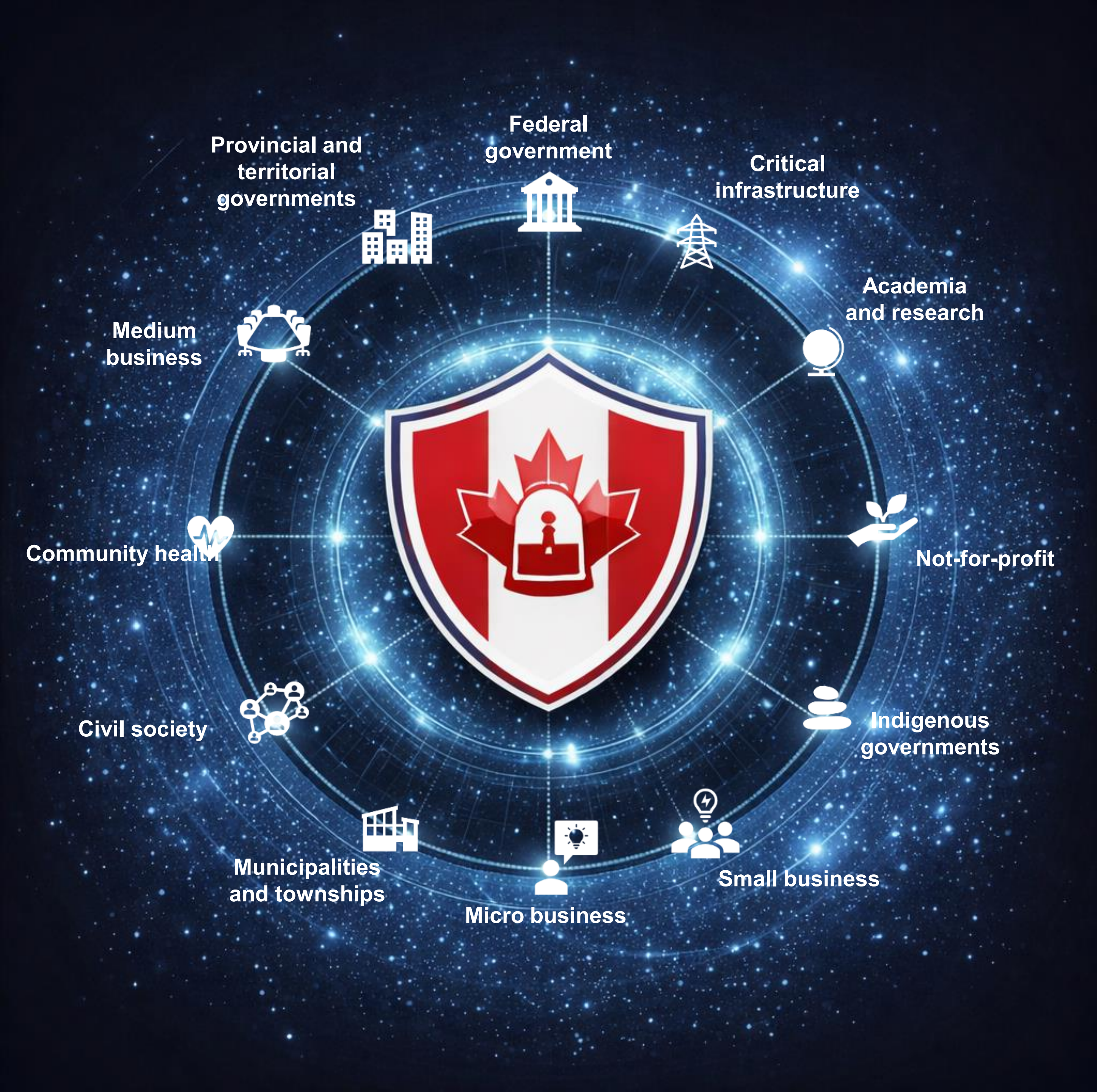
Plus…

- Project management and back-office support
- Legal or NFP status to accept offers of financial assistance
- Venues and advertising events
- Managing expectations

Update: Canadian cybersecurity context 2025



- National Cyber Security Strategy
- Federal initiatives
- Threat landscape



Reality check:

Gaps in the Canadian cybersecurity ecosystem

National level risk/leadership

- ✓ Federal government/CCCS
- ✓ National critical infrastructure
- ✓ Major technology vendors/platforms

Regional risk/leadership

- ✓ Provinces, territorial governments
- ✓ Large municipalities
- ✓ Medium business

Local risk

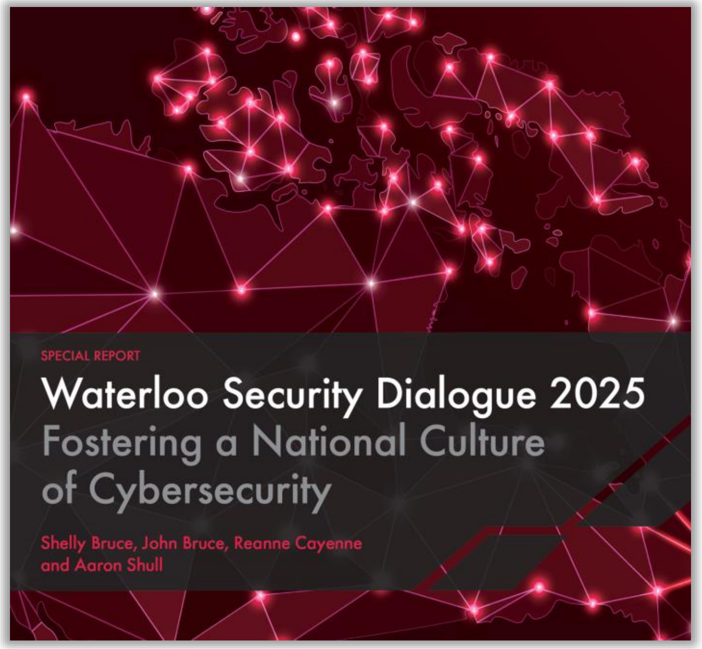
- Very small business, entrepreneurs
- Small municipalities
- Indigenous governments
- Not-for-profits
- Civil society

Examining the potential of grassroots initiatives in the fight against cyber threats in BC

Waterloo Security Dialogue

Whole-of-Community Approach

The Waterloo Security Dialogue is dedicated to **enhancing Canada's cyber resilience** by fostering connections between leaders and experts and encouraging collaboration within and across sectors, jurisdictions and organizations in Canada.

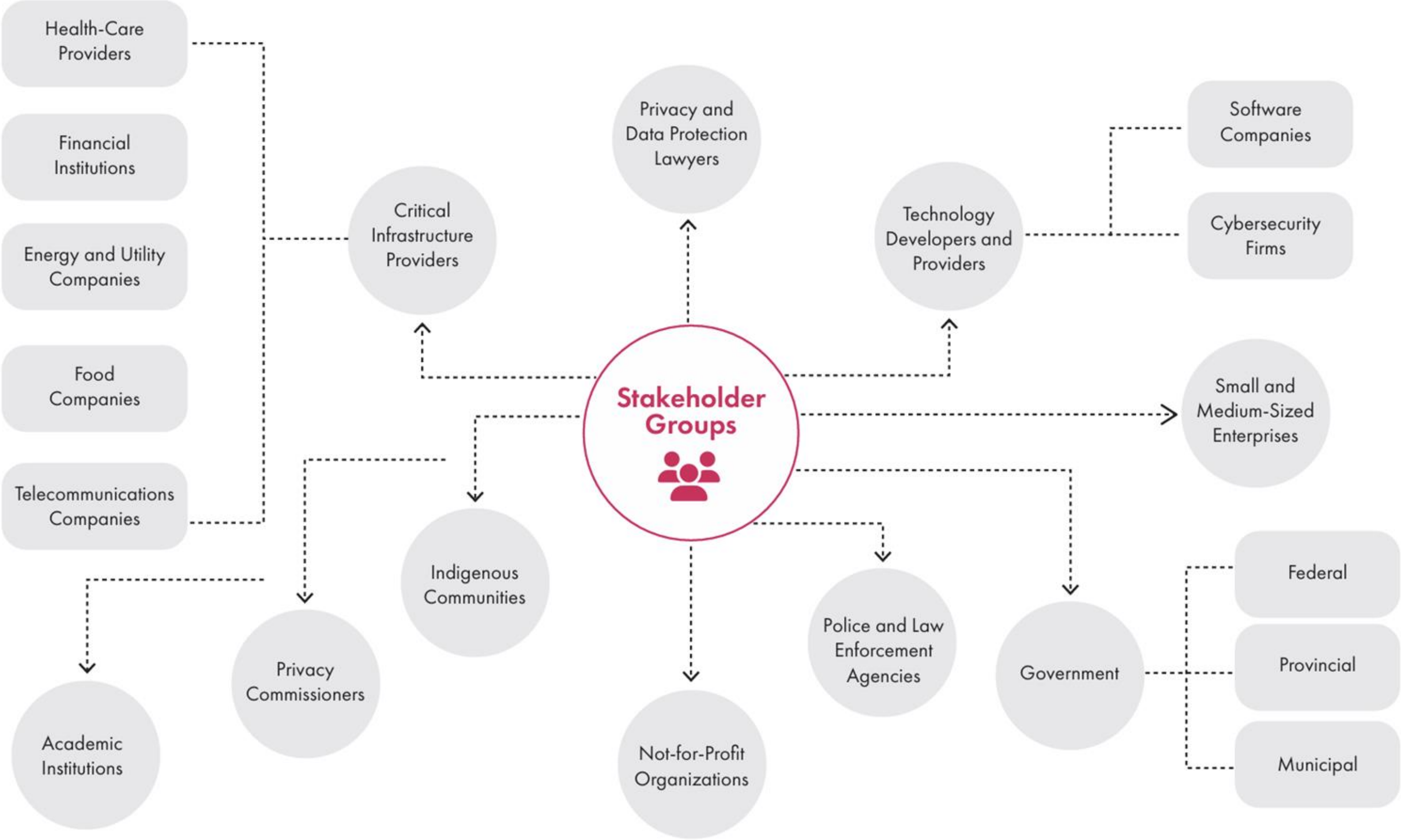


SPECIAL REPORT

Waterloo Security Dialogue 2025

Fostering a National Culture of Cybersecurity

Shelly Bruce, John Bruce, Reanne Cayenne and Aaron Shull



Stakeholder Groups

Critical Infrastructure Providers

Health-Care Providers

Financial Institutions

Energy and Utility Companies

Food Companies

Telecommunications Companies

Privacy and Data Protection Lawyers

Technology Developers and Providers

Software Companies

Cybersecurity Firms

Small and Medium-Sized Enterprises

Government

Federal

Provincial

Municipal

Police and Law Enforcement Agencies

Not-for-Profit Organizations

Indigenous Communities

Privacy Commissioners

Academic Institutions

Key takeaways from this year’s WSD dialogue

01

Recognize and promote the role of grassroots cybersecurity movements

02

Make blueprints available for others to adopt

03

Set expectations for consistent competency and ethics frameworks

04

Ensure the new strategy’s whole-of-society consultation construct includes grassroots initiatives

05

Encourage private-public partnerships as foundations of grassroots efforts

A Grassroots Approach to Service Design

Service Design

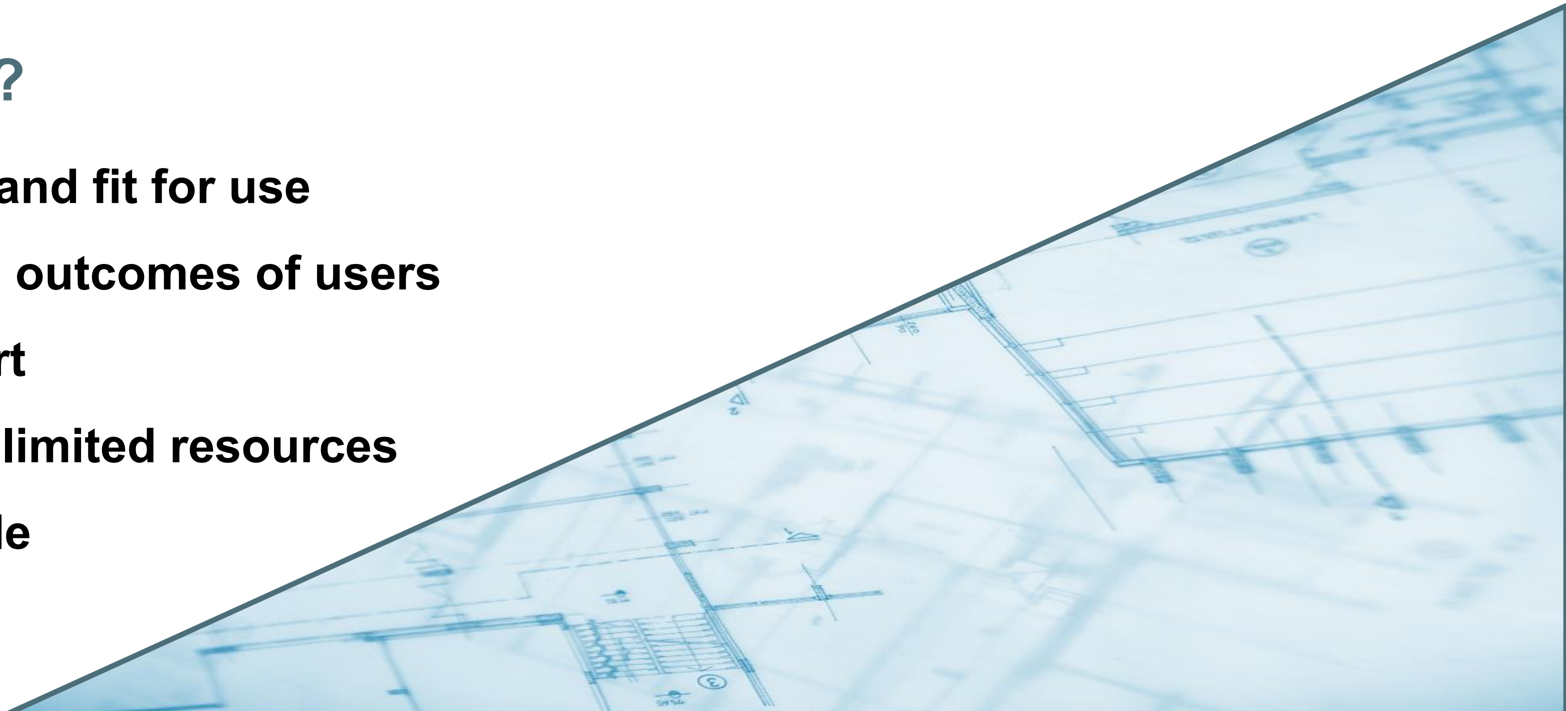
What is Service Design?

“The practice of designing services that are fit for purpose, fit for use, and that can be delivered by the organization and its ecosystem.” – IT Infrastructure Library (ITIL) 4

“*Service design is making sure the help actually helps*.” – Unknown

Why do we do Service Design?

- Ensure services are **fit for purpose and fit for use**
- Align services to **needs and desired outcomes of users**
- Design for **accessibility and support**
- Reduce **risk and make the most of limited resources**
- Create **services that are sustainable**



Best Practices in Grassroots Service Design

Success Patterns

- **Design for value, not activity**
- **Co-design with those you serve**
- **Iterate**
- **Design end-to-end**
- **Design for trust, reliability, and security**
- **Keep it simple**
- **Measure**

Anti-Patterns

- **Vision over value**
- **Design *for*, not *with***
- **Hero culture**
- **Design-as-you-go**
- **Tool-first thinking**
- **One-Size-Fits-None**
- **Finished!**

A Phased Approach to Grassroots Service Design

1 Develop Value Proposition

- The goal of the service
- The value you provide & problem you solve
- How you will fund/sustain the service

2 Explore the Space

- Engage your users and partners early and often
- Test assumptions, research, and identify priorities
- Identify opportunities, barriers, and risks

3 Design your Service Model

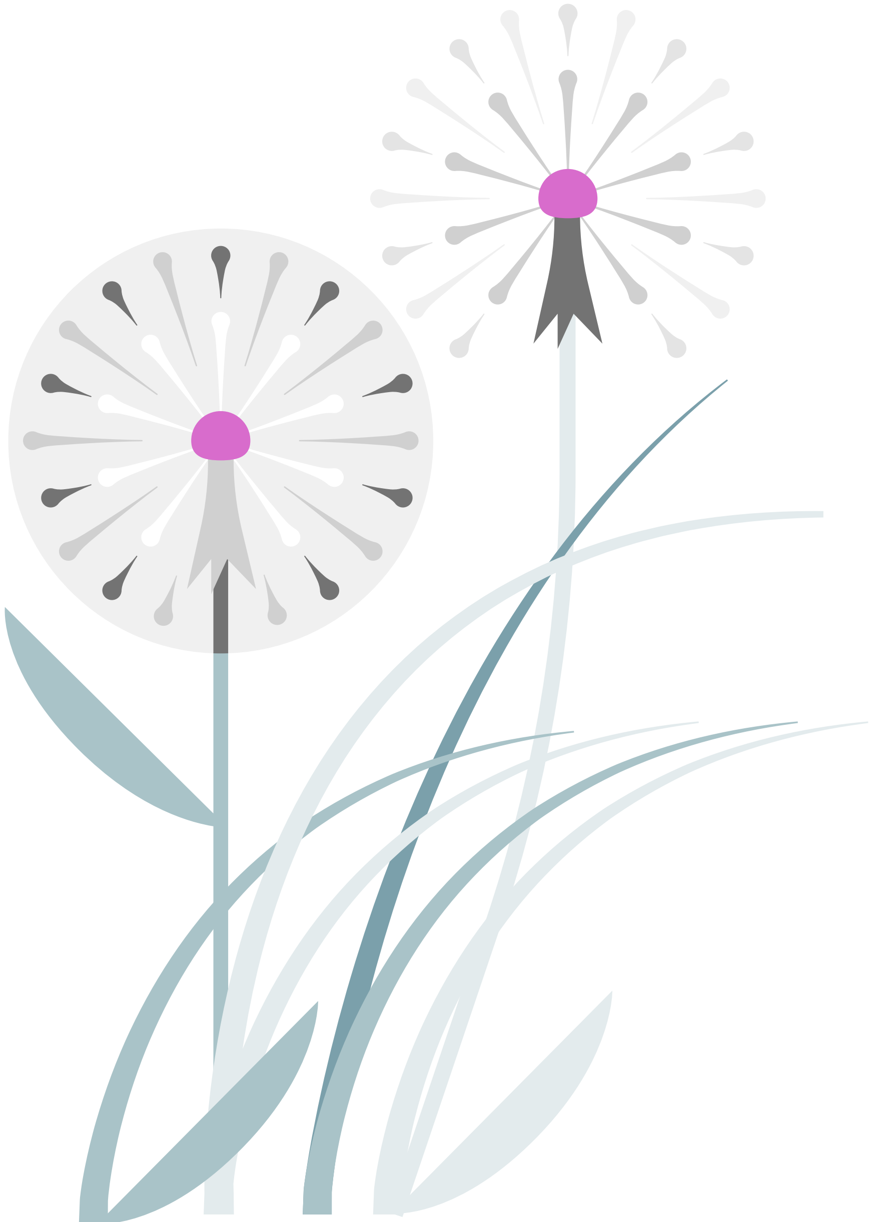
- Co-develop the service with users and participants
- Identify and build for measurable indicators of success
- Design foundations (tools, skills, people, process, policy)

4 Iteratively Build & Deliver the Service

- Deliver value to users early (e.g., pilots, alpha/beta testing)
- Closely monitor capacity, success metrics, and user feedback
- Refine the service based on feedback

5 Operate, Improve, and Expand

- Identify opportunities to iteratively expand service to more users and communities
- Monitor environment for change drivers (user needs, technology, policy)
- Monitor operations for achieving success measures, efficiency, and user satisfaction



Service Design Considerations

Cybersecurity Service Area

- This is a service area that requires high **trust**
- The communities that need these service are **diverse**
- The communities that need this service most have the most **constrained time and resources**
- Volunteers have different **capabilities and capacities**
- The communities that need this service may be prone to **engagement fatigue**
- Many threats to the organizations to the communities we serve will be **unknown unknowns** to them

Service Design Questions for Cyber Hub

For **everyone**

- What does reciprocity look like in practice?

For our **communities**

- What does value look like to you? (e.g., knowledge, policies, confidence, controls, someone to call in emergencies)
- How can we provide confidence that our experts are appropriately vetted?
- What do you want to see in a code of conduct?
- What design principles would you like to see guiding services on offer?
- What are your priorities when it comes to security?
- What can we do to make this accessible?

For our **volunteers**

- How can we help volunteers in onboarding, orientation, and guidance?
- What liability protections do our volunteers need?
- What time commitments are realistic?
- What does value look like to you? (e.g., learning, impact, community recognition, system insight, recommendations, experience)

Call to action

- IDENTIFY TO THE BC CYBER HUB YOUR CYBER-SUPERPOWER
- PARTICIPATE AS YOU CAN IN BOTH, OFFERING ASSISTANCE AND REQUESTING IT
- SUGGEST NEW IDEAS OR IMPROVEMENTS
- INVITE SMB ORGS TO JOIN THE BC CYBER HUB

Join Us..!