Stratejm

Best Cybersecurity Practices for Municipalities

White Paper

Provided by Stratejm for AUMA members

Info@Stratejm.com
888.876.0504
Stratejm.com

Stratejm Inc. | 5285 Solar Drive, Suite 204
Mississauga, ON | L4W 5B8 | Canada

Best Cybersecurity Practices for Municipalities

Contents

Understanding How the Canadian Municipal Government Works

Canada has three levels of government, as shown below:

Level	Jurisdiction	Leader	Responsibilities
Federal	Whole Country	Prime Minister	Canadian citizenship National defence Currency National parks Royal Canadian Mounted Police
Provincial	A Province	Premier	Education Hospitals Child care Driver's licenses Water and sanitation Transport infrastructure
Municipal	City/Municipality	Mayor	Emergency services Public transport services Waste management Snow removal Community centres Planning city streets and buildings Recreation centres and libraries

Table 1: The three levels of governments in Canada

Technology Advances in Local Governments

In a digital, customer-centric world, customers are accustomed to frictionless and rapid services. Today, Amazon provides same-day delivery, Uber gets you a cab in minutes, and vehicles are becoming fully self-driving.

Traditionally, local governments offered increasingly manual services through forms that people printed and mailed, paid in cash and cheque, and attended appointments that officers conducted in person strictly during working hours (9 am to 5 pm, Mondays to Fridays). By and large, municipalities missed an excellent opportunity to improve their value while enhancing the lives of residents.

However, this narrative is changing as more local governments are breaking new ground by deploying technology to serve citizens better. Cloud computing, mobile technology, and the Internet of Things has impacted all industries and government departments. Such technological advances are transforming the way municipalities provide services and streamline operations.

The Government of Canada released the Digital Operations Strategic Plan: 2018-2022 to outline the process for how the administration manages technology and technological change in government. The plan sets and provides insights into the government's departments, agencies, and officials' digital direction. The document also establishes the integrated approach for the government on digital transformation, service delivery, security, and IT. Some of the recent improvements in digital transformation have focused on simplifying user experience for access to datasets held across different levels of government. Canadian territories and municipalities have created open data portals to allow users to access the data they need.

Open Datasets in Municipalities

Municipalities give residents access to a wide range of data types. In some cases, if provincial governments collect that particular dataset, a data-sharing arrangement is usually adopted between the orders of government. An open data program features quality data that is readily accessible to municipalities:

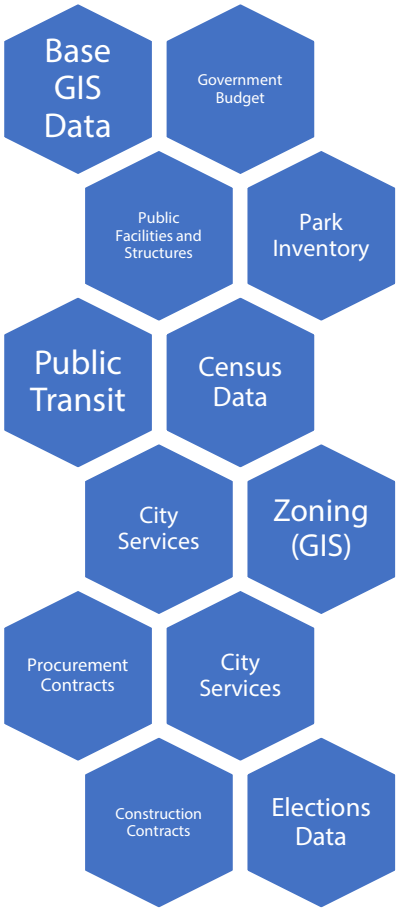
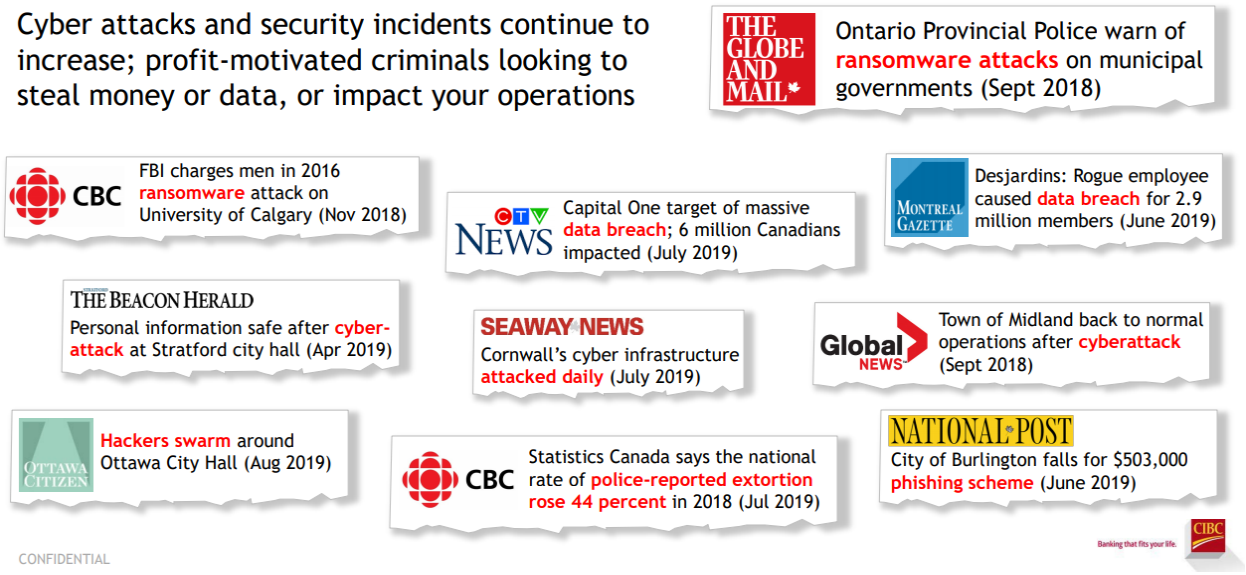


Figure 1: Data accessible to municipalities and residents

Cybersecurity in Municipalities

Massive cybersecurity incidents have been grabbing headlines over the past few years, with large corporations such as British Airways, Marriott, Facebook, Equifax, and eBay falling victim to data breaches affecting millions of people. While a preponderance of reported cyber-attacks involves the private sector, cybercriminals also target the public sector. As municipalities digitize and integrate more services and IoT projects to access and process open and confidential datasets, they have become a high-profile target for cyber-crime.

A screenshot from the Association of Municipalities of Ontario (AMO) presentation on Cybersecurity Risk Management for Municipalities shows numerous news reports on frequent cyberattacks and security incidents from profit-motivated criminals looking to steal money or data or impact operations.



What is the Threat and who are the Actors?

Apart from the benefits offered by technology in local governments, such digital transformation activities introduce vulnerabilities that hackers can exploit to cause a data breach. Most often, local governments fail to implement security controls when connecting to a computer network or the Internet. In effect, lack of adequate security protocols results in weak municipal systems that hackers can easily exploit to take control of systems, knock out public services, and steal confidential information.

"There is lack of leadership at the provincial government level when it comes to supervising, establishing standards, or even checking over the shoulders of municipalities from time to time," says Jose Fernandez, a malware expert at Montreal's Polytechnique Engineering School.

Municipalities should be worried about various threat actors, including nation-states, hackers, hacktivists, organized crime, and insiders (both malicious and non-malicious).

Figure 2: Municipalities Threat Actors

Malicious and non-malicious threat actors use a wide range of tactics and threats to target people, processes, and technology in municipalities.

Figure 3: Threat Tactics and Techniques Affecting Municipalities

1. Ransomware Attacks

Local governments are attractive targets for ransomware attacks. Hackers understand that the government-funded agencies are easily convinced to pay up instead of undertaking a costly and technical alternative route. Cybercriminals attacked Wasaga Beach and Midland with a six-figure ransom demand in 2018. The municipalities spent approximately $250,000 each in the recovery process. Last year, hackers launched ransomware attacks on Ontario municipalities such as Stratford, the Nation, and Woodstock. The Canadian Centre for Cyber Security issued a countrywide alert about Ryuk ransomware that was affecting multiple organizations, including municipal governments. In another incident, municipal employees in a region between Montreal and Quebec City discovered a warning message on their systems notifying them hackers had locked all their files. Cyber actors demanded $65,000 ransom from the regional county municipality of Mekinac.

Anonymous hackers launched a ransomware attack on Atlanta. The March 2018 incident deactivated online access, encrypted files, and demanded a $50,000 ransom in bitcoin in exchange for the decryption key. Eight thousand municipal employees in the city regained access to systems, but residents could not access some digital services. The city government's desktops, printers, and hard drives returned to normalcy for the first time in five days, which affected services such as water bill and traffic ticket online payments. An article on the New York Times described the attack as "one of the most sustained and consequential cyberattacks ever mounted against a major American city."

Today, ransomware-as-a-service campaigns allow malicious cyber actors to deliver massive attacks to municipalities.

2. Unpatched Devices

In recent months, the Canadian Centre for Cyber Security has discovered compromises that took advantage of unpatched devices exposed to the Internet. Victims reported the malicious activities to the Cyber Centre in June and July 2020. Cybercriminals deployed intensive reconnaissance-style scanning of the target system, followed by the compromise of vulnerable and improperly secured servers and network devices.

3. Malware

Hackers install malware to compromise networks and infrastructure in municipalities. In some cases, cyber actors remained active on compromised systems for months before the victims detected their activities. Cybercriminals spread different forms of malware like spyware, worms, watering holes, key loggers, and trojan horses to infect systems and extract confidential information.

4. Business Email Compromise (BEC)

Hackers impersonate senior personnel, such as mayors in municipalities, and send emails to lover level employees requesting them to transfer money or share credentials. In other cases, criminals spoof supplier emails and request local governments to update banking information before settling pending invoices. In other circumstances, cyber actors impersonate employees and email HR departments requesting change in payroll information.

5. Distributed Denial of Service (DDoS)

Hackers use bots and other malware to lock users out of essential municipal services. A classic distributed denial of service (DDoS) attack disrupts a municipal government's web services by temporarily blocking citizens' and employees' ability to transact online. In most instances, DDoS comes from a large number of infected devices that span multiple organizations.

6. Social Engineering and Insider Threats

Hackers deploy various social engineering tactics such as phishing, eavesdropping, tailgating, spear-phishing, baiting, and dumpster diving to trick unsuspecting employees into clicking malicious links, opening files with malware, or share credentials.

The Impact if You get Breached

Cyberattacks have massive impacts on local governments across Canada. Municipalities that have become easy prey for cybercriminals struggle to combat the highly sophisticated and frequent attacks. Cybersecurity attacks have penetrated foundational departments within municipal governments, including healthcare, education, and law enforcement.

David Masson, former senior manager for Public Safety Canada, believes that the country is keen on securing federal security systems. However, outside of the federal area, it is a mixed bag. Meanwhile, there is no proper reporting mechanism in place. For instance, ransomware has quietly been wreaking havoc on municipalities for years. Still, stakeholders never report such incidents, making it a challenge for the public and private sectors to track and resolve the silent devastation accurately.

With the increasing rates of cyberattacks on organizations, municipalities suffer numerous impacts. A data breach causes financial loss due to recovery costs and ransoms. Besides, increased attacks on cities cause a decline in economic investment. Additionally, it may take days or even months to fix a data breach. Sometimes, the victim may never fix the breach, and hackers put government and personal data on the black market.

A Range of Best Practices that You Can Follow

1. Updating and Patching Systems

The Cyber Centre recommends that municipalities should apply the latest security patches and operating systems updates for devices on their networks immediately. Furthermore, the institutions should upgrade and maintain the latest anti-virus signatures. Hackers check on outdated operating systems and other software to identify vulnerabilities they can exploit to gain access to critical systems and information. In effect, municipalities should raise awareness about the importance of installing updates on all devices and software as soon as vendors release security patches. Additionally, local governments should ban the use of software with an end-of-life notification from its vendor.

2. Data Encryption

Local governments should encrypt sensitive government and personal information on all computer systems, drives, cloud servers, and end-user devices. System and network admins should deploy operating systems that offer encryption in addition to third-party cloud-based solutions.

3. Awareness Training

All too often, cybersecurity strategies focus on preventing external threats from hackers, without addressing internal threats from malicious and non-malicious insiders. Indeed, employees and citizens play a critical role in helping to reduce organizational cyber risks. Several municipal associations, such as the Association of Municipalities of Ontario (AMO) and the Federation of Canadian Municipalities are now taking a proactive role in educating citizens about cyber risks. Organizations must establish comprehensive cybersecurity awareness training and testing for municipal employees. Such a program equips users with relevant information they need to recognize cyber threats such as malware, phishing scams, and BEC. All employees should be vigilant when clicking unsolicited links or opening unexpected attachments in emails.

4. Installing Security Tools

Municipalities can install security tools such as intrusion detection systems and a firewall that provide detection and protection against malware and phishing attacks by blocking user access to malicious links and attachments. Security appliances add a cost-effective and low-maintenance layer to the organization's cybersecurity footprint. The tools analyze traffic and block employees from accessing malicious sites.

Figure 4: Security best practices for municipalities

5. Enhanced Collaboration

Provincial and federal governments should work closely with municipal governments to help protect governments from cyberattacks. Jamie McGarvey, AMO President, believes that collaboration in cybersecurity helps weather attacks with less disruption. Dan Mathieson, the Mayor of Stratford, said that if fellow mayors across the country do not start working together on the problem, digital extortions will hit more communities holding municipal data for ransom.

6. Access Control

Municipalities should enforce access controls by minimizing the number of users with administrative privileges. The agencies should restrict employees from installing software on their devices without authorization.

Municipalities should establish and enforce a password management policy for employees and residents accessing online services. Users should create unique, hard to guess passwords for each account and device. Since hackers can easily crack passwords through the dictionary and brute force attacks, local governments should implement multifactor authentication (MFA) where possible, especially on all internet-facing remote access systems. MFA is a security control that requires additional information besides username and password.

7. Continuous Monitoring

System owners should disable remote desktop services, or closely monitor network traffic and logs of remote systems to detect suspicious activities. Moreover, municipalities should scan all incoming and outgoing communications to detect threats and block executable files from reaching employees and citizens. Network and system administrators can deploy open-source tools to monitor their networks for open ports and abnormal activities.

8. Cybersecurity Policies and Procedures

Municipal governments should develop and document cybersecurity policies and procedures for all employees and citizens to follow. The government agency should share the documents with all covered entities that access municipal systems and networks. Developing adequate policies and procedures requires proactive planning, risk assessment, and roles definition. An integral approach involves following industry best practices and regulations such as the NIST Cybersecurity Framework (CSF) and ISO 27001 when developing cybersecurity policies.

9. Systems and Data Backups

Municipalities should put in place controls and solutions that execute daily backups of critical systems to an offline and offsite data centre. The organizations should practice periodical backups to ensure the integrity of existing processes and information. An updated backup helps organizations avoid data loss if a catastrophic event such as fire, theft, server crash, or ransomware occurs.

10. Vendor Risk Management

Municipalities often outsource functions to third-party service providers. Some of the subcontracted activities include credit card processing, payroll services, and IT support. Improving cybersecurity posture in local governments requires adequate due diligence and risk assessment on all suppliers and contractors that have access to information and interact with municipal networks. Part of vendor risk management should entail contractual obligations on suppliers, requiring security documentation and on-time patching of vulnerabilities.

11. Partnering with a Managed Security Services Provider

Local governments can hire a managed security services provider to perform vulnerability assessment and penetration testing, and offer expert support. A team of cybersecurity professionals offers tools and expertise needed to perform real-time analysis of immediate threats and implement controls to mitigate external and internal risks.

Conclusion

The threat of a cybersecurity incident is a growing challenge without a definitive solution. For municipalities, cyberattacks can halt operations, put residents' information at risk, and compromise critical infrastructures such as water, transport, and waste management. The problem is now at the forefront as municipal governments across Canada and the world are falling victim to frequent and sophisticated cybersecurity incidents. There is no one-size-fits-all solution for security challenges. Fortunately, talking about the challenges, sharing past cyber incident experiences, and developing a wide range of best practices is the proven methodology way to address cyber threats in municipalities.