



EBOOK

FROM RISK TO RESILIENCE

Cybersecurity Best Practices for
Empowering Safer Communities



BULLETPROOF

a GLI company



Microsoft
Solutions Partner

bulletproofsi.com



Table of Contents

Introduction.....1

Chapter 1: Navigating Cybersecurity, Compliance, and IT Challenges.....2

How To Stay Compliant in a Patchwork of Regulations.....3

Chapter 2: What is Zero Trust and Why It Matters.....5

Why Does Zero Trust Matter?.....6

The Value of Zero Trust.....7

Chapter 3: Is Cyber Insurance Right For You.....9

Advantages and Limitations of Cyber Insurance.....10

How to Determine the Right Amount of Cyber Insurance Coverage.....12

Chapter 4: How Municipalities Can Protect Themselves From 99% of Attacks.....13

Fundamentals of Protecting Your Municipality14

Which Type of Security Testing is Right for You?15

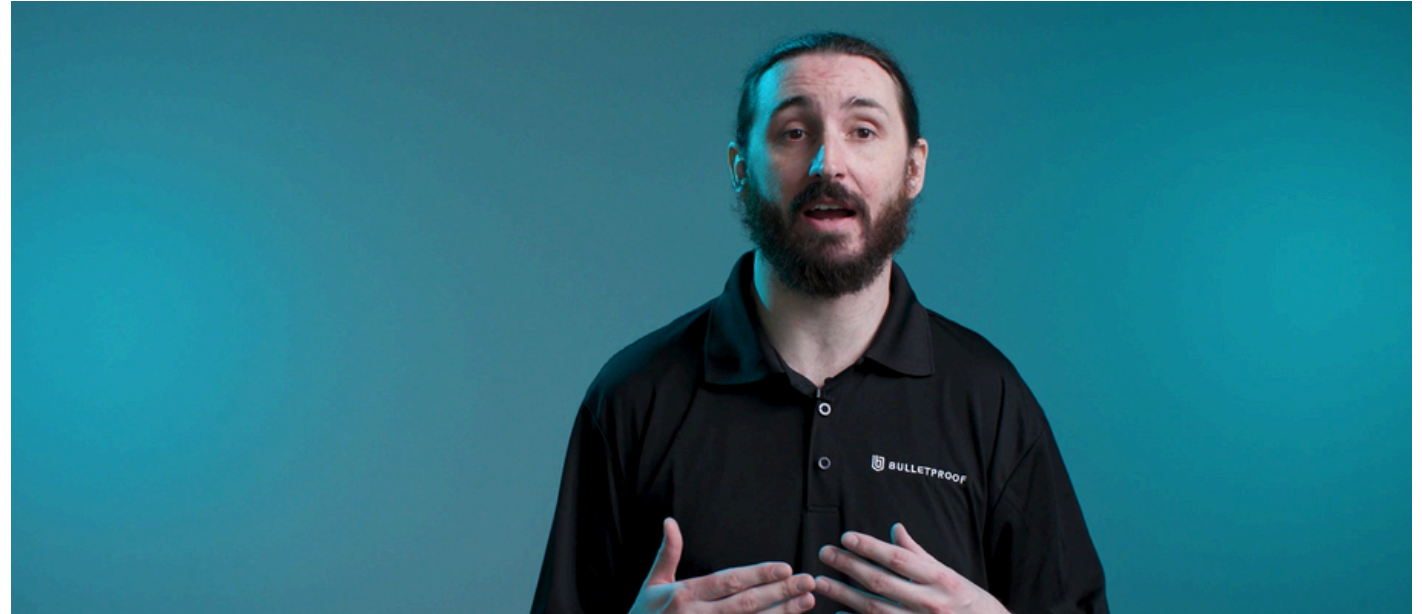
Third-Party Providers To Bolster Your Defences16

Chapter 5: The Power of Partnership: Joining Forces With IT & Security Providers17

5 Key Benefits of Partnering With Experts.....18

5 Key Steps for Municipal Leaders to Strengthen Their IT & Security Posture20

Introduction



The stakes get even higher: any breach can lead to legal consequences, reputational damage, and financial penalties for municipalities. Proactively defending against these threats is the best way that municipalities can protect sensitive personal information and ensure the continuity of essential services.

Many Canadian municipalities, constrained by **tight budgets and complex legacy systems, struggle to adopt modern IT infrastructure and advanced cybersecurity measures.** This leaves them at a high risk of cyberattacks, as cybercriminals are constantly evolving their tactics to better exploit outdated infrastructure, unpatched systems, and phishing vulnerabilities.

This eBook was developed by our team of IT and security experts, drawing on years of experience supporting municipalities across Canada. We understand the persistent challenge of maintaining security and compliance while managing large volumes of data.

Inside, you'll find clear, actionable guidance based on real-world threats and emerging trends. From understanding how cybercriminals are evolving to implementing practical steps that strengthen your defenses, this guidebook is designed to help municipal leaders make informed, proactive decisions about IT and cybersecurity. Explore the guide to better protect your systems, secure citizen data, and build a more resilient municipality.

Chapter 1 Navigating Cybersecurity, Compliance, and IT Challenges

Public behavior, the shift to hybrid work, and the rise of global threat actors have significantly changed the cyber threats municipalities face. According to a 2024 study by the Canadian Internet Registration Authority, 55% of MUSH organizations (municipalities, universities, schools, and hospitals) reported experiencing a cyberattack in the past year.^[1] Ransomware, identified by the Government of Canada as the top cybercrime threat to critical infrastructure,^[2] has become especially costly. In 2023, the average ransom paid in Canada reached \$1.13 million CAD—an increase of nearly 150% over two years.^[3]

In this chapter, we will explore the growth of cybercrime threats, the regulatory impacts on municipalities, the shortage of IT and security resources, and the opportunities for cyber grants and funding.

The Growing Cybercrime Threat

The Canadian Centre for Cyber Security has noted that the resilience of cybercrime in Canada is due in part to the rise of a Cybercrime-as-a-Service (CaaS) business model.^[4] With CaaS, threat actors sell stolen and leaked data and ready-to-use malicious tools to other cybercriminals online. For as little as \$20, a bad actor can obtain the tools and knowledge necessary to launch an attack. This low barrier to entry has contributed to the exponential increase in cyber incidents, putting immense pressure on municipalities to bolster their defenses.

Cybercriminals target municipalities for various reasons, including:



Valuable personal
data they store



Potential to disrupt
critical public services



Limited cybersecurity
measures in place

The result of a successful cyberattack can be devastating and **lead to significant financial losses, operational disruptions, and a loss of public trust.**

In February 2024, the City of Hamilton, Ontario experienced a major cybersecurity incident that severely impacted its complex technology infrastructure.

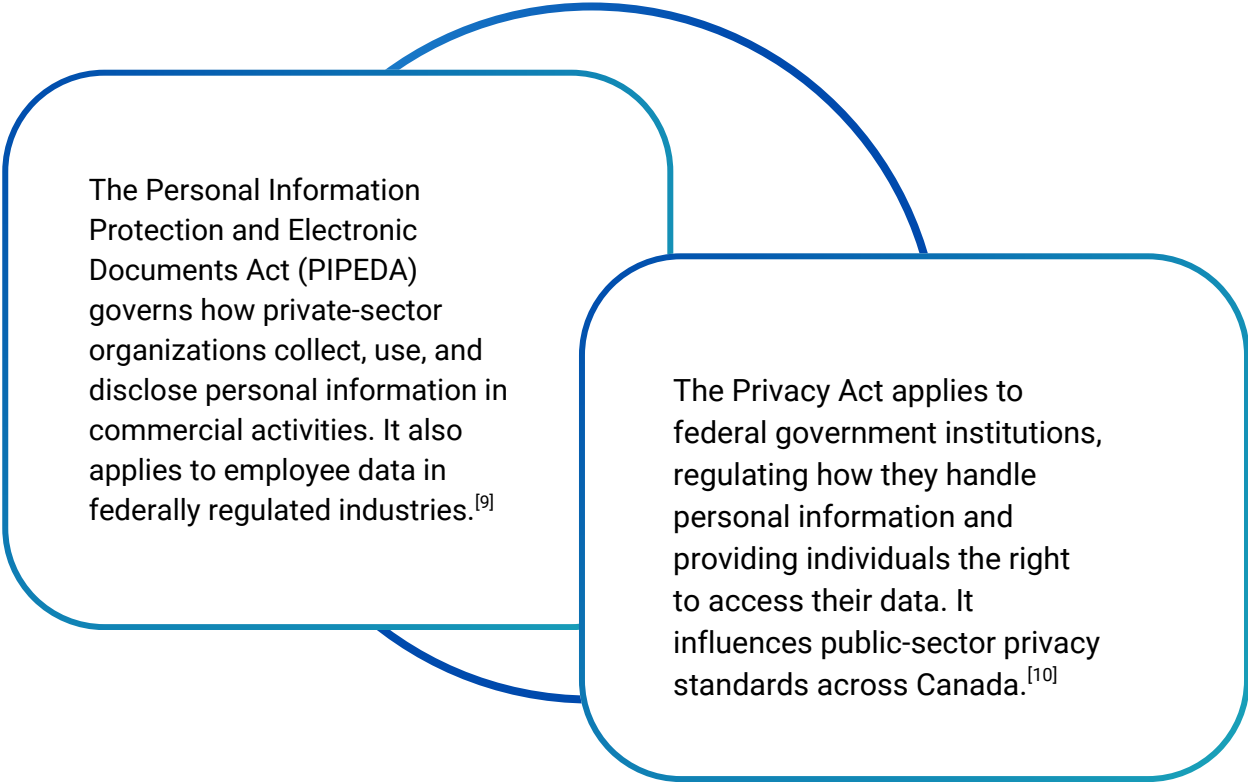
This infrastructure supports approximately 8,000 full-time city employees, nearly 600,000 residents, and around 7,000 business partners.^[5] By November 2024, recovery costs had reached \$9.6 million,^[6] with an estimated \$52 million still needed to fully rebuild.^[7]

Smaller towns and cities are also not safe from cybercriminals. In January 2024, the town of Westlock, Alberta was hit with a ransomware attack affecting over 1,600 residents.

The theft of their personal information led to the city offering affected residents credit monitoring and identity protection services.^[1] Such incidents underscore the urgent need for robust cybersecurity defences in municipalities of all sizes.

How To Stay Compliant in a Patchwork of Regulations

To combat the growing threat of cyberattacks, many Canadian municipalities are adopting cybersecurity policies and procedures to better protect their systems and citizen data. While municipalities are governed by provincial privacy laws (like Ontario's MFIPPA, Alberta's FOIP Act, and BC's FIPPA), federal frameworks such as PIPEDA and the Privacy Act still influence municipal privacy practices.



The Personal Information Protection and Electronic Documents Act (PIPEDA) governs how private-sector organizations collect, use, and disclose personal information in commercial activities. It also applies to employee data in federally regulated industries.^[9]

The Privacy Act applies to federal government institutions, regulating how they handle personal information and providing individuals the right to access their data. It influences public-sector privacy standards across Canada.^[10]

Understanding the nuances of privacy policy is particularly important when municipalities work with third-party vendors, interface with federal systems, or aim to align with national cybersecurity standards. Ensuring compliance across this mix of regulations is essential for maintaining trust, avoiding legal consequences, and minimizing reputational or financial risk. Non-compliance can lead to legal consequences, financial penalties, and reputational damage.

Battling the IT and Security Skills Gap



One of the most pressing challenges facing municipalities today is the shortage of skilled IT and cybersecurity professionals. The cyber skills gap has increased by 8% since 2024.^[11] Demand for these experts far exceeds supply, making it difficult for municipalities to attract and retain the talent needed to defend against modern cyber threats.

This talent gap is worsened by limited budgets and resources, which often can't compete with private-sector salaries and benefits. As a result, municipalities may lack the in-house expertise required to implement, maintain, and adapt effective cybersecurity measures. This shortage not only increases the risk of cyberattacks but also impairs a municipality's ability to respond swiftly and effectively to incidents—escalating the potential for serious operational, legal, and reputational consequences.

Funding & Support Opportunities



To help tackle cybersecurity challenges, Canadian municipalities can access various grants and funding programs. Resources like the following can support activities such as developing cybersecurity plans, procuring security technologies, and training IT and security staff:

- Canadian Safety and Security Program (CSSP) - The CSSP is a federally-funded program that supports projects enhancing public safety and emergency preparedness, including cyber threats and risks to critical infrastructure.^[12]
- AWS Provincial and Municipal Cyber Grant Program - Amazon Web Services (AWS) announced in 2024 that they are investing \$5 million CAD in AWS credits to new and existing AWS customers, with the goal of helping government institutions improve their security posture and advance their ransomware protection.^[13]

Securing cybersecurity funding requires a well-crafted proposal that clearly outlines a municipality's cybersecurity needs and objectives. Collaborating with other public sector partners can also improve the chances of success, as partnerships demonstrate a coordinated and comprehensive approach to cybersecurity.

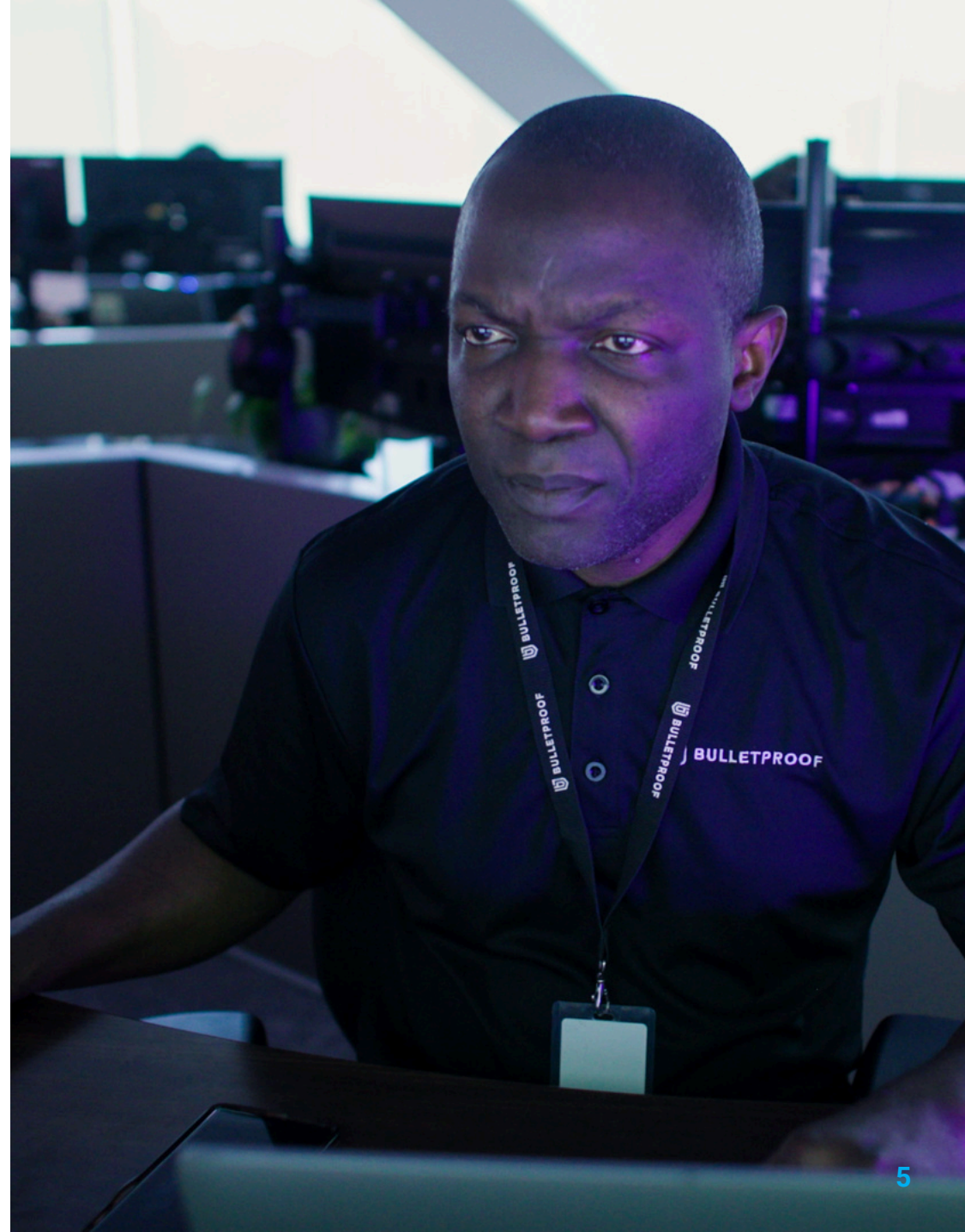
The rapid growth of cybercrime, coupled with the complexity of regulatory requirements and the shortage of skilled IT and security professionals, creates a challenging environment for municipalities. By leveraging available grants and funding opportunities, and by adopting robust cybersecurity frameworks and strategies, municipalities can strengthen their defences and better protect critical systems and data.

Chapter 2

What is Zero Trust and Why It Matters?

Zero Trust is a cybersecurity framework that fundamentally shifts how people approach network security. Unlike traditional models that rely on perimeter defences to keep out potential threats, Zero Trust operates on the principle that no one—whether inside or outside the network—should be trusted by default. This "never trust, always verify" philosophy requires continuous verification of the identity and integrity of users, devices, and applications each time they request access to resources.

Zero Trust is more important than ever as cyber threat actors adopt artificial intelligence in their toolkits. These technologies can generate realistic audio and video deepfakes that impersonate trusted individuals. AI is also used to craft personalized phishing emails at scale, mimicking writing styles to appear more convincing. Such tactics make it much harder for individual system users to detect threats, and easier for attackers to gain trust and manipulate their targets.



A Zero Trust assumption mandates that every access request must be thoroughly authenticated and authorized, regardless of its origin. Doing so minimizes the risk of unauthorized access and data breaches.

Guiding Principles of Zero Trust Include:

 VERIFY EXPLICITLY	 USE THE LEAST-PRIVILEGE ACCESS	 ASSUME BREACH
Ensuring that users are who they claim to be through multi-factor authentication (MFA) and other identity verification techniques.	Granting users the minimum level of access necessary to perform their tasks.	Keeping a vigilant eye on network traffic and user behaviour to detect and respond to anomalies in real time.

Why Does Zero Trust Matter?

Simply put: productivity, risk reduction, and compliance.

The unique nature of municipalities makes them prime targets for cyber threats. Cybercriminals are increasingly sophisticated, often targeting under-resourced IT departments. This vulnerability underscores the need for a robust security posture that Zero Trust provides.

Personal data, financial information, and confidential employment records are the types of information that cybercriminals seek out. Implementing Zero Trust ensures that only authenticated and authorized users can access this data, significantly reducing the risk of data breaches.

When it comes to securing critical infrastructure, municipalities are responsible—including water treatment facilities, emergency response, and public transit. A security breach in these areas can lead to severe disruptions and impact public safety. The Duffin Creek Water Pollution Control Plant in Ontario had a close call in 2024 when hackers breached the plant. Although the hackers were only able to access a limited part of the plant's digital systems before being stopped, a more extensive breach could have had catastrophic consequences for the wastewater treatment process that serves 1.2 million people.^[14]

Zero Trust helps safeguard these sorts of essential services by enforcing strict access controls and continuous monitoring, ensuring only verified users and devices can access sensitive systems at any time. In addition, municipalities are subject to a patchwork of regulations and compliance requirements aimed at protecting sensitive data. Implementing Zero Trust helps meet these requirements by providing a comprehensive security framework that ensures data integrity and confidentiality. The rigorous access controls and continuous monitoring can help demonstrate compliance with legal and regulatory standards.



In 2020, TransLink, the regional transportation authority for Metro Vancouver, experienced a cyberattack that exposed sensitive personal information. Former employees affected by the breach filed a proposed class action lawsuit. While the Supreme Court of British Columbia initially dismissed the case, the British Columbia Court of Appeal ruled in 2024 that it is possible for an organization that collects and fails to adequately protect personal information to be held liable for violating privacy. In March 2025, the Supreme Court of Canada declined to hear TransLink's appeal, confirming that the class action can move forward to the next stages.^[15]

The Value of Zero Trust

Public confidence is crucial for you. Data breaches and cyber attacks can erode this trust, making citizens wary of engaging with a municipality. By prioritizing Zero Trust, you can reassure the public that their data is secure and that the services they rely on are protected from cyber threats.

When it comes to day-to-day productivity, you can empower hybrid employees to work more securely wherever they choose to work from, on any device. Zero Trust helps you build a secure workforce through:

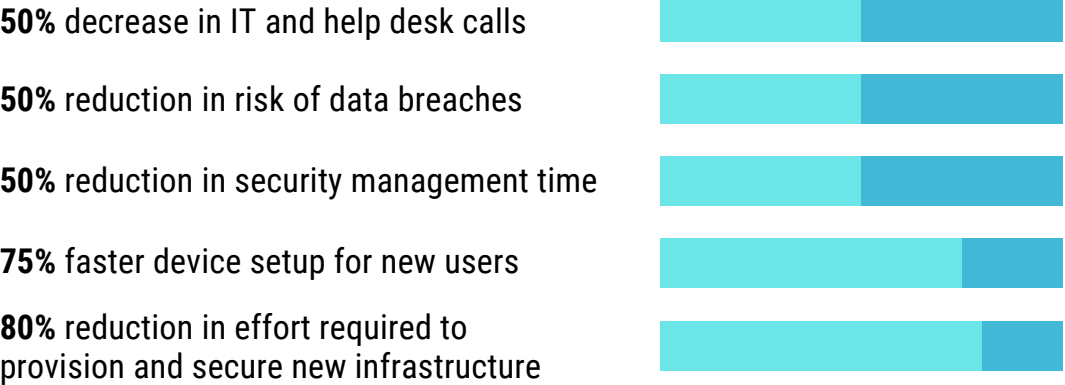
- Adaptable security policies
- Reduced security vulnerabilities
- Unified data protection and governance
- A layered defence system for access requests

According to Microsoft, their customers have saved over \$7 million in legacy software and infrastructure since implementing a Zero Trust approach. For more information about how Microsoft Security customers have benefited from adopting a Zero Trust approach, see their infographic [here](#).



Customers have seen an average of **92 percent return on investment** within less than six months of implementing a Zero-Trust approach.

Other trends reported include:



Over \$7 million in reduced spending on legacy software and infrastructure.

You can enhance your security posture, protect sensitive data, secure critical infrastructure, and maintain compliance with regulatory standards by using a Zero Trust security approach. Most importantly, you can build and maintain public trust in their ability to safeguard the essential services and information that citizens depend on.

Cyber insurance is also an important risk management component that municipalities should have. In a worst-case scenario, they will be prepared to quickly recover and minimize damage should a cyber attack occur. We will explore how to determine if cyber insurance is right for you in the next chapter.

Chapter 3

Is Cyber Insurance Right For You?

What is Cyber Insurance?

Cyber insurance is a policy product available through most business insurance providers that covers the costs incurred as a result of a cyberattack. It provides coverage for a range of cyber-related events, including data breaches, ransomware attacks, and other forms of cybercrime. Cyber insurance policies generally offer financial protection against losses stemming from cybersecurity incidents like:

DATA BREACH COSTS

Expenses related to notifying affected individuals, providing credit monitoring services, and managing regulatory compliance.

RANSOMWARE PAYMENTS

Coverage for ransom payments made to recover data or restore systems.

INCIDENT RESPONSE

Funds for hiring experts to investigate and remediate the breach, including IT forensics, public relations, and crisis management.

LEGAL FEES

Costs incurred from legal actions taken against the municipality due to a cyber incident.

BUSINESS INTERRUPTIONS

Compensation for lost revenue due to downtime caused by a cyber attack.



For municipalities, cyber insurance is particularly relevant as they manage sensitive information and critical services. The financial impact of a cyber attack on these institutions can be severe, making cyber insurance a valuable safety net.

While cyber insurance offers essential financial protection and support in the event of a cyber incident, it should never be considered as a replacement for proactive security measures.

Advantages and Limitations of Cyber Insurance

Because municipalities vary in size, resources, and risk exposure, there is no one-size-fits-all approach to cyber insurance. To make an informed decision, it's important to weigh both the advantages and limitations of coverage.



Advantages

FINANCIAL PROTECTION



Cyber insurance provides a financial buffer against the high costs associated with cyber incidents. This can mean the difference between a manageable recovery and a catastrophic financial loss.

INCIDENT RESPONSE SUPPORT



Many cyber insurance policies offer access to a network of experts who can assist in the aftermath of a cyber incident. This includes IT forensics, legal counsel, and public relations professionals who can help manage and mitigate the impact of the breach. For municipalities with limited internal resources, this support can be invaluable in navigating the complexities of incident response.

PEACE OF MIND



Knowing that financial and professional support is available in the event of a cyber incident provides peace of mind to administrators. This assurance can enable them to focus more on their primary responsibilities of serving the public and delivering essential services.

RISK MANAGEMENT



Insurers often require policyholders to implement certain security measures as a condition of coverage. This can drive you to adopt more rigorous cybersecurity practices, increase employee training and awareness, and enhance their overall security posture. Regular assessments and adherence to best practices become integral to maintaining coverage.

COMPLIANCE AND REGULATORY ASSISTANCE



Municipalities must comply with various regulatory requirements concerning data protection and breach notification. Cyber insurance policies often include resources to help organizations meet these obligations, reducing the risk of regulatory penalties and fines.

Limitations

COVERAGE GAPS



Not all cyber insurance policies are created equal. Coverage limits, exclusions, and specific terms can vary significantly between policies. Municipalities need to thoroughly understand their policy details to ensure they are adequately protected against the most relevant threats.

COST



Premiums for cyber insurance can be substantial, particularly for municipalities with a high risk profile or those that handle large amounts of sensitive data. Budget constraints for smaller municipalities might make it challenging to allocate funds for comprehensive coverage.

COMPLEXITY



The process of obtaining cyber insurance involves detailed assessments of municipalities' cybersecurity posture, which may require significant effort and resources. Additionally, the claims process can be intricate, requiring detailed documentation and proof of loss.

FALSE SENSE OF SECURITY



Relying too heavily on cyber insurance might lead some to become complacent in their cybersecurity efforts. It is crucial to remember that insurance is a complement to, not a replacement for, robust cybersecurity practices.

EVOLVING THREAT LANDSCAPE



Cyber threats are constantly evolving, and insurance policies may not always keep pace with new types of attacks. Municipalities need to continuously update their security measures and ensure their policies remain relevant and comprehensive.

```
41
42
43 class Invite {
44     use message1;
45 }
46
47 class Invite2 {
48     use message1, message2;
49 }
50
51 $obj = new Invite();
52 $obj->msg1();
53 echo "<br>";
54
55 $obj2 = new Invite2();
56 $obj2->msg1();
57 $obj2->msg2();
58
59 $x = 12345678;
60 var_dump(is_int($x));
61
62 $x = 12345.6789;
63 var_dump(is_int($x));
64
65 $d1=strtotime("December 25");
66 $d2=ceil(($d1-time())/60/60);
67 echo "There are " . $d2 . " day";
68
69
70 if (!filter_var($int, FILTER_VALIDATE_INT)) {
71     echo("Integer is valid");
72 } else {
73     echo("Integer is not valid");
74 }
75
76
77 include 'f1.p';
78
79 ?>
80
81 </body>
82 </html>
```

How to Determine the Right Amount of Cyber Insurance Coverage

Once you have decided that the benefits of cyber insurance outweigh the limitations, it's time to determine what the right amount is. This involves a careful assessment of your municipality's risk profile, resources, and overall cybersecurity strategy.

CYBER INSURANCE COVERAGE CHECKLIST

- Using risk models to help evaluate your need for cyber insurance will help visualize the potential impact. As municipalities manage sensitive personal information, financial data, and critical infrastructure, the potential impact of a cyber incident is often significant.
 - Assess your municipality's financial capacity to absorb the costs and deductibles associated with a cyber incident versus the premiums. Potential costs related to an attack can be projected based on historical data and the current threat landscape.
 - If there are gaps or weaknesses in your existing cybersecurity defences, the process of obtaining insurance may prompt you to implement necessary improvements. An audit of existing cybersecurity measures will help inform the level of insurance you will need.
 - Understand the regulatory requirements relevant to your municipality. Cyber insurance can help ensure compliance with data protection laws and mitigate the risk of penalties for non-compliance.
 - Negotiate with cyber insurance providers to find out if your municipality qualifies for any bulk purchases or flexible claims processes.
- While cyber insurance is not a panacea for all cybersecurity challenges, it plays a critical role in a comprehensive risk management strategy. It provides financial protection, promotes better security practices, and offers valuable support in the event of a cyber incident.





Chapter 4

How Municipalities Can Protect Themselves From 99% of Attacks

Municipalities are faced with many unique challenges and heightened risks due to the large amounts of sensitive data they keep, including the personal information of citizens, employment records, and government operations. The critical nature of their services makes being proactive in cybersecurity not just beneficial, but essential. This chapter will explore best practices for protecting your municipality, the importance of continuous security testing, and the value of partnering with security providers.

Fundamentals of Protecting Your Municipality

Just like brushing your teeth, showering, and washing your hands are part of good personal hygiene, there are also simple habits—known as cyber hygiene—that help keep your data and networks safe and healthy.

IMPLEMENTING MULTI-FACTOR AUTHENTICATION (MFA)

adds an extra layer of security by requiring multiple forms of verification before granting access to systems or data. This makes it significantly harder for attackers to gain unauthorized access, even if they have compromised a password. MFA should be implemented across all critical systems and applications. A study using Microsoft Entra data found that MFA reduced the risk of a cyberattack by 99.2%! ^[16]

MAINTAINING UP-TO-DATE SYSTEMS

is an important component of a strong cybersecurity defence. Unpatched and outdated systems are common entry points for attackers who exploit known vulnerabilities that have not been addressed. To mitigate this risk, it is essential to ensure that all components of your IT infrastructure, including firmware, operating systems, and applications, are regularly updated with the latest security patches and updates.

IMPLEMENTING EXTENDED DETECTION AND RESPONSE (XDR) AND ANTI-MALWARE SOFTWARE

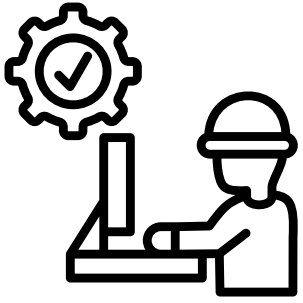
is crucial for a robust cybersecurity strategy. XDR integrates multiple security products into a cohesive system, enabling comprehensive threat detection, investigation, and response. By utilizing XDR alongside antimalware solutions, you can automatically detect and block attacks, reducing the window of opportunity for cybercriminals. These systems provide insights to security operations, allowing for real-time monitoring and swift response to threats.

APPLYING ZERO TRUST PRINCIPLES

as noted in Chapter 2 of this eBook, will help minimize the impact of an attack. As a reminder these principles are to: 1) explicitly verify, 2) use least privilege access, and 3) assume breach.

PROTECTING DATA

requires a comprehensive understanding of your municipality's critical information, its location, and the implementation of appropriate defences. Identifying and classifying important data helps in prioritizing security measures and allocating resources effectively. Knowing where sensitive data is stored and who has access to it enables the implementation of tailored protections such as encryption, access controls, and data loss prevention strategies. By continuously assessing and enhancing these defences, municipalities can ensure that their most valuable assets are safeguarded against unauthorized access and potential breaches, thereby maintaining data integrity and security.



Which Type of Security Testing is Right for You?

Cybersecurity threats are escalating. In its 2024 Digital Defence Report, Microsoft reported a 2.75x year-over-year increase in human-operated ransomware encounters and more than 7,000 password attacks blocked every second. ^[17]

To stay resilient, continuous security testing is essential. However, with various testing methods available, selecting the right approach for your municipality can be a complex decision.

A technical security assessment involves evaluating the security of a system or application by identifying vulnerabilities, assessing risks, and testing the system's response to potential attacks. Confusion often arises during the vulnerability assessment phase, as teams may struggle to determine what is required for regulatory compliance and which security tests provide the best value. This is also when some municipalities consider penetration testing, but a lack of understanding about its value and appropriate use cases can lead to ineffective application of this test.

► VULNERABILITY SCANNING

Vulnerability scanning involves a combination of manual and automated tools that search for known vulnerabilities within your systems and applications. While vulnerability scanning is less thorough than penetration testing, it is a cost-effective way to maintain security hygiene. Key attributes of vulnerability scanning include:

- Typically general in scope and includes a large assessment
- Predictable in how they identify vulnerabilities
- Unreliable at times because they do not simulate exploits
- Often invites debate among system administration
- Produces a report with mitigation guidelines and action items

► PENETRATION TESTING

Penetration testing, or ethical hacking, involves simulating real-world attacks to identify and exploit vulnerabilities. This type of testing provides a comprehensive assessment of your security posture and helps in understanding how attackers might infiltrate the network. Key components include:

- Focused in scope and may include targeted attempts to exploit specific vectors
- Simulates hacking, resulting in unpredictable findings
- Highly accurate and reliable due to expert testing and realistic simulations
- Penetration test can be a proof of concept against vulnerabilities
- Produces a binary result (yes or no)

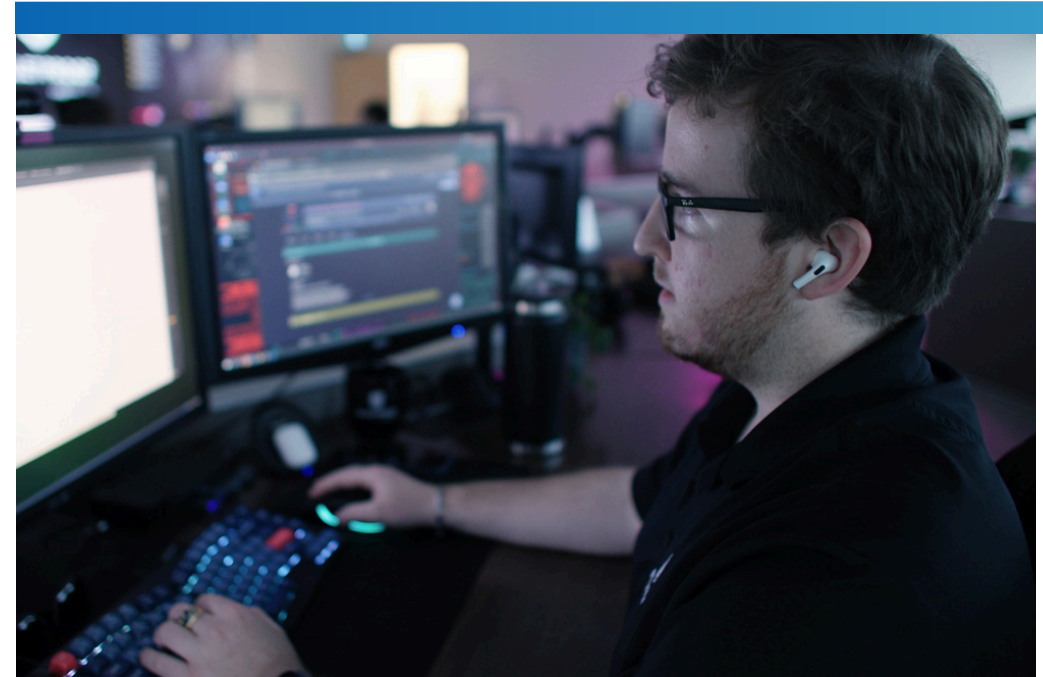
Trusted third-party cybersecurity experts enable municipalities to identify and implement the most appropriate testing methods tailored to their specific cybersecurity needs. Collaborating with an external team of experts helps determine whether vulnerability assessments and penetration testing can be enhanced by incorporating additional relevant security tests, such as vulnerability scanning, operational testing, and risk assessments.

Third-Party Providers To Bolster Your Defences

Specialized security providers can help you achieve your security goals more efficiently. One of the primary advantages of working with security providers is access to specialized expertise and advanced tools. These providers possess in-depth knowledge and experience that might not be available in-house, along with cutting-edge technologies that can bolster defences.

Another significant benefit is the scalability and flexibility that security providers offer. They can tailor their solutions to meet your specific needs. This adaptability ensures that the security measures can grow and evolve with you.

Building and maintaining an in-house cybersecurity team can be a substantial financial burden. Partnering with security providers offers a more economical alternative, granting access to high-quality security services without the need for significant investment in personnel and infrastructure. This approach allows municipalities to allocate their resources more efficiently while still maintaining a strong security framework.



In the event of a cyber-attack, these providers can respond quickly and effectively, drawing on their extensive experience and resources to manage the situation. This swift action minimizes damage and recovery time, ensuring that you can resume normal operations as quickly as possible.

By implementing the fundamentals of cyber hygiene, performing continuous security testing, and partnering with a security provider, you can protect against 99% of attacks, ensuring the safety and trust of the communities you serve.

Chapter 5

The Power of Partnership: Joining Forces With IT & Security Providers

Municipalities lacking in internal resources and expertise can benefit by collaborating with third-party experts to implement advanced security measures efficiently. External partnerships also offer the opportunity to bring specialized knowledge and cutting-edge technologies to your team. This chapter further explores the importance of such partnerships, the key benefits they offer, and actionable steps to get started.

IN-HOUSE CYBERSECURITY TEAMS

This allows for greater control and direct oversight of IT and security operations. It enables a municipality to develop a deep understanding of its unique environment and tailor solutions accordingly. However, building a proficient in-house team requires significant investment in recruiting, training, and retaining skilled personnel. Additionally, the rapidly evolving threat landscape demands continuous professional development and access to the latest technologies, which can strain resources.

PARTNERING WITH SECURITY PROVIDERS

This provides immediate access to a pool of seasoned experts and state-of-the-art tools. External providers are often at the forefront of cybersecurity advancements, offering comprehensive services such as threat detection, risk assessment, and incident response. This model allows you to scale your security efforts based on current needs and budget constraints, making it a cost-effective solution. It can complement existing in-house capabilities, creating a hybrid approach that leverages the strengths of both models. Using outside expertise to conduct security posture assessments also provides an external and unbiased perspective.



5 Key Benefits of Partnering With Experts

ACCESS TO EXPERTISE AND ADVANCED TOOLS

One of the primary advantages of partnering with IT and security providers is the access to specialized knowledge and advanced technologies. These providers possess in-depth expertise that may not be available internally, ensuring that you can implement robust and sophisticated security measures.

24/7 SECURITY MONITORING & RESPONSE

In the event of a cyberattack, having a security provider at the ready to manage threat detection & response is the ultimate in peace of mind. These providers have extensive experience in handling security incidents and can respond quickly and effectively, minimizing damage and recovery time.

REGULATORY COMPLIANCE

Compliance with regulatory requirements is a critical aspect to consider. IT/Security providers are well-versed in the various regulations and standards that apply to different sectors. They can assist in ensuring that all necessary measures are in place to comply with these requirements, avoiding potential legal and financial penalties.

COST-EFFECTIVENESS

Building and maintaining an in-house cybersecurity team can be a substantial financial burden, especially for smaller municipalities with limited budgets. Partnering with security providers offers a more economical alternative, granting access to high-quality security services without the need for significant investment in personnel and infrastructure. This approach allows you to allocate their resources more efficiently while still maintaining a strong security framework.

SCALABILITY AND FLEXIBILITY

Security needs can vary significantly based on the size, structure, and threat landscape of a municipality. Security providers offer scalable solutions that can be tailored to your specific requirements. Whether it's managed security services, security testing & audits, network or infrastructure support, these providers can adapt to your needs, providing flexible solutions that grow with the municipality.



Assembling your own cybersecurity team can be costly, and the salaries for cybersecurity professionals are rapidly increasing with no signs of slowing down. If you haven't yet considered partnering with a security company, think about the risks you are assuming by not investing in one. Explore your options to find the right IT & security provider that matches your cybersecurity needs.

How You Can Get Started

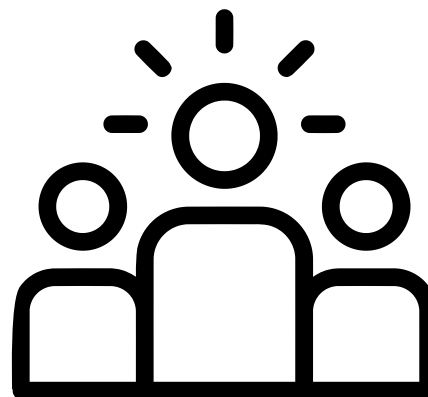
Starting a partnership with an IT & security provider involves several steps to ensure a successful collaboration.

First, you should assess your needs. Conduct a thorough assessment of your current cybersecurity posture and identify areas where you need external support. Determine the specific services you require, such as threat detection and response, ransomware protection, employee cybersecurity awareness training, risk assessment, or incident response.

With your needs identified, research and shortlist potential IT and security providers based on their expertise, reputation, and the range of services they offer. Look for providers with experience in serving municipalities, as they will have a better understanding of the specific challenges and regulatory requirements.

Once you have identified the right provider with solutions that match your needs, illustrate your business case to get leadership and budget buy-in before formalizing the partnership.

Partnering with IT and security providers is a strategic move to enhance your cybersecurity posture and protect critical infrastructure. By leveraging the expertise and advanced tools of external providers, municipalities can implement robust security measures, respond swiftly to incidents, and ensure regulatory compliance. Taking proactive steps to engage with security providers will position you to navigate the complex cybersecurity landscape effectively and ensure the safety and well-being of the communities you serve.



What Leaders Can (And Should) Do Next

With cyber threats becoming increasingly sophisticated and pervasive, it is more important than ever for you to adopt a proactive approach to cybersecurity. Municipal leadership must recognize the urgency of safeguarding their data and those of their constituents from cyberattacks.

In this eBook, you've learned why implementing proactive measures such as continuous monitoring, regular security assessments, timely updates, and employee training is fundamental to preventing cyber incidents and reducing the risk of breaches.

You've also learned that adopting Zero Trust principles, such as explicitly verifying access, using least privilege, and assuming breach, can significantly enhance security. Knowing and protecting critical data, ensuring regulatory compliance, and maintaining up-to-date systems are vital components of a robust cybersecurity strategy.

5 Key Steps for Municipal Leaders to Strengthen Their Security Posture

1. ENGAGE AND STAY INFORMED WITH LEADERS AND PEERS

Leadership should get involved and network with government experts and peers to stay informed about the latest cybersecurity trends, challenges, and regulatory changes. Participating in conferences and working groups can provide valuable insights and facilitate knowledge sharing. Understanding the broader government landscape helps leaders anticipate emerging threats and adapt their strategies accordingly. Building a network of trusted contacts can also facilitate collaboration and support in times of crisis.

2. SCHEDULE REGULAR SECURITY TESTING AND AUDITS

Regular security testing and audits are essential components of a proactive cybersecurity strategy. You should establish a routine schedule for penetration testing, vulnerability scanning, and comprehensive security assessments. These evaluations help ensure that security measures are effective and up-to-date. By identifying and addressing weaknesses proactively, you can minimize the risk of a major breach while enhancing your overall security posture.

3. INSTILL THE IMPORTANCE OF CYBERSECURITY IN YOUR WORK CULTURE

Cybersecurity is not just a technical issue but also a cultural one. A strong cybersecurity culture is built from the top down—municipal leaders must instill the importance of cybersecurity within their work culture. This involves educating employees about best practices, conducting regular training sessions, clearly communicating policies, and encouraging a vigilant mindset. Employees are often the first line of defence against cyber threats, and they should feel empowered to report suspicious activities and understand the importance of following security protocols. By fostering a culture of cybersecurity awareness, organizations can significantly reduce their risk exposure.

4. INVESTIGATE CYBER INSURANCE

While cybersecurity measures are the first line of defence, cyber insurance can provide an additional layer of protection. You should investigate the benefits of cyber insurance and determine if it aligns with your risk management strategy. Cyber insurance can cover costs associated with data breaches, such as legal fees, notification expenses, and recovery efforts. Understanding the scope and limitations of coverage is essential for making an informed decision.

5. PARTNER WITH IT/SECURITY EXPERTS

Collaborating with third-party IT/security experts who understand the unique challenges of municipal government can significantly enhance your IT & cybersecurity posture. These experts can provide guidance, support, and advanced solutions that complement internal efforts. By partnering with experienced providers, you can focus on your core projects.

Take Action Today

As the cyber threat landscape continues to evolve, government leaders must take a proactive and strategic approach to their IT and cybersecurity. By following the key steps outlined in the eBook, you can make informed decisions that will strengthen your defences and protect your critical infrastructure. Taking action now will ensure that you are prepared to face the challenges of today and tomorrow, securing a safer digital future for all.

Contact Us Today



BULLETPROOF

a GLI company



Microsoft
Solutions Partner

References

- 1 p. 23 <https://www.cira.ca/uploads/2024/09/CIRA-2024-Cybersecurity-Report.pdf>
- 2 p. 6 <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>
- 3 <https://globalnews.ca/news/10155151/companies-1-million-ransomware-attacks/>
- 4 p. 20 <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>
- 5 <https://www.hamilton.ca/cyberincident>
- 6 <https://hamiltonindependent.ca/hamilton-cyberattack-recovery-has-now-cost-9-6-million/>
- 7 <https://www.chch.com/chch-news/city-of-hamilton-budgets-over-52m-for-2024-cyberattack-response/>
- 8 <https://www.townandcountrytoday.com/westlock-news/breaking-town-of-westlock-hit-with-cybersecurity-incident-involved-personal-information-of-residents-8926444>
- 9 https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/
- 10 <https://www.canada.ca/en/parole-board/corporate/transparency/access-to-information-and-privacy.html>
- 11 p. 7 https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
- 12 <https://science.gc.ca/site/science/en/canadian-safety-and-security-program>
- 13 <https://aws.amazon.com/blogs/publicsector/aws-canada-launches-5-million-provincial-and-municipal-cyber-grant-program/>
- 14 <https://www.theglobeandmail.com/canada/article-duffin-creek-water-ransomware-hack/>
- 15 <https://knd.law/class-actions/south-coast-bc-transportation-authority/>
- 16 <https://arxiv.org/abs/2305.00945>
- 17 p. 9, p. 39 <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20defence%20Report%202024%20%281%29.pdf>