Canadian Municipal Cybersecurity in 2025

Observed Trends, Persistent Threats, and Increased Resilience

TAKEAWAYS

- Ransomware and OT attacks continued to disrupt municipal services, with incidents often costing cities millions and impacting critical infrastructure.
- AI-driven threats, including deepfake-enabled phishing, increased sharply, challenging traditional defenses.
- Talent shortages remained a concern, prompting cities to invest in workforce development and specialized training.
- Collaboration with federal agencies and peer cities became essential for sharing intelligence and best practices.

RECOMMENDATIONS

- Invest in AI-powered detection tools and segment IT/OT networks to contain threats.
- Expand staff training and support talent pipelines to address emerging risks.
- Strengthen vendor oversight and update cybersecurity policies in line with CCCS guidance.
- Foster partnerships and conduct joint exercises to enhance sector-wide preparedness.

Municipal Cybersecurity in 2025

In 2025, Canadian municipalities faced a rapidly evolving cybersecurity landscape. Ransomware remained the most disruptive risk as attackers expanded their focus to operational technology (OT) systems, targeting essential services like water, transit, and energy.
We saw cities accelerate investments in cybersecurity infrastructure, adopt AI-driven detection tools, and strengthen governance through closer collaboration with federal agencies and the Canadian Centre for Cyber Security (CCCS). Municipalities continue to grapple with talent shortage and emerging risks such as deepfake-enabled social engineering and supply chain vulnerabilities. High-profile incidents highlighted the need for robust incident response plans, network segmentation, and ongoing staff training. Canadian cities demonstrated greater preparedness and adaptability, but persistent vigilance and sector-wide knowledge sharing remain essential to protect public services and infrastructure against sophisticated cyber adversaries.

2025 Cyber Threats

This year saw Canadian municipalities faced rising cyber threats that directly targeted local government operations and critical public services. Ransomware remained the most prevalent and disruptive threat, with municipal incidents accounting for an estimated 15% of all reported ransomware attacks in Canada. Cities such as Fort St. John, Hinton, and Kingston experienced attacks that shut down permitting systems, disrupted transit, and forced temporary closures of administrative offices, with recovery costs frequently exceeding $5 million per incident. The City of Hamilton's ransomware event in early 2024 continued to serve as a cautionary example, prompting sector-wide improvements in incident response and business continuity planning. OT environments, including water treatment plants, traffic management systems, and energy grids, were increasingly targeted as attackers exploited vulnerabilities in legacy infrastructure and edge devices. CCCS reported that nearly 30% of municipal cyber incidents in 2025 involved OT systems, raising concerns about the potential for

real-world disruptions. AI-enabled threats also emerged as a significant risk, with deepfake-driven social engineering and automated phishing campaigns contributing to a 62% year-over-year increase in synthetic media attacks against public sector organizations. Shared Services Canada reported blocking over 6.6 trillion suspicious events in a twelve-month period, underscoring threat actors' relentless targeting of municipal networks.

The Local Road to Resilience

Canadian municipalities took decisive action in 2025 to strengthen their cyber resilience and safeguard essential services. Targeted investments, policy improvements, workforce upskilling, and collaborative partnerships helped cities address evolving threats and sustained security improvements.

Technology Investments and Infrastructure Modernization

Canadian municipalities accelerated their cybersecurity investments in 2025, with over 75% allocating dedicated budgets for upgrading legacy systems and deploying advanced threat detection technologies. CIRA's 2025 Cybersecurity Survey reports that cities prioritized AI-driven solutions to improve detection and response times, while endpoint hardening became standard practice for protecting both IT and OT environments. CCCS highlights the widespread adoption of zero-trust architectures and network segmentation helping with breach containment.

Governance, Policy, and Vendor Oversight

Cities updated their cybersecurity policies and procedures in alignment with evolving CCCS guidance and provincial regulations. Regular security audits and incident response simulations became routine, often involving external experts and provincial agencies. Vendor oversight was strengthened through stricter compliance checks and regular audits, ensuring that third-party providers adhered to municipal cybersecurity protocols. It was noted that such enhancements reduced recovery times and minimized service disruptions following major incidents

Talent Development

Municipalities recognized the persistent challenge of cybersecurity talent shortages and responded with innovative workforce development strategies. This year, cities expanded staff training programs to address emerging threats, including deepfake-enabled social engineering and supply chain vulnerabilities. Cities like Fredericton and Waterloo launched co-op programs and micro-credentialing initiatives to build a pipeline of skilled professionals. Specialized training modules for personnel in critical roles became standard, ensuring that staff could respond effectively to complex incidents.

Collaboration and Community Resilience

Collaboration defined municipal resilience in 2025. Cities strengthened partnerships with federal and provincial agencies, sharing threat intelligence and best practices to stay ahead of evolving adversary tactics. The CCCS National Cyber Threat Assessment emphasizes the importance of inter-municipal collaboration, with joint incident response exercises and information sharing networks enabling rapid adaptation to new threats. Community-driven initiatives, such as public-private partnerships and local cybersecurity awareness campaigns, further enhanced resilience by fostering a culture of vigilance and continuous improvement.