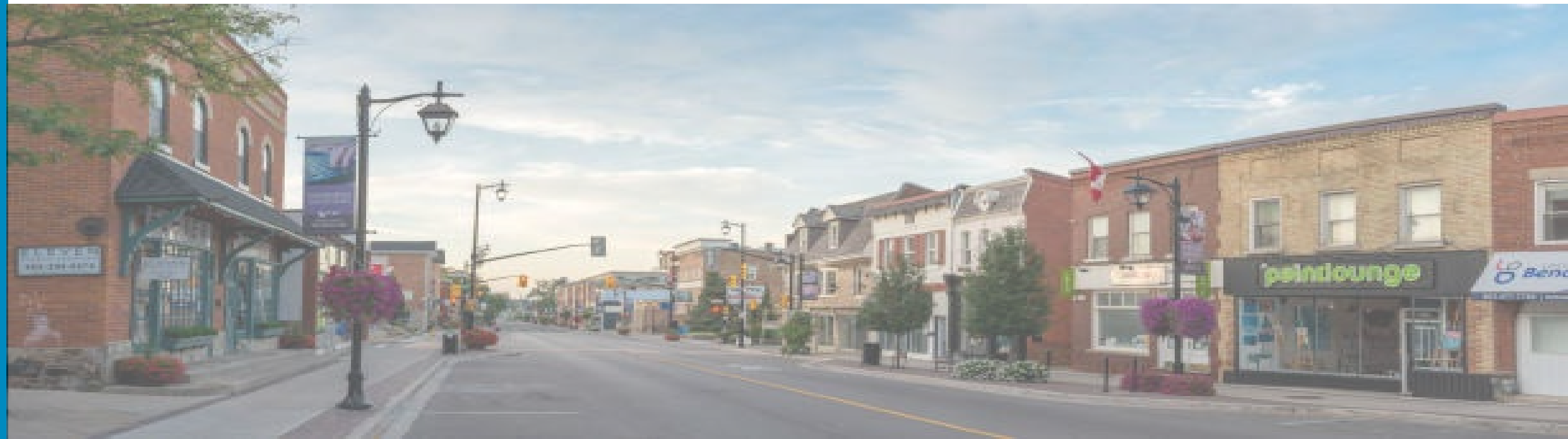
Toronto Metropolitan University

ROGERS cybersecure catalyst

ROMA
Rural Ontario Municipal Association

ROMA – Cybersecurity Tabletop Experience

20 January 2025



ROGERS cybersecure catalyst | Corporate Training & Cyber Range

DAN MATHIESON

MPA

Special Advisor, Cybersecurity and Municipal Engagement, Toronto Metropolitan University

dmathieson@torontomu.ca

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

RANDY PURSE

CD, PhD, CTDP

Senior Advisor, Cybersecurity Training & Education
Rogers Cybersecure Catalyst
Toronto Metropolitan University

randy.purse@torontomu.ca

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Your Role…

Don’t fight the scenario

Think critically about your municipal and organizational context

Define key organizational cyber risks

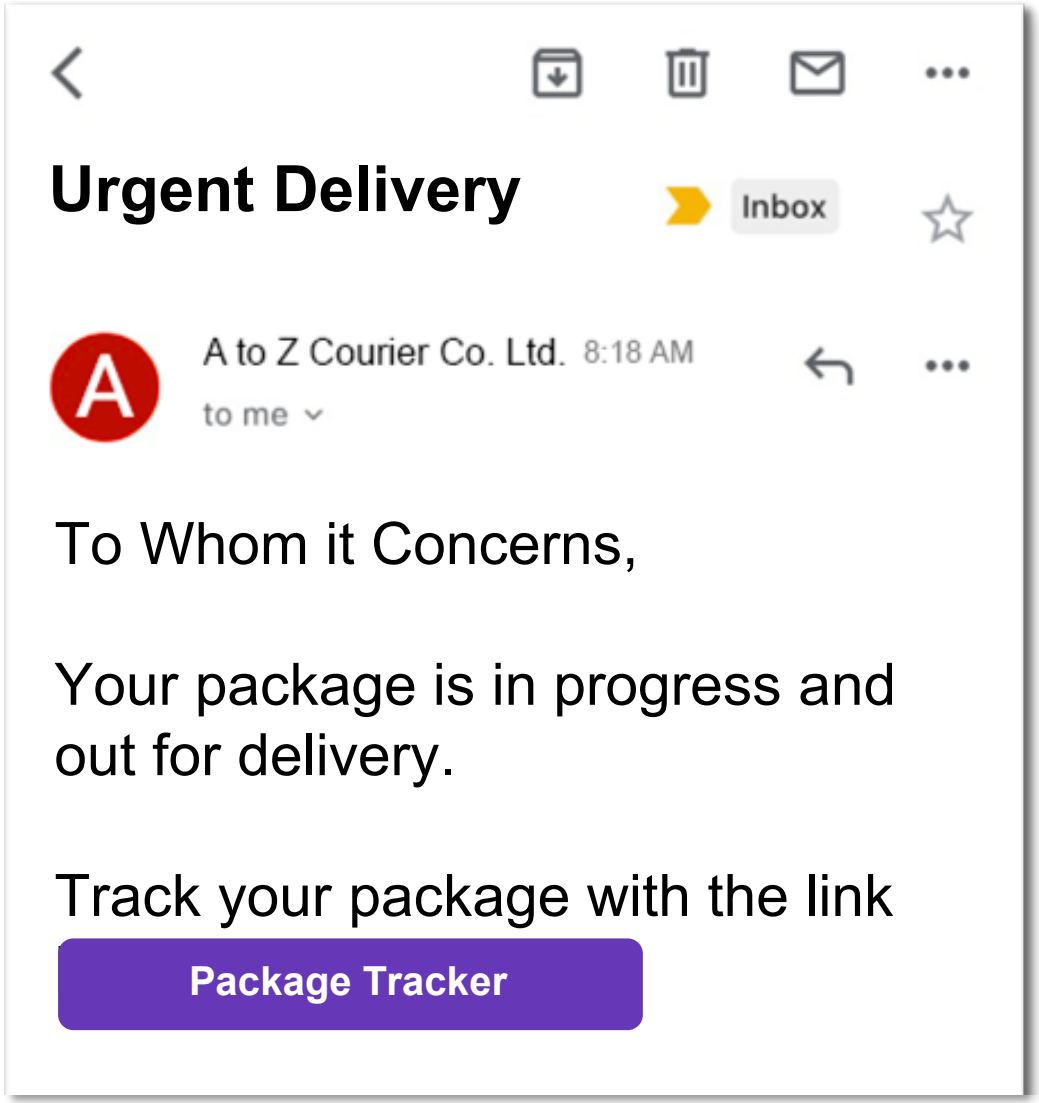
Identify organizational gaps in incident response processes, governance and communications

slido

Join at slido.com
#34200728

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Now, The Experience Will Begin



Report from the helpdesk ⚠️

An administrative employee clicked on email link and then …

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Payment will be raised in:

070 hrs 39 mins

All files will be deleted in:

166 hrs 39 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 in BITCOIN** by the time indicated.

If you try to recover your files yourself or if you don't 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

QR Code

Send $500,000 worth of bitcoin to this address:

Copy

Check Payment

Decrypt

slido Join at slido.com #34200728

Do you have an up-to-date incident response plan?

Initial Organizational Considerations

What are your immediate concerns?

What risks are exposed?

Who is responding?

How do you know?

First Responder's Assessment
+ 10 mins

Ransomware appears legitimate

"Our initial focus is on containment. We're conducting triage and scanning for other problems."

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Ransom Payment: A Business and Ethical Decision

What are the risks to paying or not paying a ransom?

What, if any, cyber insurance coverage do you have?

If you chose to pay, what would be the process?

Technical Update
+ 30 mins

Triage has been conducted and, for now, there doesn't appear to be any other issues. The technical response team believe that they have the ransomware contained.

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

MaryMary
@superaccountant22

OMG! Our office has just been subject 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 • Jan 20, 2025 • X Web App

DavetheKnave
@MayorWatch

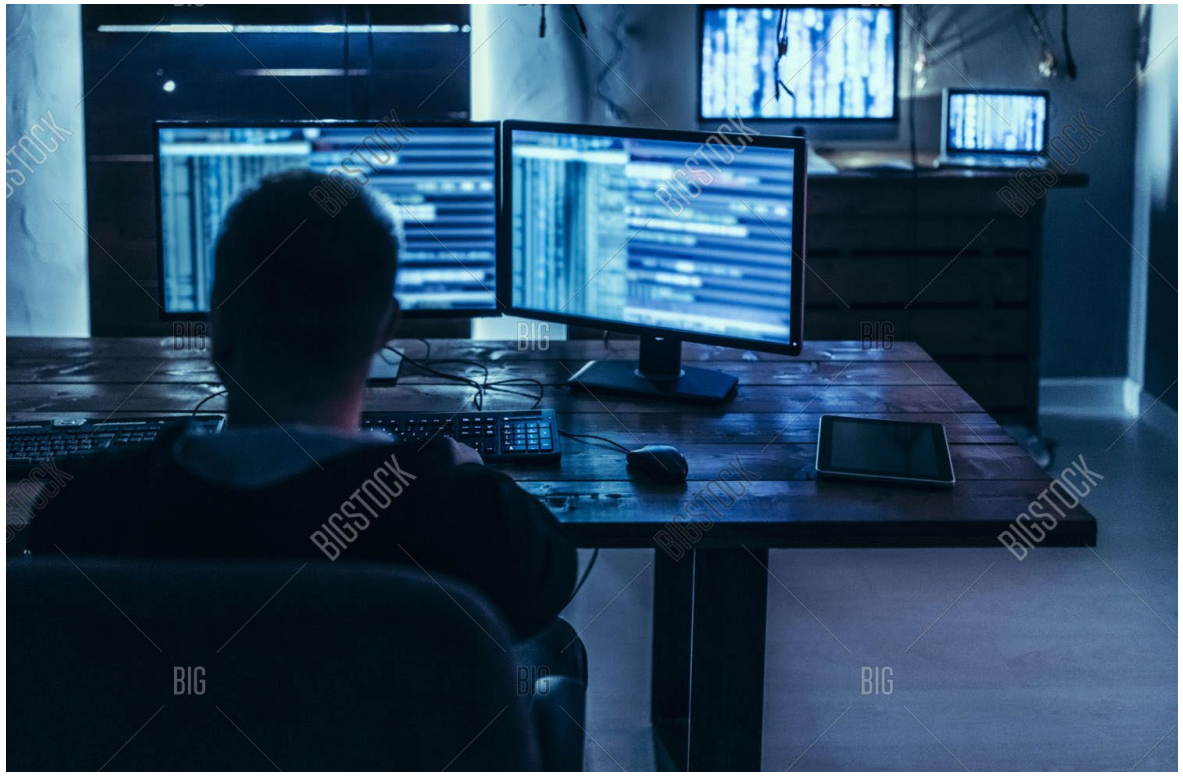
So apparently the mayor's office has been hit by ransomware but they haven't told us yet? Why haven't they said anything? What are they hiding?

12:35 PM • Jan 20, 2025 • X Web App

LIVE NOW

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

Full extent of the attack is still unknown, and it is unclear whether citizens' personal information and data have been compromised.



[Follow the latest on this developing story.]

More Top Stories

slido Join at slido.com #34200728

Do you have communication protocols that support a cybersecurity incident?

Technical Update
+ 6 hours

Exfiltration of data discovered from the attacked server

Remainder of network being scanned.

Additional containment activities are underway.

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Data Exfiltration

How does this change your exposure and risk?

What additional actions may be required?

Technical Update – Fast Forward
+ 42 hours

Server connection severed - incident contained

Accounting of data leakage ongoing

Team is continuing to work 24/7

Workarounds in place

Backups and recovery procedures are tested

Third-party forensics analysis commencing

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Recovery

How reliable are your backups?

Are both technical and non-technical stakeholders aware and confident in performing their responsibilities?

Who else might need to know?

Technical Update – Fast Forward + 27 days

Full backup from recovery completed, but some files were not successfully recovered

*Incident is **closed***

System is clean, but some cleanup continues

Precautionary monitoring

Post-Incident Analysis

Who is involved?

What additional communications and reporting requirements are there?

How will costs be tallied and absorbed in your budget?

How will you prioritize improvements relative to other projects?

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

End of Experience

slido

Join at slido.com #34200728

How prepared do you feel to respond to a cybersecurity incident?

Key Takeaways

Have a plan – consider different threat scenarios

Know who's on your team and their roles

Know who else you'll need

Understand reporting requirements

Manage the narrative - consider the local, political and technical context

slido Join at slido.com #34200728

Audience Q&A

ROGERS cybersecure catalyst | Corporate Training & Cyber Range

Thank You For Your Participation

For information on other corporate training AND Cyber Range opportunities, contact: catalyst.corporate@torontomu.ca