Cyber Security for Municipalities

Protecting Essential Services and Building Resilience

Why This Matters

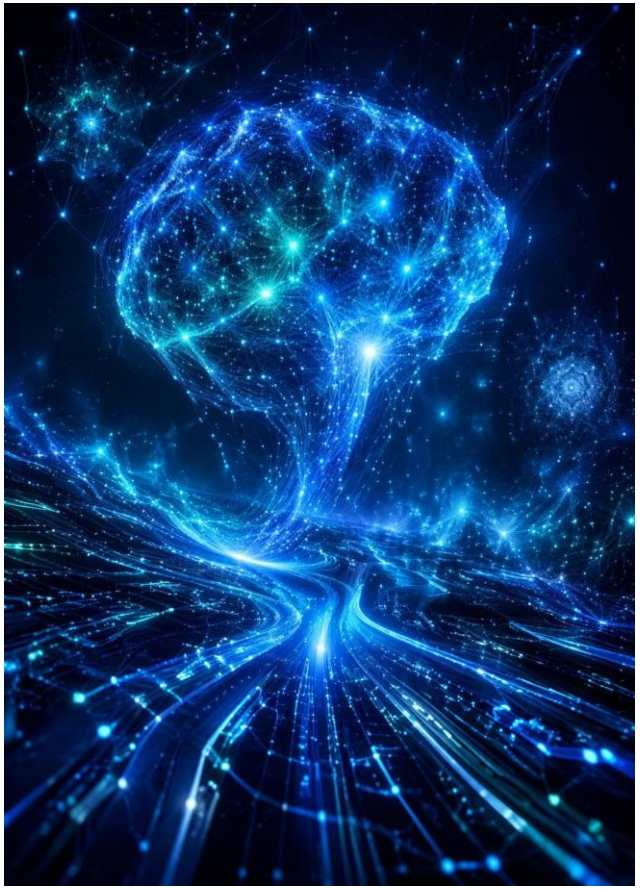
- **Cyber incidents disrupt essential municipal services**
  - Outages directly affect residents who depend on essential services
  - A single incident can erode years of community trust
  - Cyber risk is a service delivery issue - not just an IT issue

Threat Reality

- **Most cyber attacks are preventable**
  - Phishing emails remain the leading entry point for attackers
  - Weak passwords and missing MFA expose accounts to easy compromise
  - Most breaches trace back to basic controls that were skipped

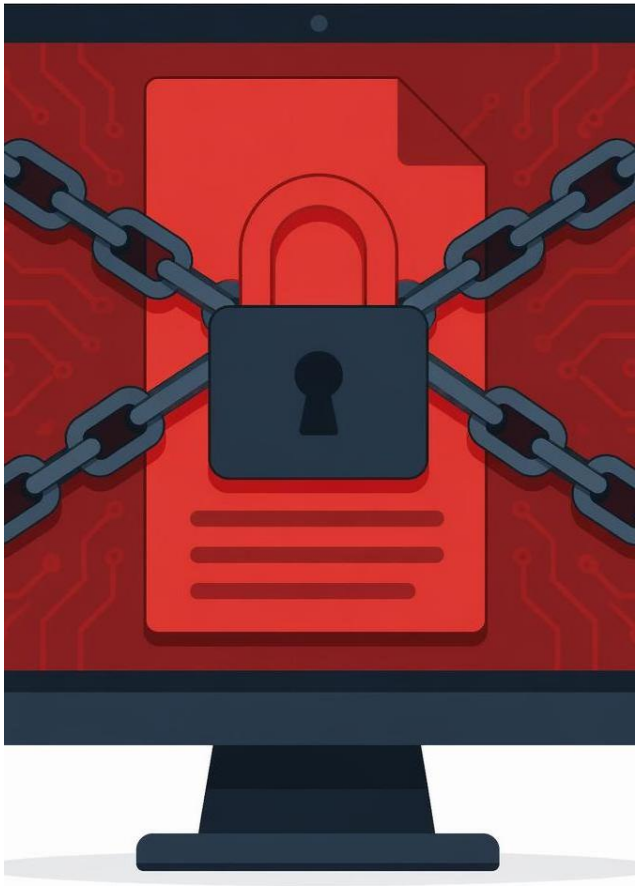
Frontier AI

- **Frontier AI is reshaping the municipal threat landscape**
  - AI-crafted phishing emails are more convincing, personalized, and harder for staff to spot
  - Deepfake voice and video can impersonate councillors or vendors to authorize fraudulent payments
  - Attackers use AI to scan systems and generate malware faster, shrinking the window to patch
  - Defenders also gain ground: AI assists with detection, triage, and faster incident response
  - Expect more frequent, lower-effort attacks—keep MFA, training, and backups current



Ransomware

- **Ransomware stops operations—not just computers**
  - Encrypts files across servers, workstations, and shared drives
  - Halts billing, permits, and emergency dispatch systems
  - Municipalities have faced multi-week service outages and recovery costs



Impact

- **Cyber incidents quickly become service failures**
  - Disrupts payroll, utility billing, and permit processing
  - Forces manual workarounds that drain staff time and raise errors
  - Recovery costs, legal exposure, and reputational damage compound quickly

48-Hour Scenario

- **What happens if your town systems are down for 48 hours?**
  - Payroll and vendor payments stall
  - Water and wastewater monitoring shifts to manual oversight
  - Emergency communications and dispatch face delays
  - Residents look for answers, and public trust takes the hit

Top Controls

- **Basic controls reduce most cyber risk**
  - Multi-factor authentication on every account
  - Timely patching of operating systems and applications
  - Tested, offline backups of critical data
  - Regular security awareness training for all staff

People

- **Staff are your first line of defense**
  - Clicking a phishing link is the most common starting point
  - Sharing or reusing passwords creates compounding risk
  - Trained, alert staff stop attacks before they spread
  - Build a culture where reporting suspicious activity is encouraged

Response

- **Act immediately: Disconnect, isolate, notify**
  - Disconnect affected devices from the network immediately
  - Isolate compromised accounts and systems
  - Notify leadership, IT, and external partners without delay
  - Preserve logs and evidence—do not wipe or troubleshoot alone

Support

- **You are not alone—support is available**
  - Canadian Centre for Cyber Security offers advisories and incident help
  - Provincial OCIO - Cyber Security Office
  - Peer municipalities and associations share lessons learned
  - Lean on these partners before, during, and after an incident

Contacts & Resources

- **Key contacts when you need help**

- **Canadian Centre for Cyber Security (CCCS)**

  - Website: cyber.gc.ca
  - Email: contact@cyber.gc.ca
  - Phone: 1-833-CYBER-88 (1-833-292-3788)

- **Provincial OCIO – Cyber Security Office**

  - Website: cybersafenl.ca
  - Email: cso@gov.nl.ca

Closing

- **Preparedness over perfection**
  - Plan for incidents—they are a matter of when, not if
  - Practice response steps so they become muscle memory
  - Small, consistent improvements build lasting resilience
  - The goal is to keep services running, not to be perfect