Cyber Defenders, LLC

The ultimate guide to municipal cyber security

Insights and advice for building better defenses

FIELD EFFECT / Partners

Table of Contents

Introduction

It might sound strange, but The Hobbit offers some wisdom for municipalities looking to defend against cyber threats. In it, J.R.R. Tolkien wrote, “It does not do to leave a live dragon out of your calculations, if you live near one.”

If you were to imagine a map of the cyber security landscape, it would be full of “Here be dragons” warning signs. The fact is, these days there are dragons living near every municipality.

Attacks on towns and cities are becoming far more common and complex, and municipalities everywhere have become targets of sophisticated attacks that can bring civic operations to a grinding halt. The unique intersection of personally identifiable information, critical services and infrastructure, and varying levels of needed protection put municipalities squarely in the crosshairs of cyber criminals.

Adopting effective cyber security measures and defending against this onslaught is particularly challenging for municipal governments and public utilities—but it’s far from impossible.

This ebook will show you:

- The changing threat landscape facing municipalities
- The regulatory requirements to navigate
- Best practices for defending against ever-increasing threats
- What the future has in store

Rising municipal cyber threats

The rising tide of cyber threats facing municipalities can be chalked up to several factors, chief among them the scarcity of cyber talent and resources. Combined with expanding threat surfaces and the growing cyber crime-as-a-service (CaaS) economy, it's no wonder that municipalities are finding it harder and harder to defend themselves.

Challenges in accessing cyber talent and resources

Cyber security expertise is at a premium, meaning that finding the human resources you need, let alone having the money to hire them—at a time when budgets are facing even more intense scrutiny—is a very tall task. Resources are stretched thin, and building an in-house security team is often not an option.

What's more, replacing and updating legacy IT systems can be almost impossible in a municipal setting. Individual tools and solutions might fit your budget needs, but building a complete toolset can often exceed what's been allocated for the year.

Expanding threat surfaces

The world is more and more digitized, with tools and technology creating new connections between information technology (IT) and operational technology (OT). Problem is, each new connection increases an organization's threat surface, also known as the areas of an IT network where bad actors can exploit vulnerabilities and access critical systems and confidential data.

From a business perspective, it makes sense to digitize OT; it helps increase efficiency, letting organizations automate and manage systems that would otherwise demand more time out of already busy days. But for as many benefits and efficiencies as it provides, if your digitized OT is left unsecured, it presents a perfect target, whether for direct attack or as a way to infiltrate other parts of your infrastructure.

Compounding all of this is the fact that employees are still getting used to remote work. While the rush to deploy new technologies in a COVID-19 world made it possible to work safely from home, each remote connection to your IT environment introduces risk. For staff not familiar with remote work tools, this shift has made them, and your network, more vulnerable to cyber attacks.

The cyber-crime-as-a-service economy

The technology employed by cyber criminals is also evolving, and much of it is now easily accessible through the online black market. Inexperienced hackers can now buy ransomware kits for as little as $50. Fast access to premade tools has given rise to the cybercrime-as-a-service (CaaS) economy, removing the barrier to entry for staging highly sophisticated attacks. Because someone else has already done the work and built the software, would-be attackers can quickly automate a cyber-attack on a municipality that, if successful, could result in significant ROI.

HOW ATTACKERS ARE CHANGING THEIR TACTICS

Until very recently, the goal of an attacker was to infiltrate a network, deploy malware or ransomware as quickly as possible, make a sizable ransom demand, and hope the victim hadn't backed up their data.

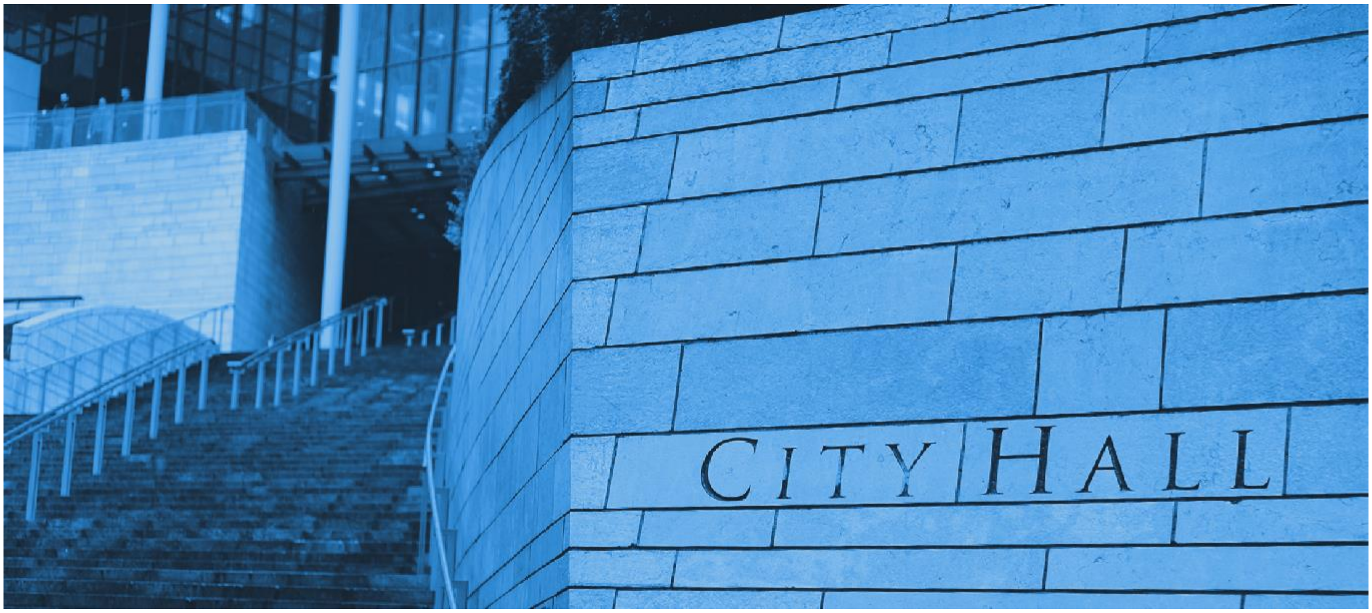
Today, when an attacker gains access, they're more likely to hide on your network and gather more intel, letting them target data backups alongside OT, or gather enough information to compromise other aspects of your IT infrastructure. Payment demands are typically lower but much more frequent; attackers have learned that insurance companies will pay some ransoms just to make the problem go away.

THEN

- Access a network and deploy malware or ransomware as soon as possible
- Huge ransom demands
- Smash-and-grab approach
- Easily thwarted with regular data backups

NOW

- Infiltrate a network and gather information about how it works and is used
- Make social engineering techniques more effective
- Relatively reasonable ransom demands increase the chances of payment
- Slower-paced approach
- Attacks can take place long after a criminal has gained access and infiltrated multiple systems



The regulatory landscape

The unique combination of confidential data, critical services, infrastructure, and financial information held by municipalities and utilities puts them in scope of a range of complex regulatory requirements. Municipal regulations around cyber security and IT are designed to protect the public (both in terms of confidential data and ensuring services and infrastructure are safe and secure), but it can sometimes feel like wading into a rough sea of compliance acronyms.

Following accepted standards can help your municipality ensure continued compliance while delivering benefits and improvements to your overall cyber security posture.

These frameworks build on the body of expertise found in the cyber security field, letting organizations take advantage of established knowledge and put it to work for their needs. For the most part, they emphasize easy-to-implement practices that impact network and security processes and focus on improving visibility into network configuration and behaviour.

Navigating regulations and frameworks

To better understand how these regulations and frameworks interact, consider the compliance responsibilities of electric utilities in the province of Ontario. The Ontario Energy Board (OEB) is a provincial regulator overseeing how utilities operate, with considerations for privacy concerns. Electric utilities must be able to demonstrate compliance with two pieces of legislation: the Municipal Freedom of Information and Protection of Privacy Act at the provincial level, and the Personal Information Protection and Electronic Documents Act at the federal level.

On top of this, the OEB has its own cyber security and privacy framework, created in response to concerns raised by a 2016 survey of electrical distribution companies. Based on NIST's Cybersecurity Framework, the OEB's goal is to raise awareness of cyber security and privacy risks, supporting utilities as they improve their security posture. Following NIST's framework would more than likely mean you've checked the boxes for the OEB, too.

But there's a wrinkle: energy flows across borders. If a Canadian municipal utility sells surplus energy to a community in the United States, they'll also have compliance requirements under the Federal Energy Regulatory Commission (FERC). FERC oversees cyber security for electrical utilities, following the NERC Critical Information Protection (CIP) standard as part of the compliance process for transmission owners, generators, and distribution systems. Any tools connected to OT that could interact with bulk energy systems could fall in scope of additional regulatory requirements with FERC.

While the CIP and NIST's Cybersecurity Framework share some overlap, they don't have one-to-one alignment, and additional work may be necessary to ensure compliance.

COMMON REGULATIONS AND FRAMEWORKS

NERC CIP:

The North American Electric Reliability Corporation Critical Infrastructure Protection is a security standard designed to help protect bulk electric systems, meaning operational technologies in US utilities.

NIS DIRECTIVE:

The European Union's (EU) Security of Networks & Information Systems (NIS) Directive is a set of regulations that was created to increase the cyber security and resilience of key systems across the EU.

NIST:

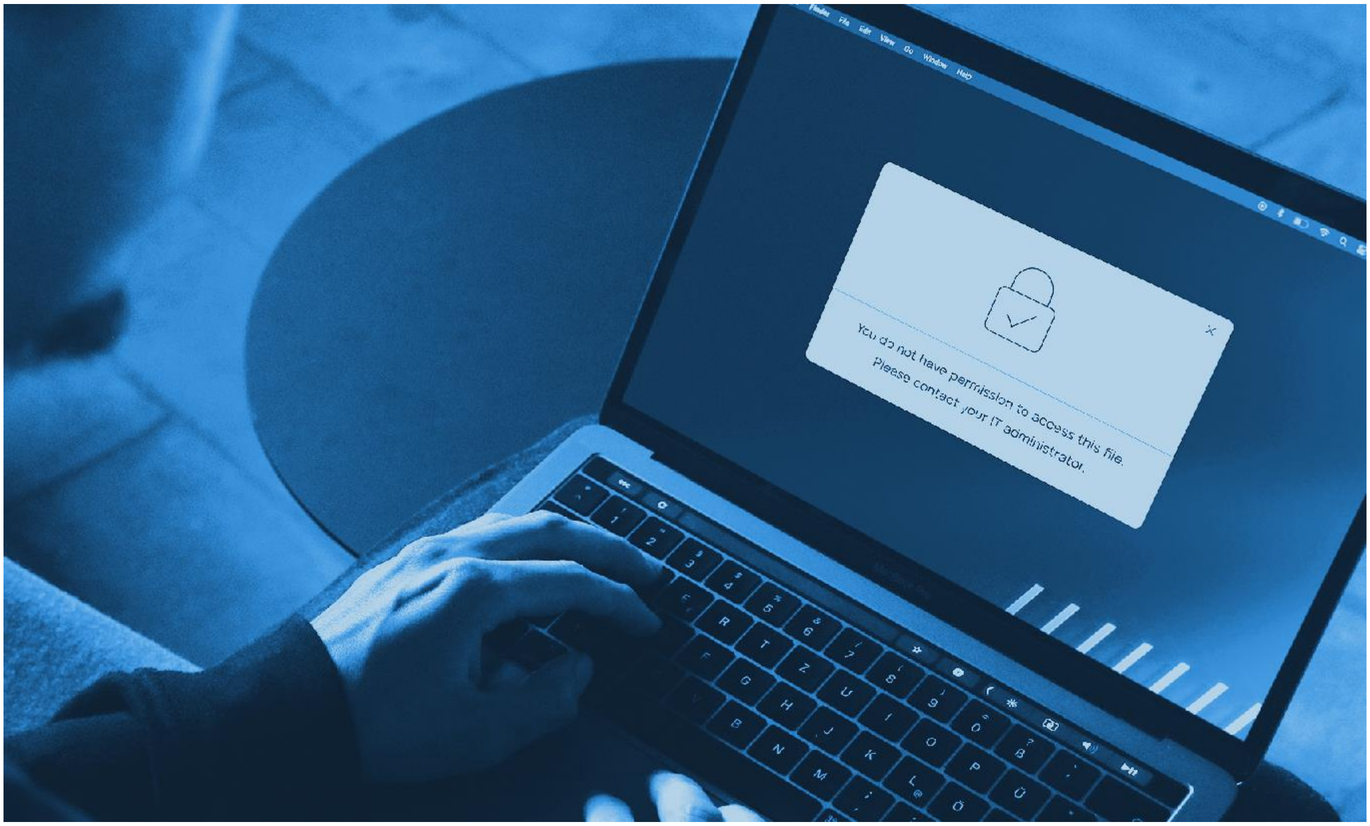
The National Institute of Standards and Technology (NIST) is an agency within the United States Department of Commerce. Though not a regulatory agency, NIST developed and maintains the widely used NIST Cybersecurity Framework, which helps organizations meet their regulatory requirements and improve their security.

ISO/IEC:

ISO/IEC 270001 is a security standard jointly developed by the International Organization for Standardization (ISO) and the International Electrochemical Commission (IEC) that outlines accepted best practices for managing information security.

PCI DSS:

The Payment Card Industry Data Security Standard is used by organizations that handle branded credit cards and was created to enhance controls around cardholder data in an effort to reduce credit card fraud.



You do not have permission to access this file.
Please contact your IT administrator.

Defending against rising cyber attacks

Benjamin Franklin said, “An ounce of prevention is worth a pound of cure.” He may not have been speaking about municipal cyber security, but it applies just the same. Taking the time now to ensure you’re following accepted best practices can help in the event of an attack–or help prevent one entirely.

Getting the basics right

Human error remains one of the leading causes behind a data breach. Taking the time to check that your IT network and cloud services, including viewing permissions, are properly configured can help you identify and resolve security issues to limit the possibility of human error. Putting basic cyber security controls in place will immediately have a strong, positive effect on your defences.

This process builds your cyber situational awareness (CSA), which is best defined as knowing your network, knowing the threats facing it, and knowing how to respond to them. With this insight, you can identify and address "quick win" issues like correcting access privileges.

CSA can also help you develop a cyber security playbook. You might already have similar guides for municipal emergencies like wildfires, floods, or public health crises; having one for a cyber attack is just as important.

Your cyber security playbook should detail key action steps for:

- Incident detection, notification, analysis, and forensics
- Response actions, specifically containment, remediation, and restoration
- Ongoing communication with stakeholders and customers
- Post-incident analysis to determine what happened and how your organization handled it

Start by focusing on the mission-critical aspects of your organization to identify priorities following an attack. What needs to be fully operational as soon as possible? What systems can wait? These questions, along with an understanding of your requirements from a regulatory perspective, can help identify key components of your cyber security plan. Making a playbook can also help get boards and senior leadership invested in the issue. Highlighting risks, potential impact, and steps you can take to respond will make it easier to get buy-in on security initiatives.

Remember to test your plans regularly, too. For example, it's important to back up your data, but you need to be sure you have quick access to those backups so you can restore operations as soon as possible. Consider the financial services sector, where organizations commonly conduct annual IT disaster recovery tests followed by a business continuity test. Apply the same thinking to your cyber security plans. Regularly testing and assessing your incident response capabilities will help you spot areas of improvement and address them accordingly.

Low-cost steps you can take right now

It may sometimes feel like the only way to defend your municipality is to increase budget or allocate additional resources. The good news is there are plenty of steps you can take now to dramatically improve your security posture, some of them without any additional spend.

Know your network

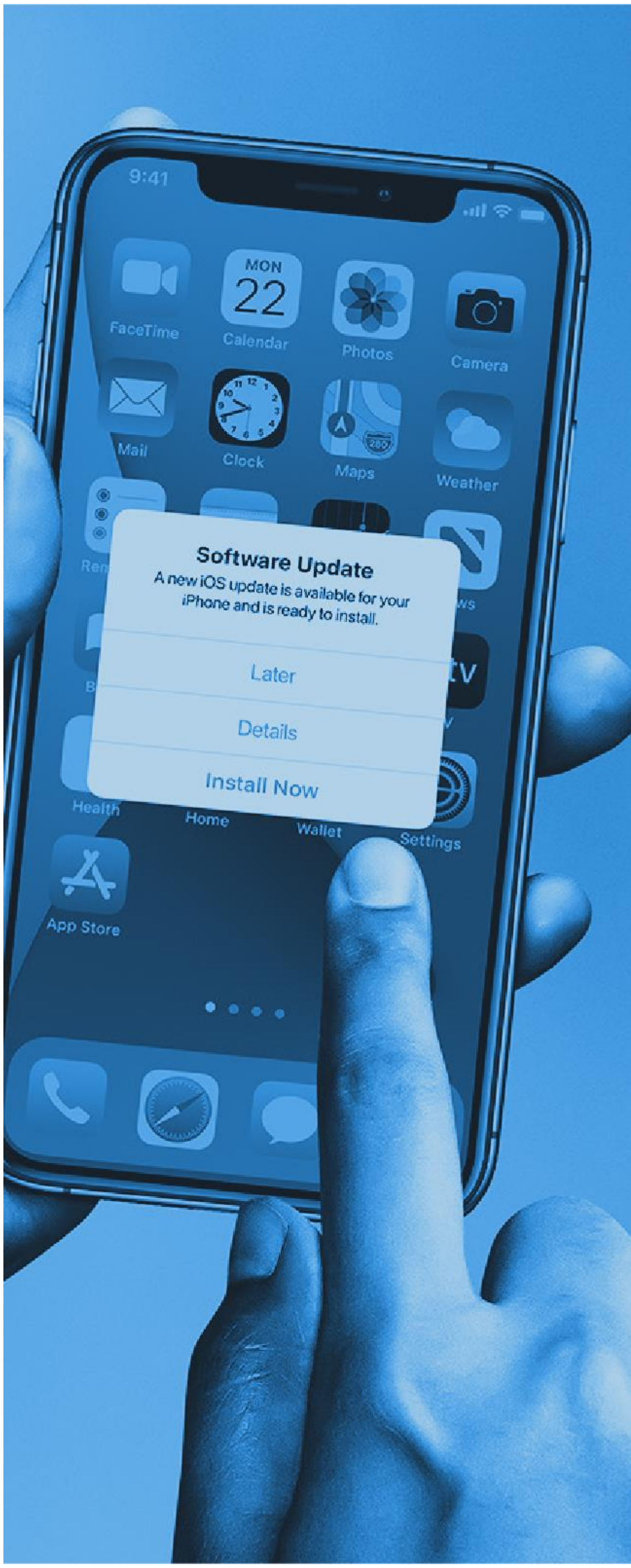
Gaining a better understanding of your IT network is the first step in reducing your threat surface. It’s vital to know what devices are on your network, how they’re used, and who’s using them. You should also understand how your network is configured. This will all help you spot potential vulnerabilities and suspicious activity early, letting you act quickly to close gaps.

Patch software (and keep patching it)

A recent report found that a shocking number of data breaches occur due to security gaps that could have been closed if an available software patch had been applied. Patches and updates don’t just remove potential software bugs, they’re also created to address known security issues. If there’s a patch available, apply it.

Invest in employee education

The weakest link in the chain of cyber security is always going to be the user. Humans make mistakes, and the only way to prevent them is through education. Training employees to identify potentially malicious emails, links, and activity will take time, but it will help foster an invaluable security-first culture.



Software Update

A new iOS update is available for your iPhone and is ready to install.

Address the human element

Security is the responsibility of every employee in an organization. It's vital that staff at every level understand their role and are up-to-speed with practices and policies designed to protect your municipality.

Developing a security-first mindset and culture can help your organization share knowledge and expertise across your workforce, ensuring users always feel empowered to raise a red flag when they notice something suspicious. Ongoing cyber security education and training doesn't have to be costly, there are plenty of free resources available to organizations of all sizes and in every sector.

Improve municipal network visibility

Your best defence is the ability to spot and stop a threat before it can cause an issue. Getting visibility across your network is absolutely vital. Think of it like this: if you ran a bank, you'd want to have guards on duty to watch for suspicious activity. People can only watch so much at any given time, though, so you'd also need security cameras. As an extra layer of protection, you'd add motion detectors to particularly sensitive parts of the bank.

Modern municipal cyber security demands a similar sort of visibility. Without accurate insights into what's going on in your cloud services, digitized operational technology, and the endpoint devices your staff use, it's much harder to spot potential threats to your services. You need to be able to monitor, detect, and respond to threats in a timely manner to mitigate the risks of a cyber attack.

Looking ahead

Attacks on municipal utilities are becoming so common that many executives believe it's not a question of "if" but "when."

One theme that keeps rising to the top of the cyber security conversation is prevention. Planning ahead is vital; building playbooks to deal with natural disasters and other emergencies is common, and cyber security incidents should be no different. But cyber threats are always evolving, making long-term predictions about the future challenging—but not impossible.

Finding a partner that provides these insights along with 24/7/365 cyber threat monitoring, detection, and response across all of your endpoints, networks, and cloud services is critical. An all-in-one solution not only helps you reduce your costs, but it eliminates security gaps and simplifies IT administration so you can focus on delivering innovative services to your community.

Sources

1 https://www.forbes.com/sites/daveywinder/2020/04/28/revealed-the-supermarkets-that-will-sell-you-malware-for-50/?sh=4f793a9930ae

2 https://www.nerc.com/Pages/default.aspx

3 https://www.nist.gov/cyberframework

4 https://www.iso.org/isoiec-27001-information-security.html

5 https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

6 https://www.oeb.ca/sites/default/files/Staff-Report-Cyber-Security-Framework-20170601.pdf

7 https://enterprise.verizon.com/resources/reports/dbir/2020/results-and-analysis/

8 https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

Contact our team today

About Cyber Defenders LLC

Cyber Defenders LLC is a Service Disable Veteran and Minority owned Managed Security Service Provider. We, along with our partners, provide a hands free managed detection and response solution. We protect your endpoints, networks and cloud services – all from one platform.

Email
r_wyche@cyberdefendersllc.com

Phone Number
888-314-9444

Website
https://cyberdefendersllc.com/contact-us

FIELD EFFECT™

CYBER DEFENDERS, LLC