Toronto Metropolitan University

ROGERS cybersecure catalyst

Municipal Cybersecurity Risk Management Workshop

23 October 2024

Your facilitator

Randy Purse CD, PhD, CTDP

Senior Advisor, Cybersecurity Training and Education

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Participant introductions

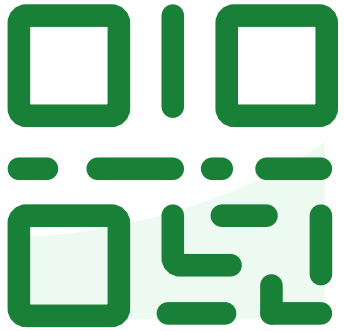
Who are you and what is your role?

What are your expectations for this workshop?

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

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



Join at slido.com
#3747839

ⓘ Start presenting to display the joining instructions on this slide.

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

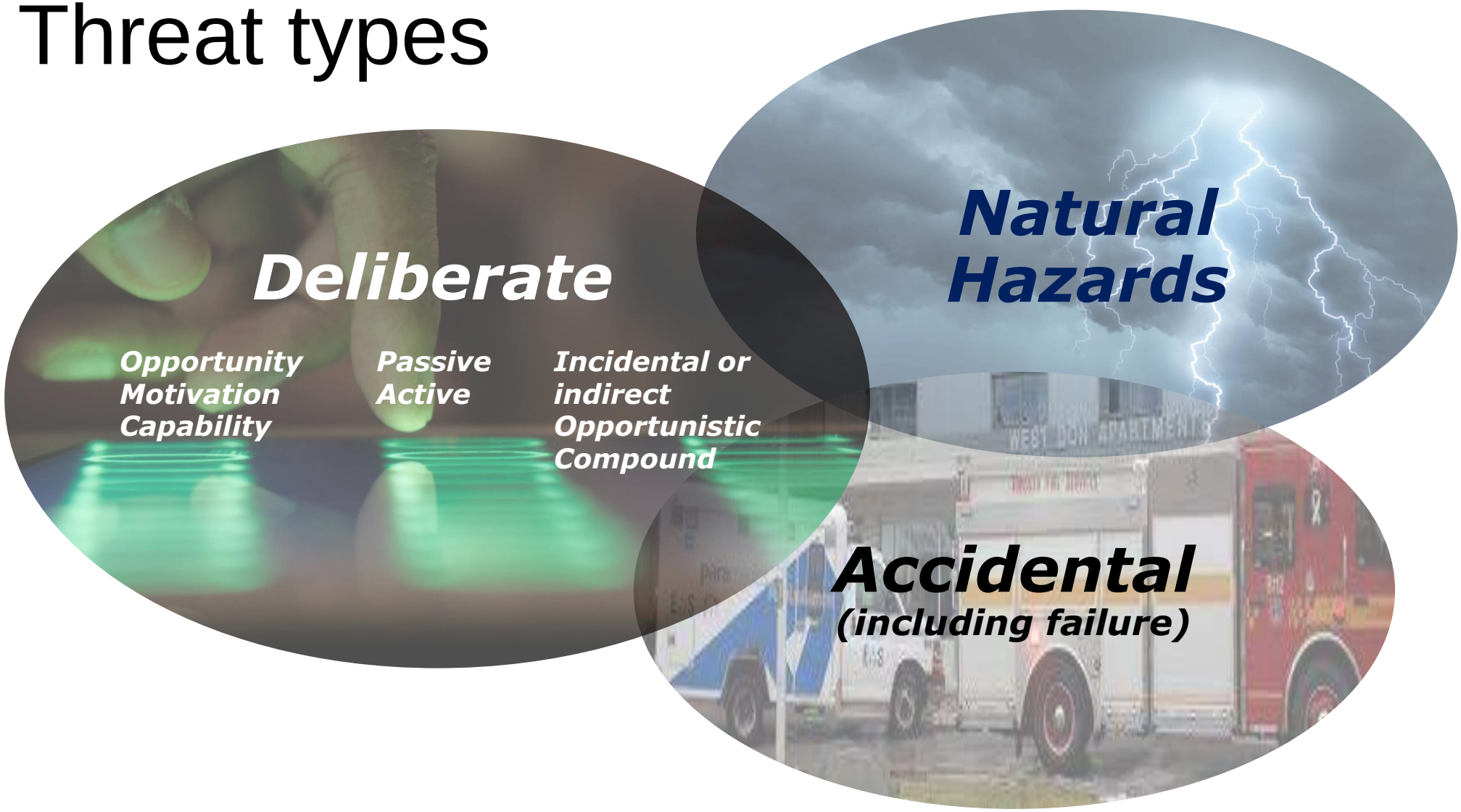
Municipal Threats

Appreciating the cyber threat landscape within the municipal context

Digital Dependencies

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Threat types



ROGERS cybersecure catalyst | Corporate Training & Cyber Range

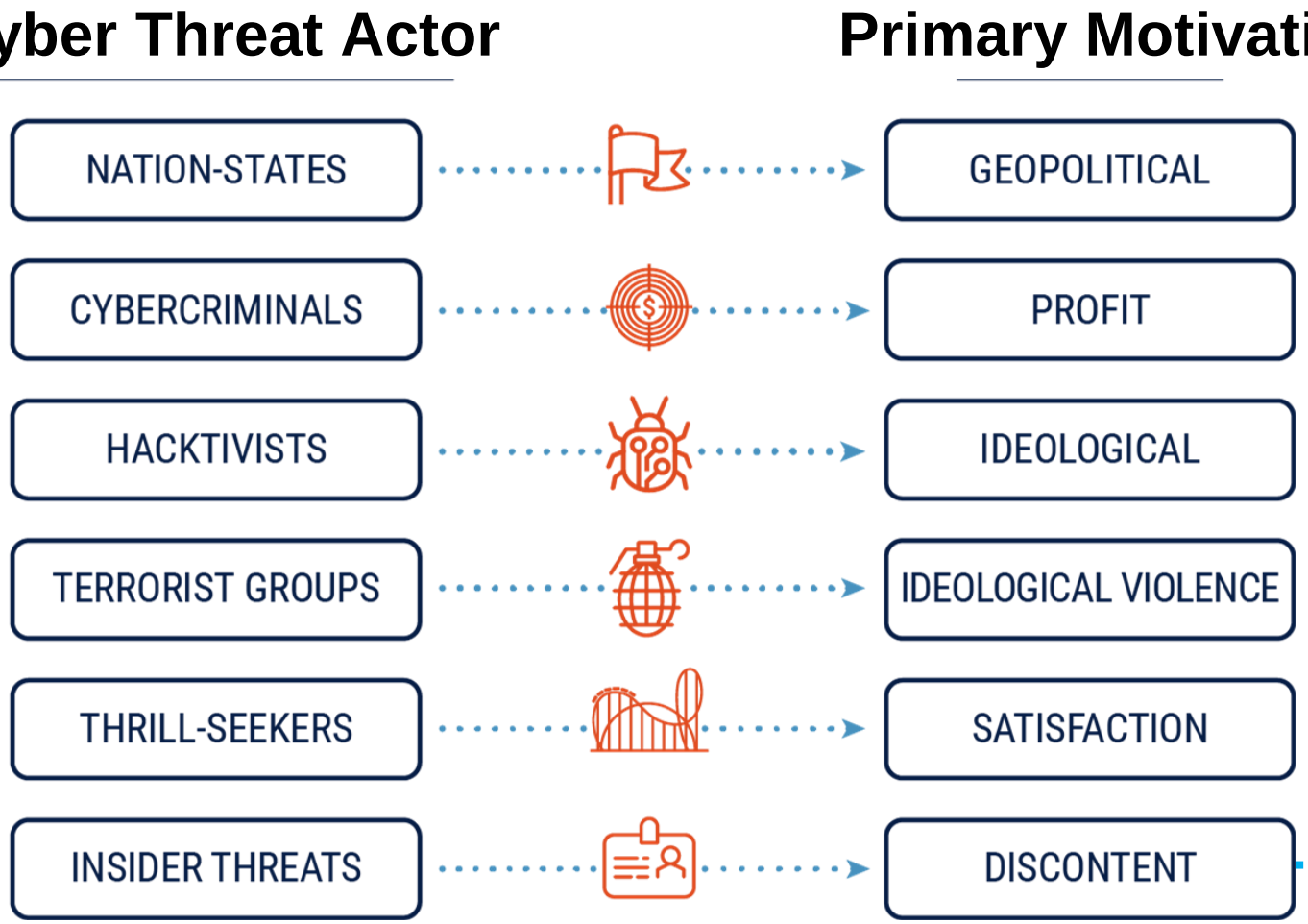
8

Threat Landscape

Ransomware
Critical Infrastructure
State or State-sanctioned Activities
Online Trust
Disruptive Technologies

- Vulnerability exploitation (#1 vector)
- Compromised accounts
- Low cost and high impact ‘user friendly’ malware
- Supply chain attacks
- Insider threats – cybercrime and espionage
- Increased frequency of:
  - Natural hazards – climate change
  - Accidental occurrences – system complexity, changes, etc.
- Rapidly evolving technology (AI and emerging quantum threats)

Deliberate threats



Different:

- Motivations
- Funding
- Sophistication
- Resources

Incl. partners, supply chain (close access)

Source: Canadian Centre for Cyber Security (2018), *An Introduction to the Cyber Threat Environment* https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environmen

Common deliberate threats

- **Hacking** – Identifying and exploiting technical vulnerabilities to gain unauthorized access.
- **Social engineering** – Psychological manipulation of people into performing actions or divulging sensitive information against the best interests of the organization.
- **Malware** – Malicious software intended to do harm – e.g. damage, encrypt, spy, manipulate, delete, or steal.
  - Ransomware – file encryption followed by ransom demand
- **Insider threat** – An individual with authorized access to systems, software, or data that intends to do harm to the organization.

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

TARGETS

Money

Data

Systems and software

(including AI models and data)

Critical Infrastructure

ATTACK SURFACES

Digital
(IT, IoT)

Human

Physical

Supply Chain (Third party services)

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Activity: Identify primary threats

What do you think are the predominant cyber threats to **your** municipality?

- Municipal operations
- Critical infrastructure

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Cyber Risk

Translating cyber risk into municipal risk

Cyber risk (a.k.a. digital risk)

The likelihood of loss or harm related to a compromise of an organization's digital information or digital systems (including IT, OT, IoT).

When assessing likelihood and severity of impact consider:

- Immediate effects
- Extended impacts

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Municipal risk factors

Do you ….?

- ❑ Use or store personal data
- ❑ Possess financial information
- ❑ Have a wide range of end users
- ❑ Have multiple device / tech environment
- ❑ Employ commercial IoT
- ❑ Use connected facilities systems (OT)
- ❑ Have limited cyber security investment
- ❑ Leverage new or unproven technologies
- ❑ Allow users a broad range of permissions
- ❑ Allow for use of unsanctioned applications

Translating cyber risk to municipal risk

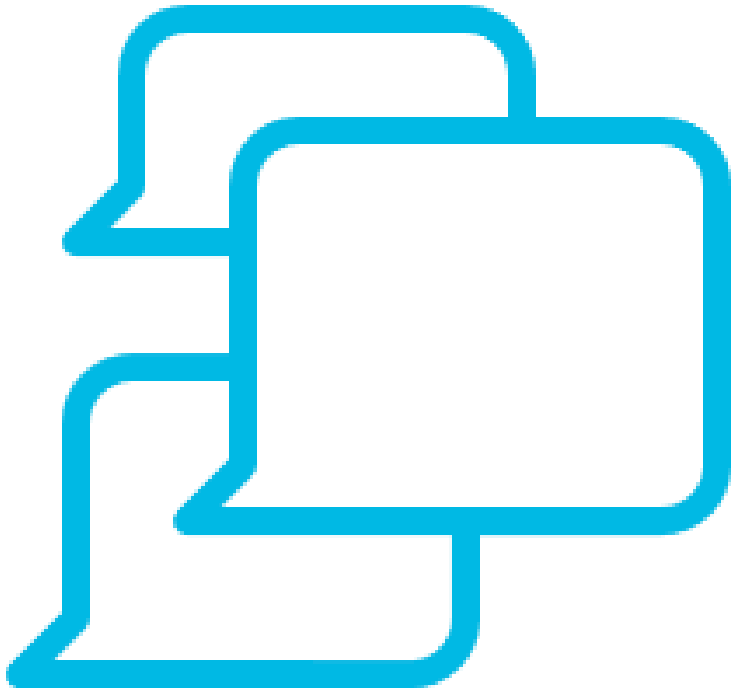
- A vulnerability is exploited and a hacker gains access to detailed financial information about your municipality (contracts, financial commitments, etc).
- An employee clicks on a weblink in an email that launches ransomware that restricts access to your administrative network.
- A skilled, disgruntled citizen launches a denial-of-service attack against your municipal website/social media accounts.
- A digital copy of your tax roll is saved on a USB by and employee and then lost.
- After a recent software update, malware is found on the operational water treatment system.

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Discussion: Municipal impacts

What are some of the potential impacts of a cyber incident?

- *Technical*
- *Operational*
- *Financial*
- *Legal Impacts*
- *Life & Safety Impacts*
- *Strategic Impacts*
- *Reputational*
- *Political*



Cybersecurity and compliance

Compliance is necessary

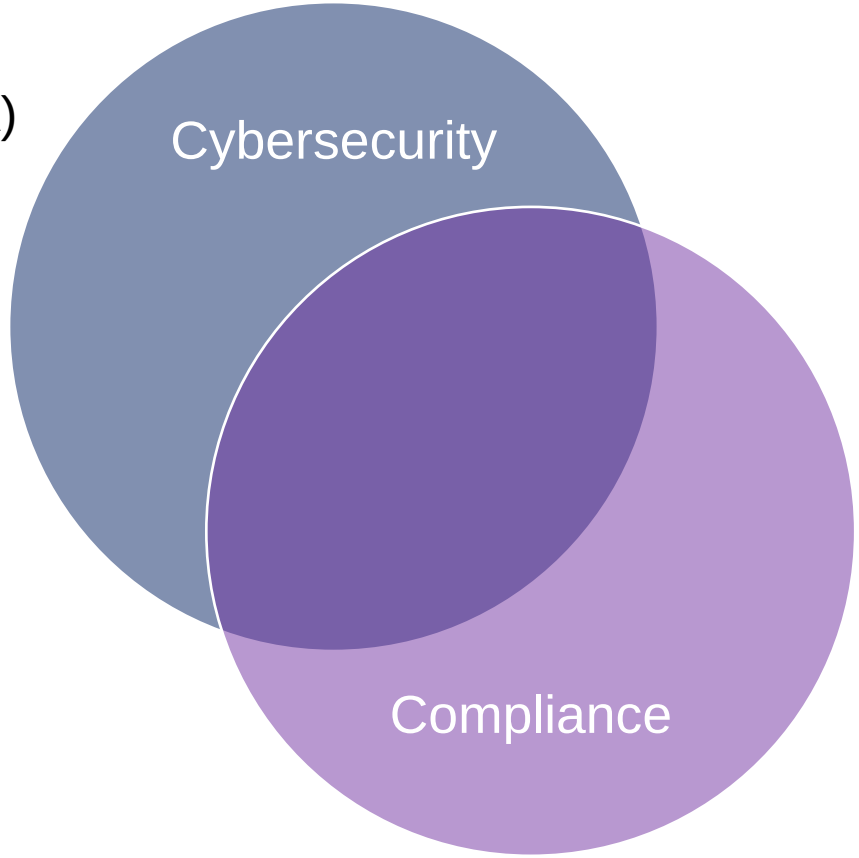
- Freedom of Information and Protection of Privacy Act (FIPPA) (Ontario)
- Personal Information Protection and Electronic Documents Act (PIPEDA National)
- Impending legislation (Bill C-26 for Critical Infrastructure)

Compliance does not equal security

- Cybersecurity – Protecting data and digital systems
- Compliance – Expectation for adherence to specific requirements

Compliance does not necessarily reduce other risks

- Legal, reputational, operational, and HR risk

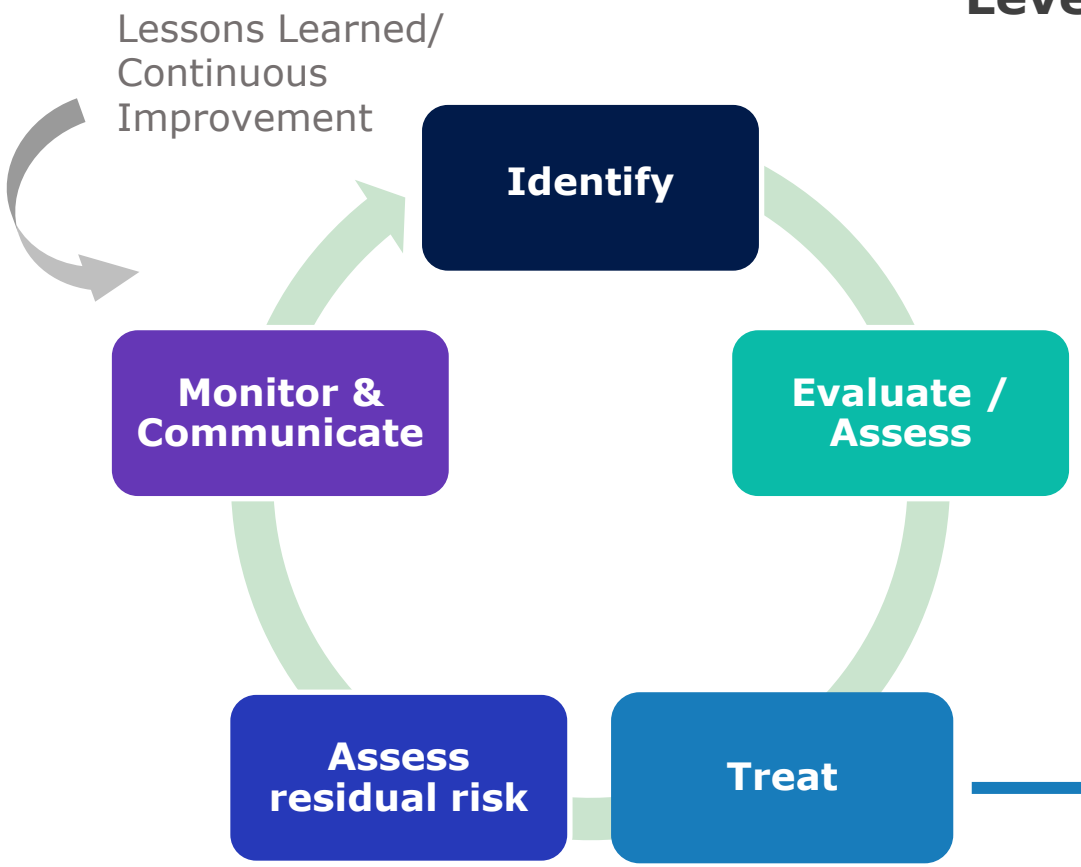


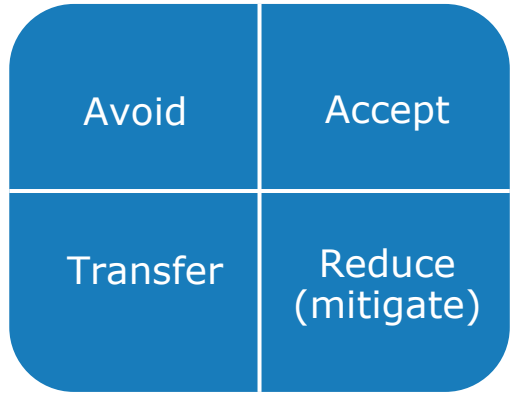
ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Risk Management

A strategic (ongoing) process that identifies, assesses and takes steps to control risks.

Risk = uncertainty
Level of risk = **likelihood** **and** **impact (severity).**





Residual Risk: *Level of risk remaining after measures have been applied*

Risk Appetite: *Amount of risk desired to pursue objectives*

Risk Tolerance: *Readiness to bear risk after risk treatment*

Source: Adapted from ISO Guide 73:2009 Risk Management – Vocabulary
https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

A framework for discussing cyber risk

Quantifying and qualifying risk

IMPACT		PROBABILITY (LIKELIHOOD)	
1. Assets at Risk **(potential for harm to organization or others)**	**2. What if the assets are compromised? (CIA and value)**	**3. Vulnerabilities** **(digital, human, physical, supply chain)**	**4. Threats** (deliberate, accidental, natural hazards)
Intangibles (reputation, trust, IP, compliance)			
Tangibles (financial, physical, production, infrastructure)			
Greater good (health/safety, environment, civil liberties, privacy)			

Adapted from World Economic Forum, Advancing Cyber Resilience 2017

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Activity: Define and communicate cyber risk

- Select a common threat to your municipality.
- What are the potential impacts?
- What is at risk? Go beyond the technical.
- Be prepared to provide a short summary (1 min).

Example – A DoS attack against our municipal website will result in a web service disruption that will impact client service and carry both operational and reputational risk. There will likely be financial costs to both addressing and cleaning up the attack. There may be other risks depending on other web-based services affected.

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Coordinate mitigating actions

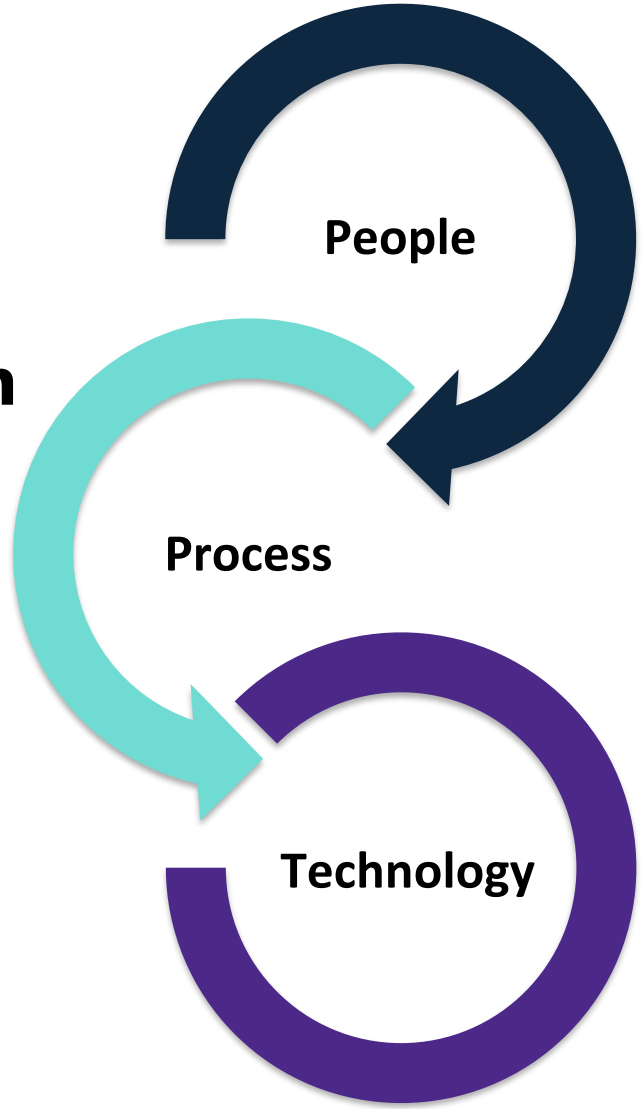
Mitigating cyber risks

Cybersecurity & organizational resilience

Cybersecurity

"…**is the protection of digital information and the infrastructure on which it resides."**

(National Cyber Security Strategy, 2018)



Resilience

'There's no such thing as 100% security'

- Resilience:
  - Failing securely
  - Maintaining operations
  - Recovering safely, securely, & quickly

What are we trying to protect?

The CIA triad and **protecting** important **data and systems throughout their lifecycle**.

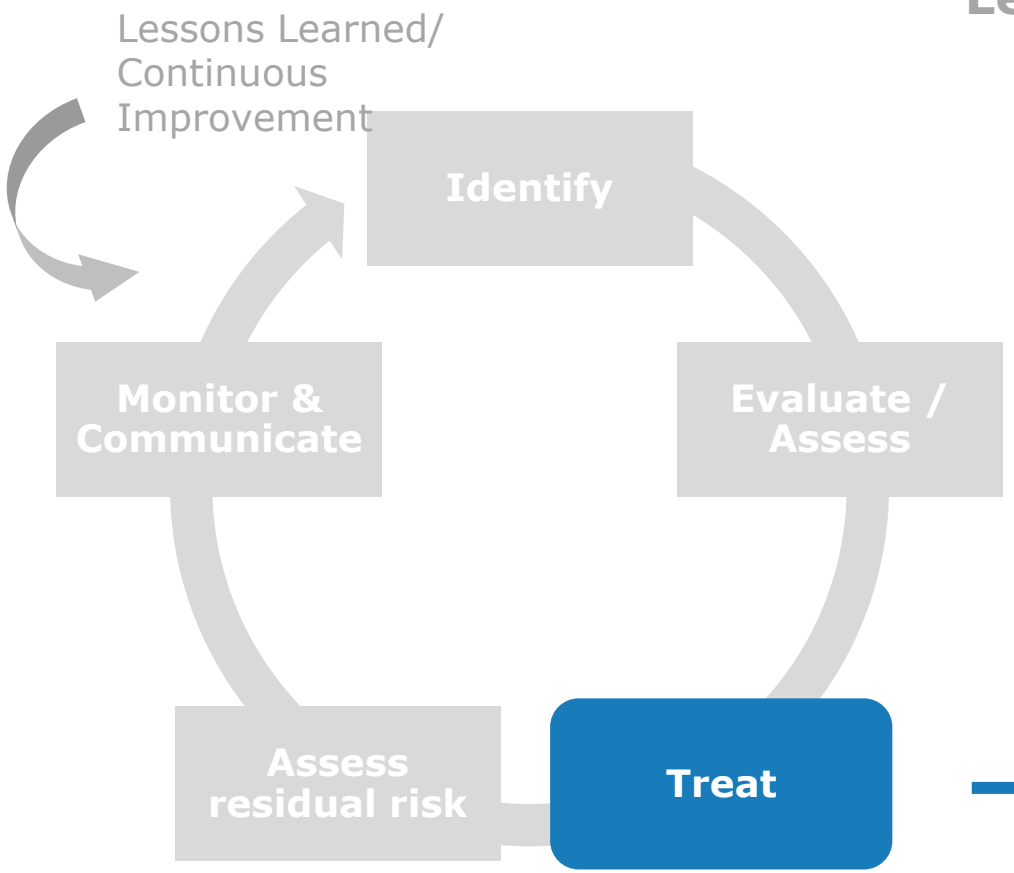
Principle	*Primary Concern*
CONFIDENTIALITY	***Unauthorized access*** *- What data or systems do you work with that is sensitive and should not be disclosed to unauthorized parties?*
INTEGRITY	***Unauthorized manipulation*** *- What data or software needs to be authentic, accurate, and complete, and upon which systems do they reside?*
AVAILABILITY	***Degradation or loss of access*** *- What important data, software or systems do you rely upon?*

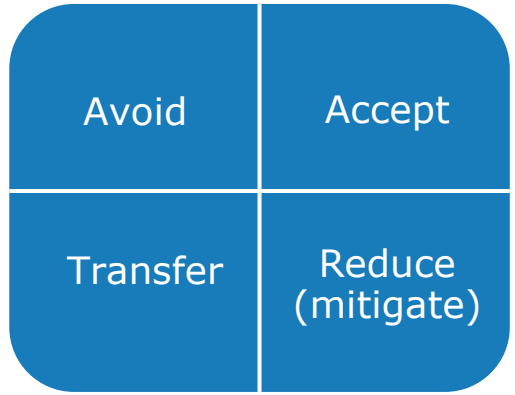
ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Risk Management

A strategic (ongoing) process that identifies, assesses and takes steps to control risks.

Risk = uncertainty
Level of risk = likelihood and impact (severity).





Residual Risk: *Level of risk remaining after measures have been applied*

Risk Appetite: *Amount of risk desired to pursue objectives*

Risk Tolerance: *Readiness to bear risk after risk treatment*

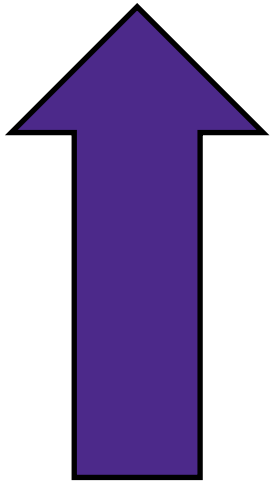
Source: Adapted from ISO Guide 73:2009 Risk Management – Vocabulary
https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

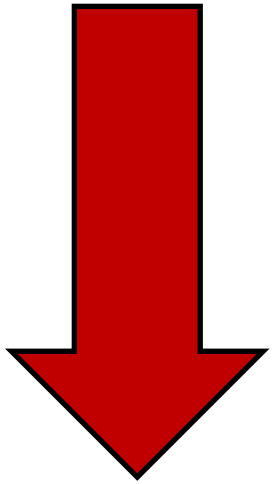
ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Managing risk through security control selection

Security

(within organizational constraints)





Risk

(to an acceptable level)

Non-technical Best Practices

1. **Establish governance** - Define roles and responsibilities, authorities, processes
2. **Maintain Asset Inventory –** Know what you need to protect
3. **Identify cyber risks** - Create a cross-functional risk committee and develop a risk register
4. **Plan** - Develop an incident response plan (IRP). Review your business continuity / disaster recovery plan
5. **Implement role-based training and awareness**
   - Employee detection and response
   - Management team training
   - IT first responders & technical team training
   - IRP exercises – to orient, train and improve all IR functions
6. **Consider cyber insurance –** If it makes sense & is worth the cents
7. **Engage partners & suppliers** - Review and clarify third party service provider and shared responsibilities

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Technical Best Practices

1. **Install and activate security** applications/tools such as anti-virus, firewalls, detection systems, etc.
2. **Test / verify** your system & device security against known threats (e.g., vulnerability assessments and pen testing)
3. **Patch /update** software and systems
4. **Enable end-point detection and response (e.g. EDR)**
5. **Implement effective identity and access management**
   - Password / passphrases
   - Multi-factor authentication (MFA)
   - Least Privilege
6. **Segment networks/systems**
7. **Conduct regular backups and testing** – *At least* 3,2, 1 rule of thumb:
   - 3 copies of critical data
   - 2 copies stored in separate locations
   - 1 copy stored off-site/offline (immutable backup)

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Who can help? (Examples)

Resources

- Internal
- Other municipalities
- Local organizations / companies
- Insurer
- Internet Service Provider / Cellular Service provider
- Third-party services (IT, security, cloud)
- Third party software (security software, data management)
- AMO LAS (Cyber prevention and incident response)
- The Rogers Cybersecure Catalyst (Training and exercises)
- Canadian Internet Registry Authority (CIRA) (DNS Firewall and Security Awareness)

Guidance

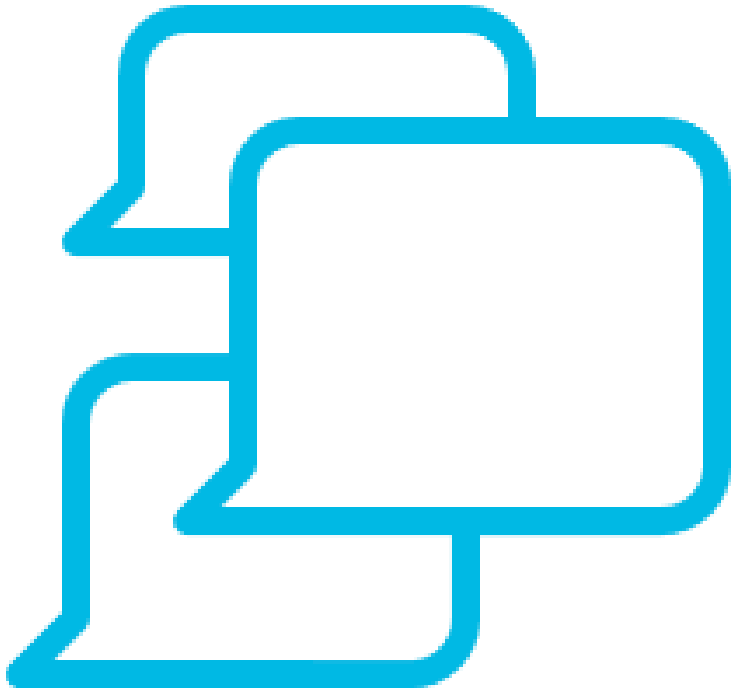
- Cyber Security Ontario
  - Advice and guidance
  - Learning portal
- Privacy Commissioner
- AMO Cyber Tool Kit
- Canadian Centre for Cyber Security
- National Institute of Standards and Technology (NIST)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Center for Internet Security (CIS)

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Discussion: Coordinating actions

What are the internal challenges?

- Acquisition and financing
- Testing and Implementation
- Policies and processes
- Training
- Maintenance



What are the challenges with external stakeholders such as:

- Municipal partners?
- Contracted services?
- Public?

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Integrate risk-based decision making into incident response

A tabletop experience

Participant Guidelines

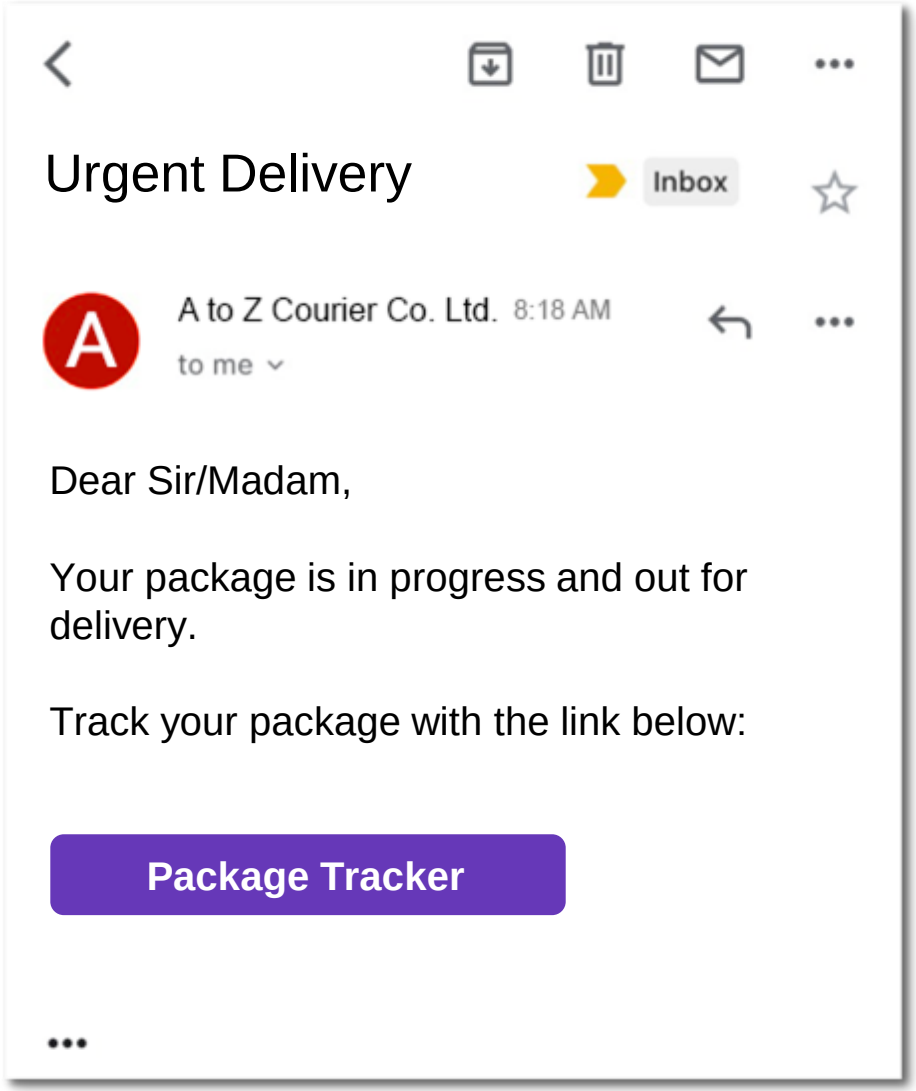
- Consider the scenario in your current role and context
- Accept scenarios at face value
- Stay engaged, focus on the situation, explain decisions and their implications. Consider relationships and expectations.
- This is a safe, threat-free learning environment so think out loud.
- Explore potential gaps or opportunities for improvement.
- **REMEMBER:** this is for learning and improvement**.**

Start of Exercise

Toronto Metropolitan University

ROGERS cybersecure catalyst

Good afternoon! (or is it?)



Report from the helpdesk –

Apparently, an employee in the finance department clicked on an email supposedly from a courier.

His screen went blank for about a minute and then…

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

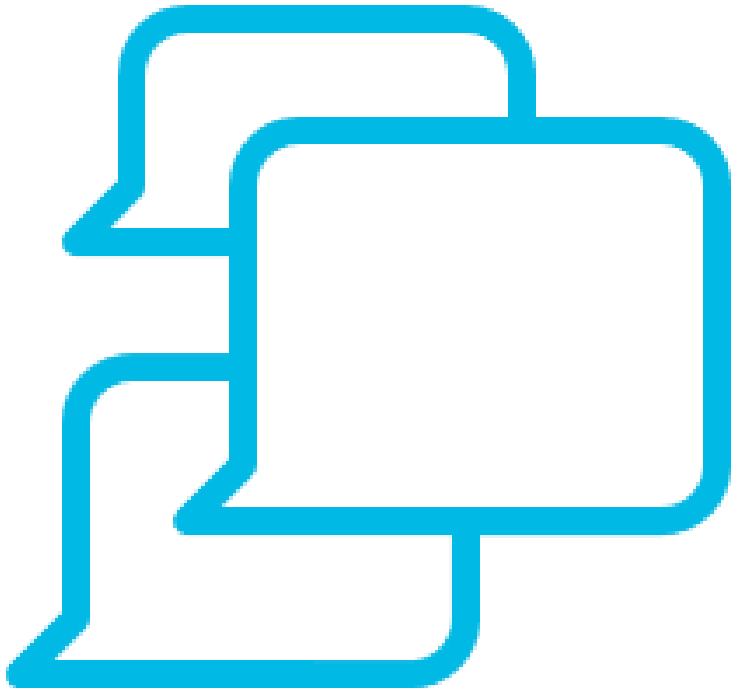

Payment will be raised in:
070
39
hrs
mins
All files will be deleted in:
166
39
hrs
mins
Your files have been encrypted with a special key.
To get access to the key and regain access to your files, you will need to pay the ransom of $500,000 by the time indicated.
If you try to recover your files yourself or you do not pay, your files will be destroyed.
See the instruction below to pay the ransom in bitcoin. If you have any difficulty, click the "Contact Us" link and it will connect you with someone who can help.
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $500,000 worth of bitcoin to this address:
QR Code
Copy
Check Payment
Decrypt

Do you have a cybersecurity incident response plan?

ⓘ Start presenting to display the poll results on this slide.

Initial Assessment and Actions

- What are your primary concerns at this point?
- What are the first steps that need to be taken?
- What is the escalation protocol (to whom and when)?
- Who else needs to know?
  - Legal counsel
  - Third-party security or IT services
  - Insurer
  - Law enforcement
- Are these in your plan?



Ransom Payment—an Ethical Decision

- Has this situation been discussed?
- What are the risks to paying or not paying?
- Do you have cyber insurance and what can you claim?
- If you choose to pay:
  - How would you do it?
  - What are the implications?

Situation Report: + 1.5 hours

- Ransomware considered legitimate
- All users locked out from the targeted server.
- Triage and investigation ongoing.
- Containment actions in progress.
- Courses of action being considered.

- What else should be happening beyond technical actions?

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

MaryMary
@superaccountant22

OMG! Our office been the target of a cyber attack. All work has stopped in my office. I'm not sure why I'm still here!!! I can probably still work from home if they would just let me.

12:15 PM • Oct 10, 2024 • X Web App

DavetheKnave
@MayorWatch

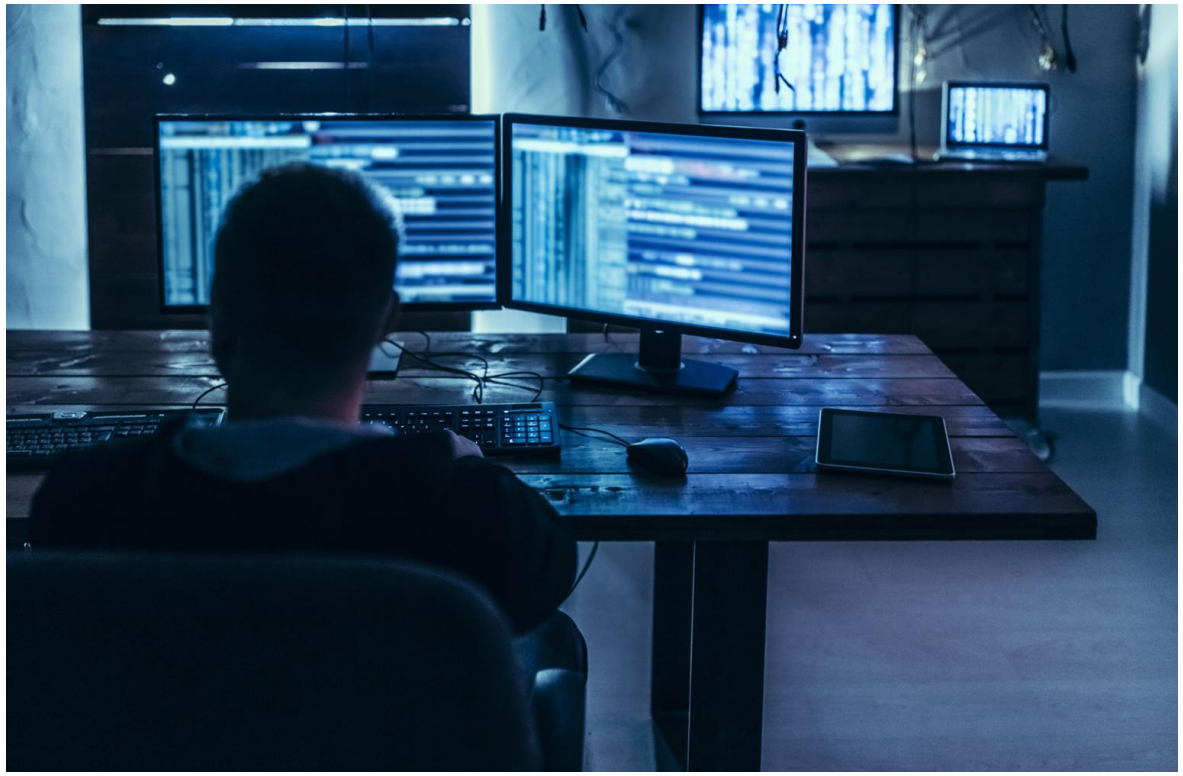
So apparently the mayor's office has been hit by ransomware but they haven't told us yet? Why haven't they said anything? What are they hiding?

12:30 PM • Oct 10, 2024 • X Web App

For exercise purposes only

LIVE NOW

Municipal Office under cyber attack—attackers reportedly asking for $500,000 payment



Full extent of the attack on is still unknown, and it is unclear whether employee or client data have been compromised.

Follow the latest on this developing story.

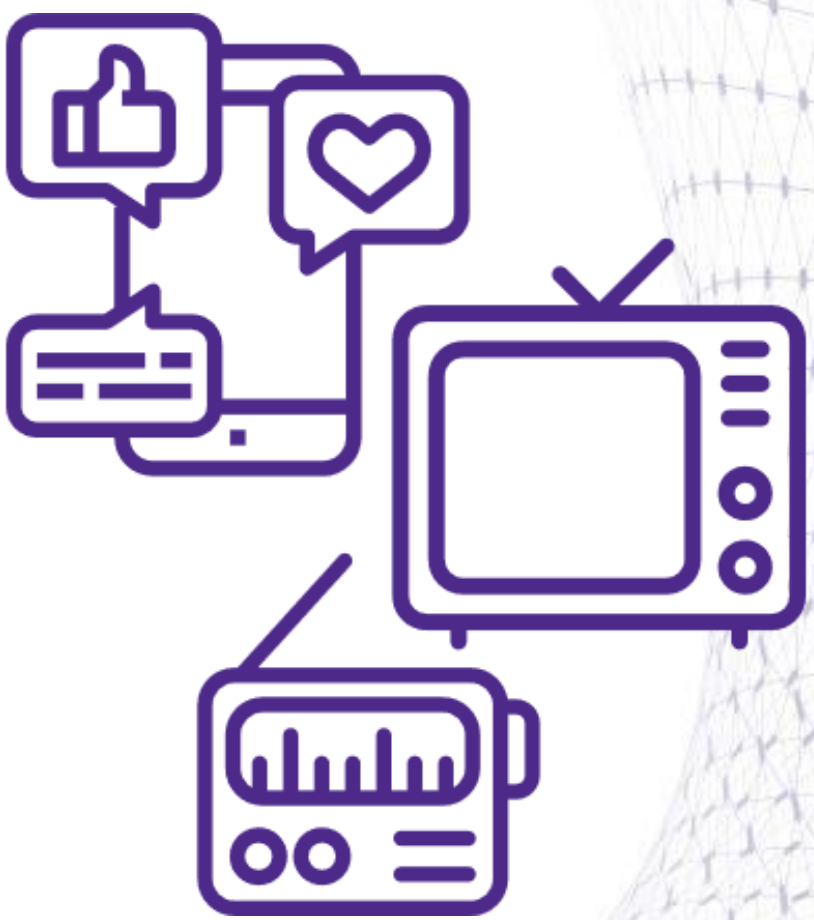
More Top Stories

Do you have communications protocols for cybersecurity incidents?

ⓘ Start presenting to display the poll results on this slide.

Communications Strategy

- How is ‘the message’ managed?
- Are there draft scripts or templates ready?
- Is there a crisis management team?
- What about other stakeholders and what should they hear?
- Do you have coordination on messaging with third party service providers?



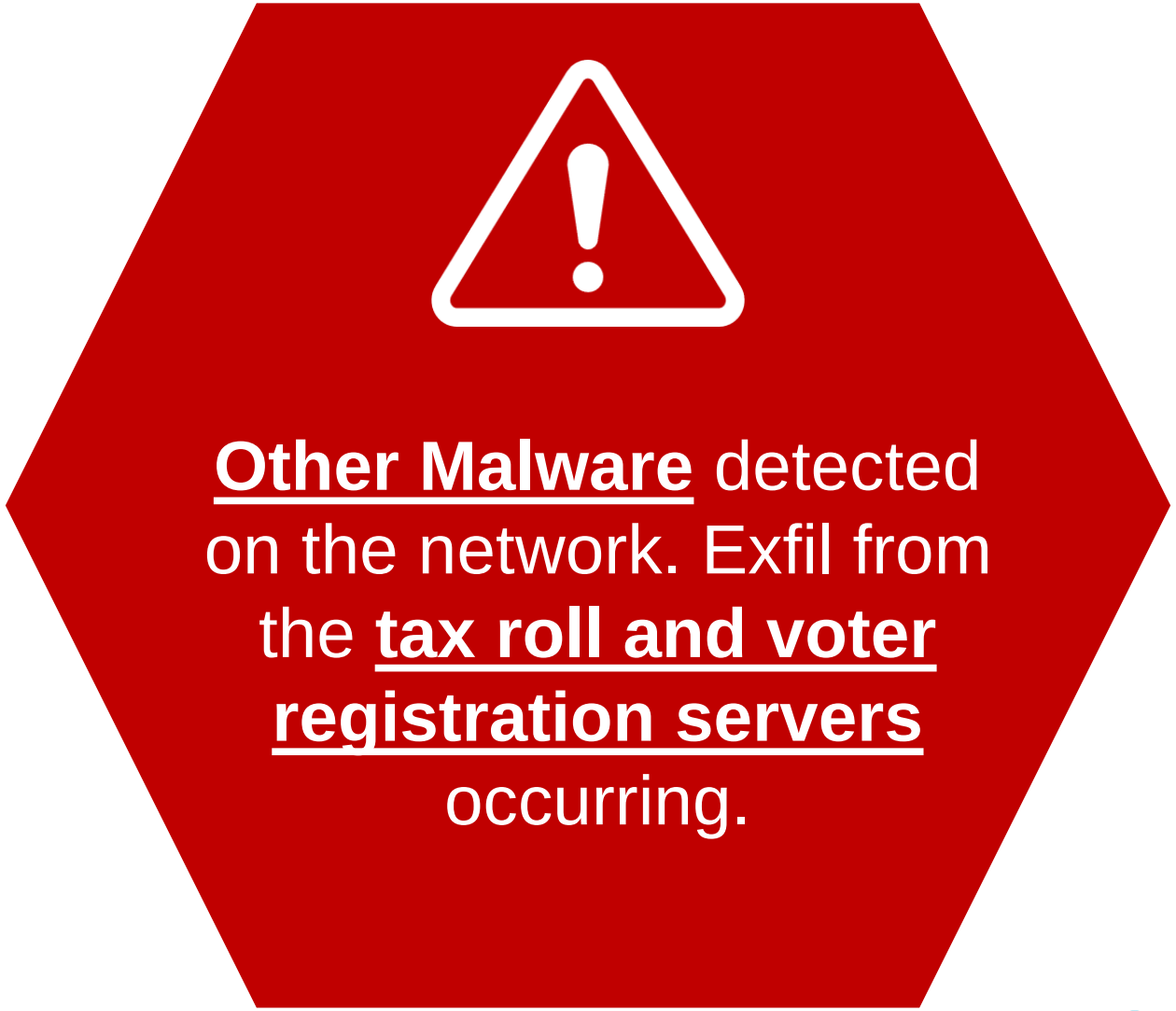
Situation Report: + 15 Hours

- The ransomware is assessed as fully contained; enterprise being closely monitored
- Technical workarounds are almost completed to return disrupted services
- Backups have been tested and recovery may start as early as tomorrow morning
- Initial public statement released on organization’s website and social media accounts
- Law enforcement coming on site tomorrow

Things are looking up!

ROGERS
cybersecure
catalyst

Corporate Training
& Cyber Range


Other Malware detected on the network. Exfil from the **tax roll and voter registration servers** occurring.

Discussion: Additional risk assessment

- What is the potential injury and impact now?
- What are the risks?
- How might this change the scale of the incident and the urgency?
- Is there anyone else who needs to know?
- What should the messaging be?
- How might this influence your communications strategy?

Situation Report: + 24 Hours

- New ticket raised and another investigation commenced for the recent incident
- Initial investigation - Attack through escalation of privileges through the targeted workstation
- Additional 3rd party specialized services being considered
- What else should be going on?

Situation Report: + 72 Hours

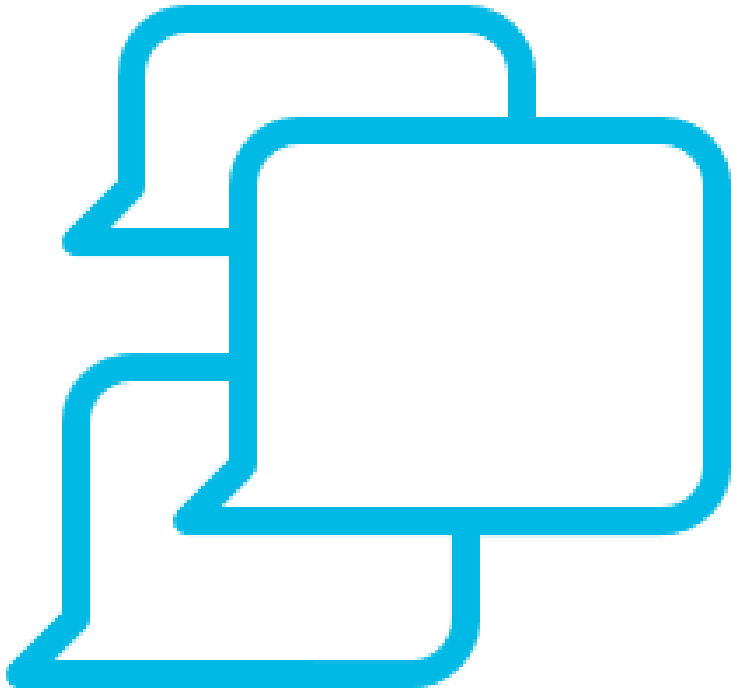
- IT team working 24/7 operations
- Estimated time to full operational capability (FOC) is unknown
- Backups tested and recovery procedures being reviewed and prioritized

Situation Report: + 350 hrs

- Tickets closed, system clean and CIO declares system back to normal operations
- Back up tested and completed—no indications of ransomware
- Third party forensics analysis ongoing on old server—no other IoCs at this time
- Additional precautionary monitoring for next 24-48 hours.
- Expenses being tallied
- Comms strategy adapted to recovery actions

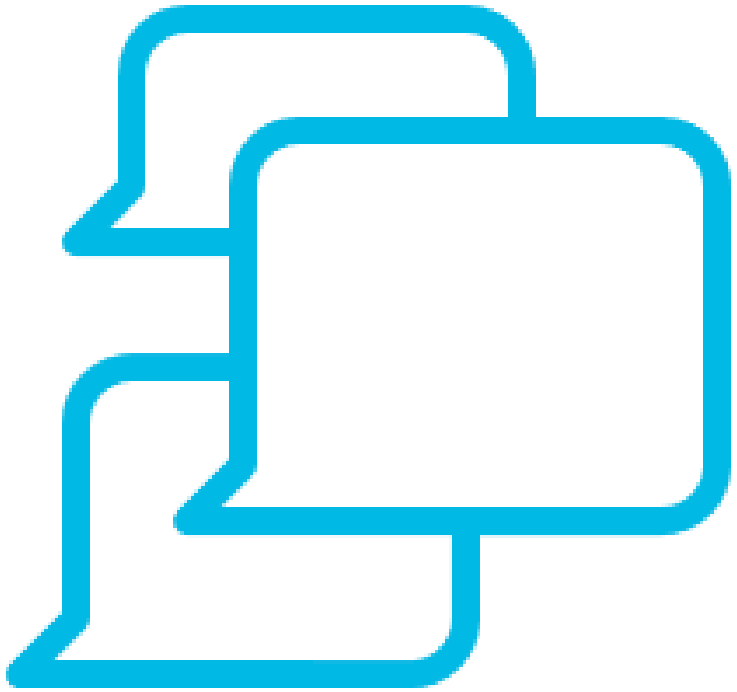
Discussion: Recovery

- What and who is in place to support recovery?
- Are they capable?
- Who provides ‘authority to operate’ on a recovered system?
- Who needs to know once you’ve recovered?
- Who would be involved in post-incident analysis and lessons learned?

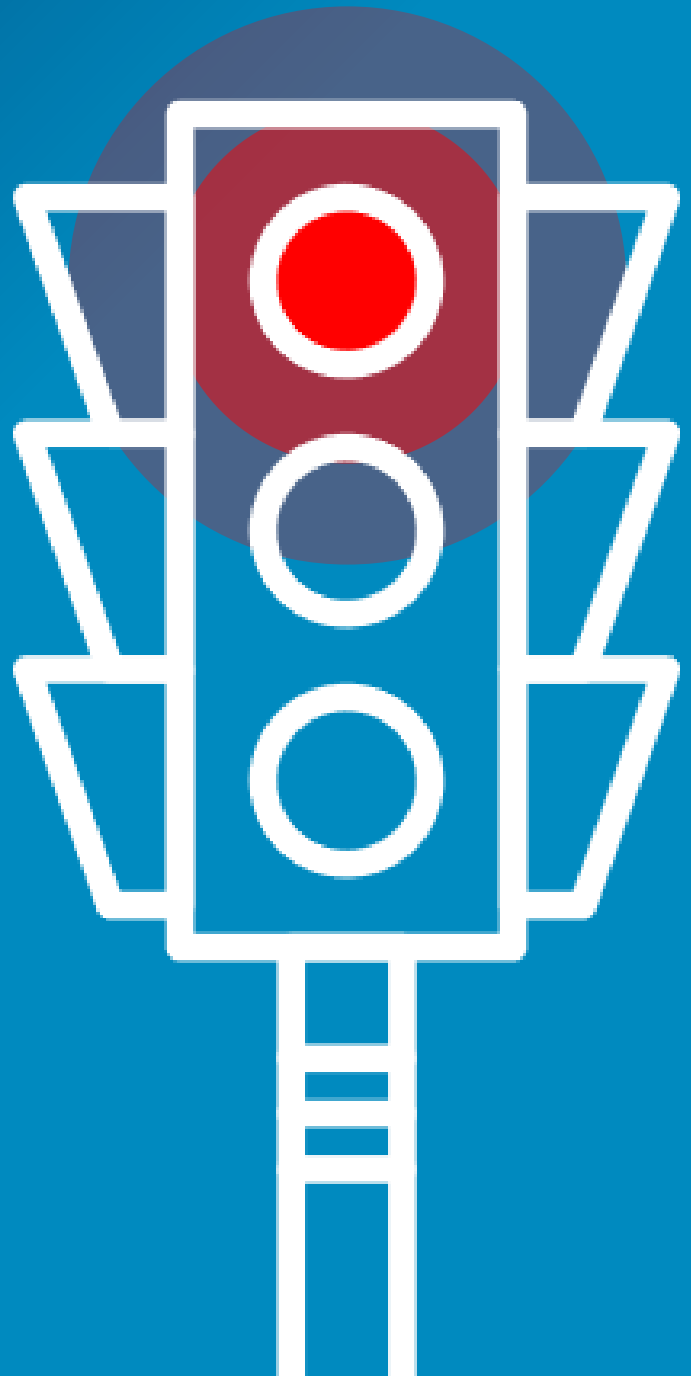


Discussion: Post incident activities

- Who would be involved in post-incident analysis and lessons learned?
- What reporting may be required?
- How are costs being tallied?
- How will lessons learned be integrated into practice and by whom?
- What modifications have there been to your threat and risk profile?



End of the Exercise



Toronto Metropolitan University

ROGERS cybersecure catalyst

Debrief: Questions To Consider

- Does your plan adequately address incident response requirements?
- Do you have an effective escalation protocol?
- Is there reliable risk-based decision making throughout an incident? Are authorities and responsibilities clear?
- Do you have a supporting communications plan with needed scripts, contact lists, etc.?
- Would the same decisions / actions hold in a different scenario?
- Are there any new technologies that need to be considered in our plan (e.g., cloud, edge devices, AI)?

How prepared do you feel?

ⓘ Start presenting to display the poll results on this slide.

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Conclusion

Summary and wrap up

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

Expectations

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

slido

Please download and install the
Slido app on all computers you use

Audience Q&A

ⓘ Start presenting to display the audience questions on this slide.

Selected Resources

Associations of Municipalities of Ontario (2020), A Municipal Cyber Security Toolkit, https://www.amo.on.ca/advocacy/emergency-services/municipal-cyber-security-toolkit

Canadian Center for Cyber Security (2020), Baseline Security Controls for Small and Medium organizations, https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Center for Internet Security (CIS) (2021), CIS Controls Version 8, https://www.cisecurity.org/controls

National Institute for Standards and Technology (2018), Cybersecurity Framework https://www.nist.gov/cyberframework/framework

Rogers Cybersecure Catalyst (2021), Simply Secure: Cybersecurity for Small and Medium-sized Businesses, https://www.cybersecurecatalyst.ca/simply-secure-for-smbs

Technation (2021), Municipal Cybersecurity Best Practices, https://technationcanada.ca/wp-content/uploads/2021/04/Municipal-Best-Practices-2021-EN.pdf

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Thank you for your participation!

Contact us

cybersecurecatalyst.ca/corporate-training

randy.purse@torontomu.ca