ROGERS cybersecure catalyst

Baseline Cybersecurity Controls

January 2026

Lester Chng

CISSP, PMP
lester.chng@torontomu.ca

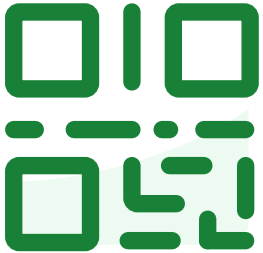
Senior Cybersecurity Advisor
Rogers Cybersecure Catalyst,
Toronto Metropolitan University

Agenda

- Welcome + Introductions
- Canadian Cyber Threat Landscape
- Key Cybersecurity Concepts
- Understanding your Risks
- Baseline Cyber Security Controls
- Q&A
- Resources

Introductions in the chat

- Name
- Role
- Organization
- Cybersecurity knowledge
  (Scale of 1 – 5; 1 being the lowest)
- Expectation of today’s session



Join at slido.com
#1529652

Why Does Cybersecurity Matter?

A failure to protect
our **systems** and **data**,
is a failure to protect those whom we serve.

What is your current state of cybersecurity?

The Canadian Cyber Threat Landscape

The Canadian Cyber Threat Landscape

National Cyber Threat Assessment 2025 - 2026

Cybercrime threats remains a persistent, widespread, and disruptive threat to individuals and organizations.

26% YoY growth of Ransomware incidents between 2021 and 2024.

Factors contributing to this rise:

- Cybercrime-as-a-service
- Increased digitalization of organizations
- AI improves and allows scale of attacks

National Cyber Threat Assessment 2025-2026
https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Implications for the Charitable and Nonprofit Sector

Why are we attractive targets?

- Sensitive Data
- Financial Transactions
- Public Trust and Visibility
- Community Role

Why are we at risk?

- Resource Constraints
- Limited In-House Expertise
- Reliance on Third-Party Vendors
- High Turnover & Volunteers

What are your top cybersecurity concerns?

Key Cybersecurity Concepts

Key Cybersecurity Concepts

- Defence in Depth
- Principle of Least Privilege
- Attack Surface Reduction
- Operational Resilience > Cybersecurity

Defence in Depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

- Administrative Controls
- Physical Controls
- Technical Controls

Principle of Least Privilege

The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

- System access
- Account access
- Financial system access
- Sensitive information access

Attack Surface Reduction

Attack surface reduction is having a clear inventory of all your assets and making it harder for a cybercriminal to find a way in.

- Laptops
- Features
- Accounts
- Software
- Devices

Methods:

- Removal
- Updates
- Limit access
- Block

Operational Resilience > Cybersecurity

Operational Resilience:

The ability of systems to resist, absorb, and recover from, or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of the ability to perform mission-related functions.

If you experience a significant cybersecurity incident

- Can you continue operations (sub-optimal)?
- Are you able to recover quickly?

This is enabled by:

- Incident response planning
- System design – data backup, alternatives
- Business continuity
- Disaster recovery

Which concepts are currently implemented in your organization?

Understanding your Risks

Understanding your Risks

What are you protecting?

- Sensitive information - Data
- Assets – Hardware, Software, Website
- Operations - Processes

Enablers

Asset Inventory

Process and Procedures

What are the main threats?

- Data breach
- Disruption to operations - Ransomware
- Fraud
- Business Email Compromise

Enablers

Baseline Cybersecurity Controls

Baseline Cybersecurity Controls

Baseline Cyber Security Control for Small-Med Orgs

CCCS Baseline Cyber Security Controls -
https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Starting Point

Four Controls to Start with:

- Develop an incident response plan
- Patch operating systems and applications
- Enforce strong user authentication
- Backup and encrypt data

Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)- *https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035*

Develop an Incident Response Plan

Having an incident response plan (IRP) allows your organization to:

- Manage incidents
- Mitigate threats and risks
- Recover quickly from incident

Simplified Incident Response Plans includes:

- Key stakeholder contact list
- Critical asset list
- Alternative processes
- Back up options

Developing your incident response plan (ITSAP.40.003)
https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003

Develop an Incident Response Plan

Incident Response Plan Development:

- Conduct a risk assessment
- Establish your response team
- Develop your policies
- Create your communications plan
- Educate your employees

Phases of Incident Response

1. Prepare
2. Observe
3. Resolve
4. Understand

Developing your incident response plan (ITSAP.40.003)
https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003

Does your organization have an incident response plan?

Patch Operating Systems and Applications

Cybercriminals exploit vulnerabilities in outdate systems and applications.

Risk of not patching:

- system lags or crashes during use
- unresponsive applications
- vulnerabilities that are exploited to infect devices with malware
- hackers gaining access to, stealing or encrypting your sensitive information, or preventing your device from working
- inaccessible features on applications

Activate **automatic** patches and updates for all software and hardware.

Important to have a good inventory of all your assets.

Are you aware of how your vendor/third-party manage their updates?

How updates secure your device (ITSAP.10.096)
https://www.cyber.gc.ca/en/guidance/how-updates-secure-your-device-itsap10096

Patch Operating Systems and Applications

The patch management process includes the following actions:

- identifying when a new patch has become available for your device
- testing the patch (when possible) to ensure it is compatible with your existing software and environment
- reviewing additional requirements that may be necessary for the patch to be installed or function as expected
- sending notifications when patches are available
- installing the patches
- verifying the patches have been installed effectively

How updates secure your device (ITSAP.10.096)
https://www.cyber.gc.ca/en/guidance/how-updates-secure-your-device-itsap10096

Enforce Strong User Authentication

Password Policies and Management

Passwords are used for devices, accounts, website log-ins. Most passwords are re-used and this creates additional risks.

- Use complex passwords
- Avoid common password mistake
- Use password managers*

Best practices for passphrases and passwords (ITSAP.30.032)
https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

Multi-Factor Authentication (MFA)

Implementing MFA provides an additional layer of authentication and does not rely on passwords alone.

- Enable in all available devices/accounts
- Prioritize where to implement

Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
https://www.cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030

Backup and encrypt data

These controls address 2 key risks:

- Disruption to operations
- Disclosure of sensitive information

LifeLabs®

An Open Letter to LifeLabs Customers

To our customers:

Through proactive surveillance, LifeLabs recently identified a cyber-attack that involved unauthorized access to our computer systems with customer information that could include name, address, email, login, passwords, date of birth, health card number and lab test results.

Personally, I want to say I am sorry that this happened. As we manage through this issue, my team and I remain focused on the best interests of our customers. You entrust us with important health information, and we take that responsibility very seriously.

We have taken several measures to protect our customer information including:

Backup and encrypt data

Having tested and validation backups gives you options for responding to a cybersecurity incident.

When are backups used:

- Failure or outage
- Ransomware
- Denial of service attack
- Natural disasters
- Lost or stolen devices

Tips for backing up your information (ITSAP.40.002)
https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002#when

Backup and encrypt data

Where to store are backups:

- Onsite [Removable storage media, Network-attached Storage]
- Offsite [Vendor storage]
- Cloud-based storage

3-2-1 rule for data storage

- 3 copies of your information (1 original and 2 backups),
- 2 different media types,
- 1 copy kept off site

Remember to test your backups!

Tips for backing up your information (ITSAP.40.002)
https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002#when

What is the current state of your backups?

Backup and encrypt data

What is encryption?

Encryption encodes (or scrambles) information, and this protects the confidentiality of the information. Even if someone attains the encrypted information they are unable to access the information.

Consider for:

- Websites
- Message applications
- Sensitive data

Using encryption to keep your sensitive data secure - ITSAP.40.016
https://www.cyber.gc.ca/en/guidance/using-encryption-keep-your-sensitive-data-secure-itsap40016

Baseline Cyber Security Control for Small-Med Orgs

CCCS Baseline Cyber Security Controls -
https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Q & A

Resources

Resources

Baseline cyber security controls for small and medium organizations – https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Best practices for passphrases and passwords (ITSAP.30.032) - https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

Developing your incident response plan (ITSAP.40.003) – https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003

How updates secure your device (ITSAP.10.096) - https://www.cyber.gc.ca/en/guidance/how-updates-secure-your-device-itsap10096

National Cyber Threat Assessment 2025-2026 - https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) - https://www.cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030

Tips for backing up your information (ITSAP.40.002) – https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002#when

Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035) - https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035

Toronto Metropolitan University

ROGERS cybersecure catalyst

Thank you

Get connected with the Catalyst today

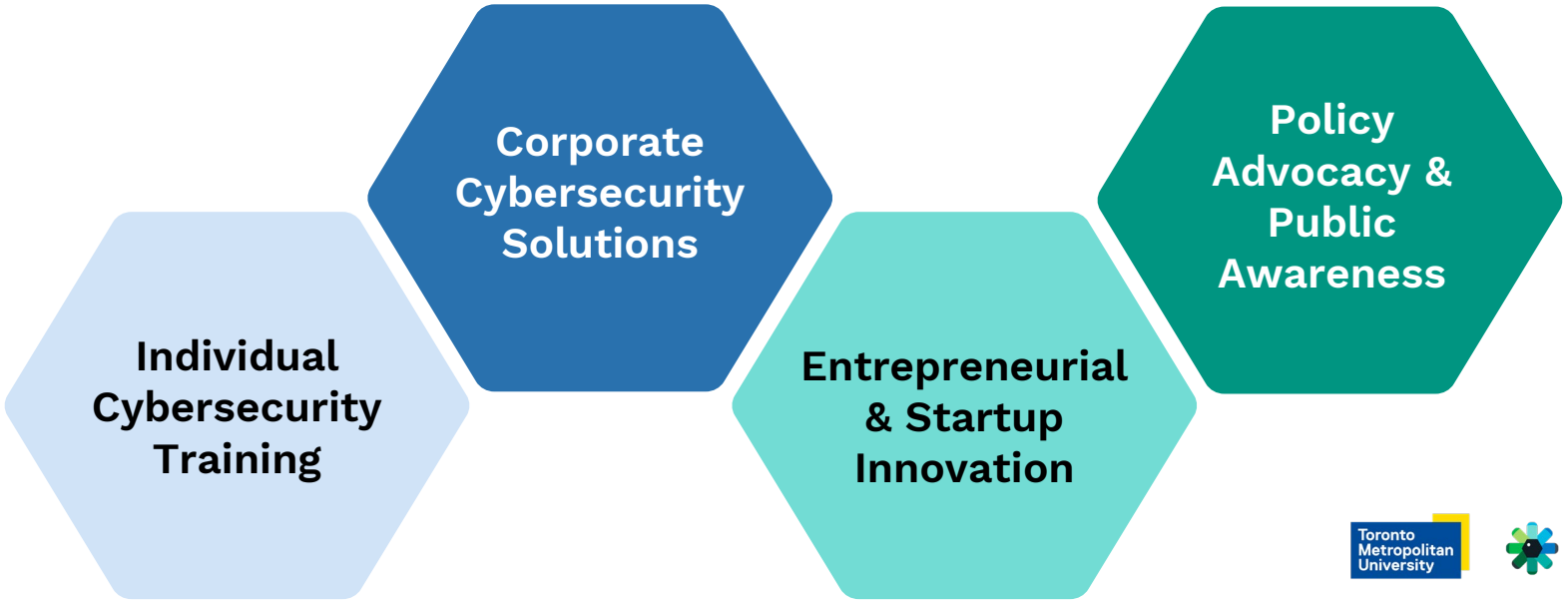
About Rogers Cybersecure Catalyst

Toronto Metropolitan University

ROGERS cybersecure catalyst

Rogers Cybersecure Catalyst

The Catalyst is Canada's cybersecurity hub. Our programs and services across the country, empower individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity. We offer:



Toronto Metropolitan University

ROGERS cybersecure catalyst

Mission

Headquartered in Brampton, Ontario, and offering programs and services across Canada, **the Catalyst empowers individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity**.

Vision

Together with our partners and collaborators, we work to realize a vision of **healthy democracies and thriving societies, powered by secure digital technologies.**

Toronto Metropolitan University

ROGERS cybersecure catalyst

Founding Partners

Canada

ROGERS

BRAMPTON innovation DISTRICT

RBC

Strategic Partners

SANS

BlackBerry

Funding provided in part by the Government of Ontario

Ontario

CCTX

Upskill Canada POWERED BY palette skills

Canada

RHEA GROUP

okta

Achieving Impact: Catalyst Milestones

- More than **7,000 people** have directly benefited from the Catalyst's groundbreaking programs
- Over **500 businesses** have been fueled by the Catalyst
- Over **800 jobs** have been created or filled in the cybersecurity sector through Catalyst programming
- More than **1,000 women, girls and non-binary individuals** have been empowered by the Catalyst
- Over **10,000** cybersecurity experts, mentors, thought leaders, entrepreneurs, program participants, alumni and partners make up the Catalyst community

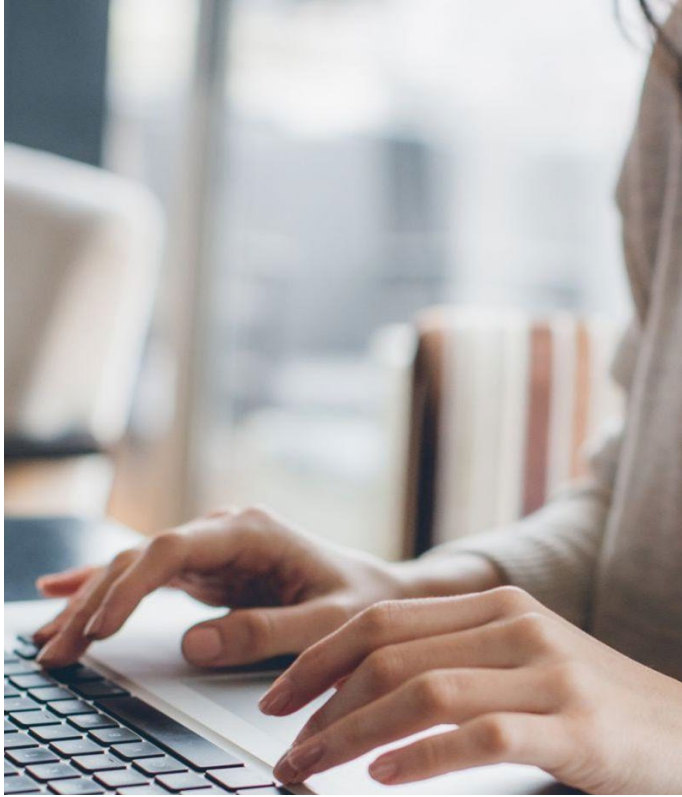
In November 2023, we brought nearly **300 cyber stakeholders** to the Rose Theater to celebrate the 5-year anniversary of Catalyst's founding

Toronto Metropolitan University

ROGERS cybersecure catalyst

Catalyst Cyber Clinic

One of the first of its kind in Canada, the Catalyst Cyber Clinic provides free cybersecurity support to under-resourced and vulnerable non-profit and social impact organizations in Canada. The Clinic is staffed by learners and graduates from Catalyst cyber training programs who, as Cyber Consultants, gain practical, real-world work experience while empowering vulnerable organizations to secure themselves.



We are a proud member of The Consortium of Cybersecurity Clinics

ROGERS cybersecure catalyst | Corporate Training

Toronto Metropolitan University

ROGERS cybersecure catalyst

okta

mastercard

Disclaimer

This disclaimer governs the use of this document. By using this document, you accept this disclaimer in full. You must not rely on the information in this presentation as an alternative to legal, financial, privacy or professional advice outside the area of cybersecurity. Notwithstanding the previous sentence, the Rogers Cybersecure Catalyst (the Catalyst) does not represent, warrant or guarantee that the use of guidance in this document will lead to a particular outcome. The Catalyst is not liable to the client in respect to any business losses, including and without limitation, loss of or damage to profits, income, revenue, use, productions, anticipated savings, business, contracts, commercial opportunities or goodwill.

This document is provided for educational and non-commercial purposes only to the intended recipient(s). Reproduction, distribution, or use of this material, in whole or in part, for any commercial purpose, including but not limited to offering services to third parties, charging fees, or incorporating into commercial products, is strictly prohibited without the express written consent of the Rogers Cybersecure Catalyst.

Connect with us

Subscribe to our **Catalyst Connect** newsletter:
cybersecurecatalyst.ca/subscribe

Follow the Catalyst on social media or email us:

@cybersecure.catalyst

linkedin.com/school/cybersecure-catalyst

cybersecurecatalyst@torontomu.ca

Toronto Metropolitan University

ROGERS cybersecure catalyst