Cyber Risk Management Workshop

Rogers Cybersecure Catalyst

Toronto Metropolitan University

ROGERS cybersecure catalyst

AMO Association of Municipalities of Ontario

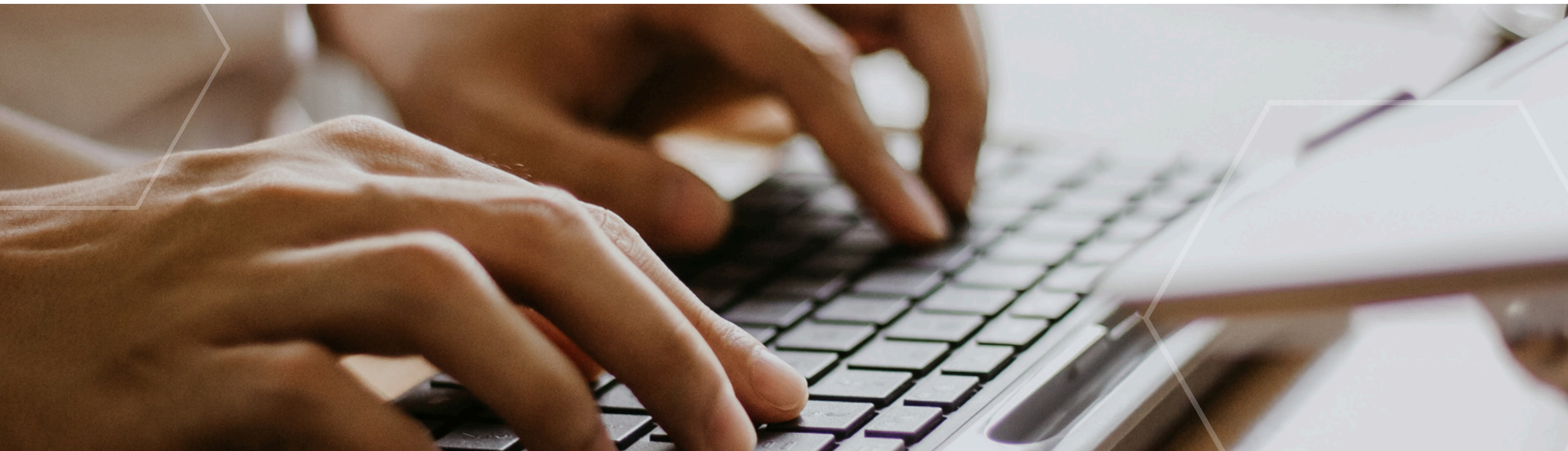
Objectives

This ½ day training session will be delivered by a Catalyst Senior Cybersecurity Advisor who will guide you through short lectures, guided discussions and activities that are focused on the following learning objectives:

1. Appreciate the cyber threat landscape within the municipal context
2. Translate cyber risks to municipal risks
3. Coordinate mitigating actions
4. Integrate risk-based decision-making in cybersecurity incident response

Outcomes

This session will orient municipal risk managers and their staff with the concept of cyber risk and how to mitigate it through technical and non-technical actions. Upon completion of this session, risk managers and related staff will have the knowledge needed to better assess cyber risks and have the outline of a plan to address key risks.



Agenda

Component	Topics	Timing
Introduction	Session overview and introductions	10:00-10:15
Module 1 – Municipal cyber threat landscape	General threats Organizational cyber threats and threats to critical infrastructure Activity	10:15-10:45
Module 2 – Municipal cybersecurity	Risks to: • Municipal operations • Critical infrastructure • Public safety • Quantifying and qualifying cyber risk • Activity	10:45-11:15
Break		11:15-11:30
Module 3 – Coordinating mitigating actions	Risk treatment and mitigation Risk tolerance Technical and non-technical security controls Who can help? Facilitated discussion	11:30-12:15
Module 4 – Risk and incident response	Integrate risk-based decision-making in cybersecurity Incident response	12:15-12:45
Conclusion	Review of objectives and key points	12:45-01:00

Key Terms

Threat	Any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise.
Attack surface	All points on any surface (digital, human, physical) where an deliberate threat actor can launch an attack, a.k.a threat surface.
Attack vector	The pathway or means of the attack (email, password cracking, backdoor, etc.)
Risk	Uncertainty on achieving organizational objectives. A probability exists that there could be damage, injury, liability, loss, or any other consequence from an event. Likelihood + impact = risk
Exposure	The total risk created by exploitable vulnerabilities across the system or attack surface.
Vulnerability	A weakness – Any factor – human, technical or physical - that could increase susceptibility to compromise.
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (e.g., keys, metadata, or other security-related information) or the unauthorized modification of a security-related system, device or process in order to gain unauthorized access.
Security Control	A technical or non-technical that satisfies a specific security requirement (a.k.a. safeguard).

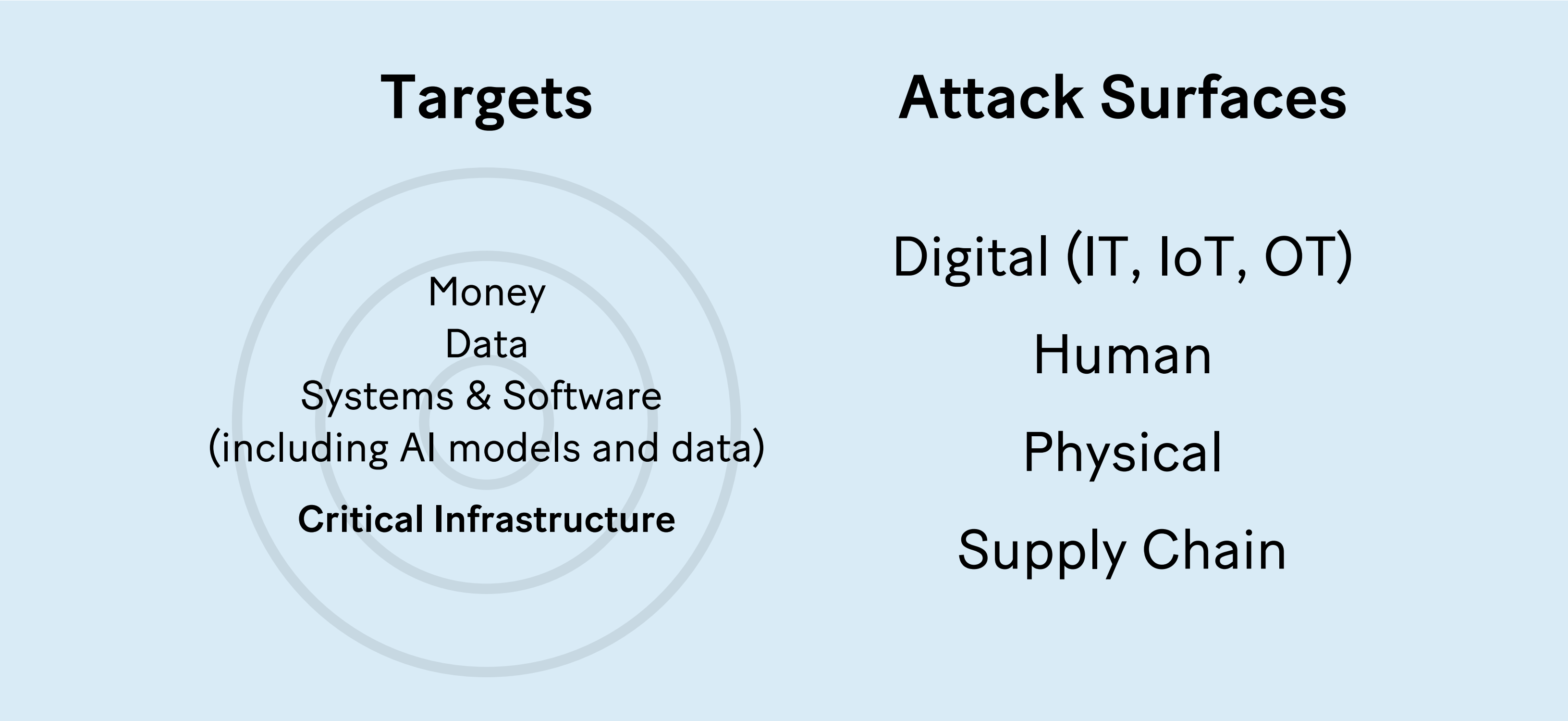
Municipal Threat Context – A Primer

There are several aspects to the threat that are critical to effectively managing the cybersecurity picture for your municipality.

1. Remain apprised of the general threat landscape in the municipal context.
    - Read the Canadian Centre for Cyber Security's An introduction to the Cyber Threat Environment and National Cyber Threat Assessment.
    - Have your technical team subscribed to the Alerts and Advisories from Cyber Security Ontario and keep you up to date on significant changes to the threat landscape.

2. Consider not only deliberate threats, but the potential for accidents or natural events to have an impact on municipal systems, software and services.

3. Consider high value targets and the potential attack surfaces.



Targets

Money
Data
Systems & Software
(including AI models and data)
Critical Infrastructure

Attack Surfaces

Digital (IT, IoT, OT)
Human
Physical
Supply Chain

Figure 1 — Municipal targets and attack surfaces

4. Run through potential threat scenarios that may relate to your municipality to determine the potential likelihood and severity of impact including:

- Deployment of malware including ransomware
- Denial-of-service attacks
- Phishing campaigns
- Supply chain attacks
- Vulnerability exploitation and compromised credentials
- Insider threats

5. Ensure there is a current risk assessment that determines priority risks and potential technical and non-technical security actions to prevent and properly prepare for cyber events. If you have the resources, encourage the IT and cyber team to conduct threat modelling or employ a threat management service.

6. Maintain awareness of the changes in your municipality, your technological or threat context so that you can identify how they might influence your cybersecurity posture.

Translating cyber risk to municipal risk

One of the most significant opportunities to help leaders and managers better appreciate the value of cybersecurity is through ensuring that cyber risks are translated into business risk.

It's common for cybersecurity professionals to discuss threats and impacts to systems, software and data in technical terms. For example, a report from a cyber incident might be:

> *"Our F3-2023 server has been encrypted by ransomware."*

While these may be technically accurate descriptions, senior leaders and other business stakeholders are often left to trying to interpret what that might mean. Depending on their understanding of how that particular technology enables the business, the potential impacts may not be clear.

Organizational leaders should be prepared to address critical risks and be able to engage in effective decision-making during a cyber incidents. To help them fulfill these crucial tasks, you may find it helpful to translate cyber risks to business risks. Using the previous example, a more comprehensive, translation of the cyber risk that expresses business impacts and risks would be:

> *"Our financial has been encrypted by ransomware. This means that we do not have any access to files that support organizational administration such as payroll, contracting and accounts receivable / payable. As well, there is sensitive corporate information on that server including important financial data on the company as well as sensitive data about our clients. So, in addition to the financial risks associated with the unplanned costs in dealing with this incident, we are potentially exposed to compliance, legal and reputational risk that could also have financial and strategic impacts."*

As you work through the translation process, consider the five suggestions below.

Maintain Business Focus

Understand the cyber risks in terms of business impacts and how cyber incidents may impede achievement of business goals and priorities.

Have Data

Leverage data that can help qualify and quantify the cyber risks and impacts such as revenue loss, downtime of services, asset loss, costs for response and recovery, loss of potential customers etc.

Use Visual Aids

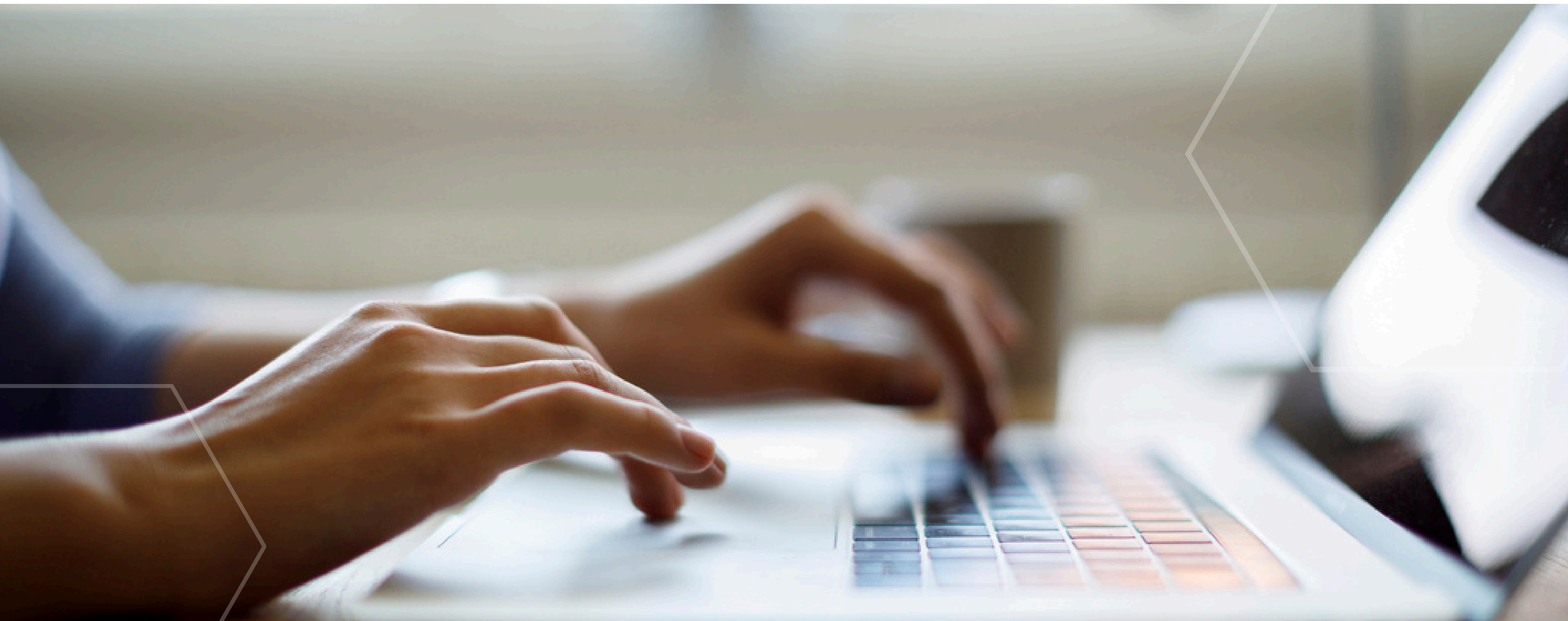
Apply data visualization techniques to help explain the cyber risks such as risk heatmaps, dashboards, improvement charts, etc.

Avoid Jargon

Speak to business stakeholders in their terms. This may mean that you have to familiarize yourself with business terms as well as the various business lines within your organization.

Tailor to the Audience

Understand the perspectives of the different business stakeholders and what would be important to them and their business. Consider the different needs of different audiences: C-suite executives, business line owners, data managers or others.



Selected References

Association of Municipalities of Ontario (2023), Municipal Cyber Security Toolkit, https://www.amo.on.ca/policy/finance-infrastructure-and-economy/municipal-cyber-security-toolkit

Canadian Centre for Cyber Security (2023), Information for Government Institutions, https://www.cyber.gc.ca/en/government-institutions

Cybersecurity and Infrastructure Security Agency (2023), https://www.cisa.gov/

Government of Ontario (2023), GO-ITS 25.0 General Security Requirements, https://www.ontario.ca/page/go-its-250-general-security-requirements

National Institute for Standards and Technology (NIST) (2023), Cybersecurity Framework 2.0, https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

NIST (2012), Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Public Safety Canada (2023), Critical Infrastructure, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

About the Catalyst

Rogers Cybersecure Catalyst is Toronto Metropolitan University national centre for training, innovation, and collaboration in cybersecurity. Headquartered in Brampton, Ontario, the Catalyst is home to ground-breaking training and certification programs; unique innovation programming for start-ups & scale-ups; a first-of-its-kind cyber range; wide-ranging public education programs; and many other cybersecurity programs and initiatives.

The Catalyst offers many corporate cyber training offerings, both on-site and virtual, across Canada. Our range of services are:

- Interactive & experiential — minds-on, hands-on training that is engaging and practical.
- Customizable — we tailor our offerings to your specific organizational needs and sector.
- Inclusive — we offer targeted training for every level of employee - executive, technical, non-technical.

Our training solutions include:

- Tabletop exercises
- Incident response planning workshops
- Technical exercises in the Catalyst Cyber Range
- Non-technical and technical workshops

Contact us today

Catalyst cyber experts and trainers will work with you to develop a training solution that meets your needs, goals, and budget.

✉ catalyst.corporate@torontomu.ca

🌐 cybersecurecatalyst.ca/cyber-training-for-municipalities

Toronto Metropolitan University

ROGERS cybersecure catalyst

AMO Association of Municipalities of Ontario