ISSUE PAPER SERIES

Municipal Cybersecurity: Quick Q&A Guide for Local Officials

December 2025

NEW YORK STATE TUG HILL COMMISSION

DULLES STATE OFFICE BUILDING · 317 WASHINGTON STREET · WATERTOWN, NY 13601 · (315) 785-2380 · WWW.TUGHILL.ORG

Municipal Cybersecurity: Quick Q&A Guide for Local Officials

Table of Contents

The Tug Hill Commission Technical and Issue Paper Series are designed to help local officials and citizens in the Tug Hill region and other rural parts of New York State. The Technical Paper Series provides guidance on procedures based on questions frequently received by the Commission. The Issue Paper Series provides background on key issues facing the region without taking advocacy positions. Other papers in each series are available from the Tug Hill Commission. Please call us or visit our website www.tughill.org for more information.

Introduction

This guide provides municipal officials with practical, actionable cybersecurity information tailored to the needs of small towns and villages. It summarizes essential concepts and focuses on the risks, responsibilities, and low-cost actions that matter most. Local governments can use this document as a quick reference during planning, training, and incident response.

Why should my municipality worry about cyberattacks?

Cyberattacks are no longer rare, big-city problems- they now routinely hit towns and villages. Criminals target local governments because their systems are essential and often under-resourced. When a cyber incident occurs, services can stall, billing systems can lock up, websites can go dark, and sensitive data can be exposed. These disruptions aren't just technical issues - they undermine resident trust, interrupt basic governmental operations, and can take months, and a considerable amount of money, to fully resolve. Municipal governments are soft targets, and attackers take advantage.

What types of cyberattacks hit small local governments?

The most common are **phishing emails** that trick staff into clicking on dangerous links or handing over credentials, **ransomware** that locks files and demands payment, **business email compromise** that redirects payments to fraudulent accounts, and **malware infections** from outdated systems. Increasingly, attackers impersonate help desk or vendors over the phone (**vishing also known as voice phishing**) to gain remote access. Even third-party vendors like Information Technology (IT) contractors or software providers can be exploited and used as a pathway into your systems.

Why are small municipalities targeted by cybercriminals?

The overwhelming motive is financial. Criminal groups target municipalities because they assume towns have outdated systems, limited monitoring, and limited staff capacity. Some attackers simply blast thousands of phishing emails hoping someone clicks; others target critical infrastructure like water systems. Insider threats, both intentional and accidental, also occur, especially when account access isn't well managed. State sponsored attackers focus more on intelligence or disruption, but most small-municipal incidents come from financially driven cybercriminals. These attackers deliberately target smaller municipalities because they assume security is limited. Attackers search for the most vulnerable targets, not the biggest. Towns with a single clerk, part-time IT, or aging systems are often easier to compromise than large governments with full security teams. Many of the worst real-world incidents have occurred in small or mid-sized municipalities where monitoring, training, and software updates were inconsistent.

What does a cyber incident look like in real life?

It rarely starts dramatically. It usually starts with something simple: an email password stops working, the billing system locks up, files display strange extensions, the water plant's SCADA screen flickers, or the printer suddenly spits out unreadable pages. Within minutes, attackers may move across systems looking for sensitive data or administrator privileges. If ransomware

is involved, computers may display a note demanding payment, usually in cryptocurrency. Meanwhile, staff scramble to determine what still works and what data might have been accessed. Once a cyber incident begins, even with minor technical issues, it can quickly escalate into disruptions that affect every essential municipal service. Cyber incidents can shut down permitting, payroll, tax collection, emergency dispatch communication links, and even water or wastewater control systems. Websites used for public notices or payments may go offline. In some cases, towns have been forced back to paper records for weeks. Water systems have been manipulated in attempted contamination events. Even after systems come back online, the public may question whether their information is safe, or whether the municipality handled the event properly.

What can a cyberattack cost and how does it disrupt municipal services?

Costs vary, but even small incidents can exceed a municipality's contingency budget. Expenses include IT forensics, system rebuilds, hardware replacement, data recovery, legal support, overtime, and communication costs. Insurance deductibles are often high. Studies show that public sector breaches average nearly $3 million in total impact, and ransomware recovery regularly exceeds the ransom demand. Even after recovery, long-term costs can include higher insurance premiums, reduced investor confidence, and delayed projects.

What does New York law require municipalities to do?

Under Article 19-C, all municipalities must report cybersecurity incidents within 72 hours, ransom demands within 24 hours and must file a written explanation if ransom is paid. These reports are confidential under the Freedom of Information Law (FOIL). Under State Technology Law §103-f, all municipal employees must complete annual cybersecurity awareness training beginning in 2026. Under GML §300, municipalities with populations of 1,500 + must maintain a ".gov" website, which also introduces new cybersecurity responsibilities for public facing systems.

What is the board's role in cybersecurity?

Boards should provide oversight. That means ensuring policies exist, confirming employee training is up to date, asking vendors for regular status updates, and verifying that backups, updates, and account management practices are being maintained. Boards should receive short, quarterly check-ins and annually reapprove the cybersecurity policy and incident response plan. Good governance rather than technical ability, is key.

What is an incident response plan and what should it include?

An effective incident response plan for a municipal government should clearly outline the steps staff must take the moment something looks wrong, assigning roles, communication pathways, and responsibilities so that even small towns without an IT department can respond quickly and confidently. The plan should specify who disconnects affected devices, who contacts the IT vendor or county IT, who suspends compromised accounts, and who notifies leadership and state authorities, including required Article 19-C reporting deadlines. It must include printed emergency contacts, NYS DHSES, CISA, FBI, State Police, and vendor support so they are

available during outages, and should define which officials are authorized to make public statements if services are disrupted. As most municipal cyber incidents begin with subtle systems malfunctions, the plan should emphasize early detection, documentation of what happened and when, and coordinated communication between clerks, administrators, elected boards, and external IT partners. Ultimately, a municipal incident response plan provides a simple, repeatable framework that helps towns and villages contain damage, protect public services, and recover efficiently. This response plan can fit into the broader incident response plan by forming the practical, first hour playbook that anchors the entire response cycle. While a full incident response plan includes responses to various other scenarios, this will be a good addition to any plans already established.

Who is responsible for cybersecurity in a small municipality?

In most towns and villages, there is no dedicated IT department, so the responsibility is split. Elected officials handle oversight and resource allocation. A clerk, treasurer, administrator, or designated “cyber liaison” coordinates with IT vendors or county IT. Technical tasks (patching, account setup, backups) are usually performed by a vendor or shared service provider., The municipality, not the vendor, retains final accountability for decisions before, during, and after an incident.

What low-cost actions reduce cybersecurity risk the most?

Some of the most effective defenses are inexpensive or free:

- Enabling multifactor authentication (MFA)
- Regular software and website updates
- Removing accounts for former employees
- Using strong, unique passwords
- Keeping offline or protected backups
- Basic staff training on phishing
- Segregating public Wi-Fi from internal networks
- Reviewing vendor contracts for security requirements

These basic steps help mitigate the most common attack paths and improve overall security. However, these actions do not replace the services that a qualified IT vendor can offer.

How should we handle cybersecurity if we don’t have an IT department?

Most small municipalities rely on contracted IT providers, county IT, or shared service arrangements instead of maintaining an internal IT department. Regardless of the model, municipalities should expect their IT partners to apply updates promptly, assist with incident response, support backup processes, maintain administrator credential under municipal ownership, and notify the municipality immediately of any suspect breach. Vendors should also help segment networks, especially separating website management from internal systems, and provide lifecycle notifications for outdated hardware or software.

Municipalities without an internal IT department can still maintain effective cyber security if responsibilities are clearly assigned. A designated municipal point of contact is usually the clerk, administrator, or treasurer should coordinate communication, maintain documentation, and advisory services. Clear expectations and ongoing oversight help ensure these external partners effectively protect municipal systems.

What should we do the moment something looks wrong?

The first steps are simple and don't require IT expertise:

- Disconnect the affected device or system from the network (but don't shut the device down)
- Contact your IT vendor, or designated support person
- Suspend potentially compromised accounts
- Document what happened and when
- Notify your leadership (board, NYS, county) and follow your incident response plan

Who can help us during a cyber incident?

Municipalities can request assistance from:

- New York State Division of Homeland Security and Emergency Services (incident reporting, coordination, and technical support)
- FBI (criminal investigation and guidance)
- NYS Police (criminal investigations and guidance)
- Vendor contracted IT service
- Cybersecurity and Infrastructure Security Agency (federal cybersecurity advisors, scanning, and response support)

Having these contacts printed and accessible during outages is critical to an effected cyber incident response.

Should our municipality get cyber insurance?

Cyber insurance can help cover forensic costs, system restoration, business interruption, and liability to residents after a breach. However, policies vary widely, and many include strict exclusions. Insurance should be viewed as financial protection, not as a replacement for cybersecurity practices. Premiums and deductibles have risen in recent years, so municipalities must weigh insurance costs against risk exposure. Insurers typically require baseline protections such as MFA, regular updates, secure backups, strong passwords, an incident response plan, and vendor oversight. Municipalities lacking these controls may face higher premiums or be denied coverage entirely. These requirements closely align with cybersecurity best practices, so meeting them strengthens the municipality overall.

Why is bringing your own device (BYOD) a concern for municipalities?

Many small municipalities rely heavily on personal devices because they often do not provide laptops, or work cell phones. While practical, this introduces major security risks. National

breach data shows that nearly half of compromised logins used in cyber incidents were stored on personal, unmanaged devices, including personal phones, and home computers. Attackers understand that these devices often lack updates, antivirus protection, and proper configuration, making them the easiest entry point into municipal networks. Municipal email, financial records, shared drives, and even water system alerts are often accessed from personal devices. If even one of these devices are compromised, the attacker can harvest login credentials, move latterly into municipal systems, or use the compromised device to impersonate officials. The risk is amplified when municipal accounts are stored in personal browsers or when personal email and municipal emails are both active on the same device.

What rules should municipalities adopt for personal devices?

Small municipalities don't need to ban BYOD, but they must set clear expectations, so officials and employees know how to protect municipal data. A simple BYOD policy can include the following requirements:

- Personal devices used for municipal work must be updated regularly, have basic security features enabled (device lock, antivirus, and automated screen lock), and must use multi-factor authentication for all municipal accounts.
- Municipal passwords may not be saved in personal browsers, and employees should use a separate app or browser profile for municipal email to prevent mix-ups and credential theft. Lost or stolen devices must be reported immediately so accounts can be secured.
- Municipal documents may not be stored in personal email or cloud apps.
- Devices accessing sensitive systems such as water/wastewater alerts, payroll, or financial transfers must be secured, updated, and free of suspicious behavior.

How can we keep cybersecurity manageable year after year?

Keep cybersecurity simple, repeatable, and integrated into routine governance. Conduct quarterly check-ins, maintain updated documentation, confirm staff training annually, and review vendor performance regularly. Build cyber incidents into emergency planning just like storms or power outages. A coordinated, consistent approach rather than large, expensive initiatives keep municipalities protected over time.

Cyber Preparedness Quick Check

This checklist is designed to help municipal leaders quickly confirm that basic cybersecurity practices are being maintained. It can be reviewed quarterly during a regular board meeting and does not require technical knowledge to use.

Municipality: _____

Date: _____

Reviewed By: _____

1. Training and Awareness

Item	Yes	No
All employees and board members have completed annual cybersecurity awareness training.	☐	☐
Staff know how to recognize phishing and report suspicious emails.	☐	☐
Employees know who to contact if systems appear compromised.	☐	☐

2. Accounts and Access

Item	Yes	No
Accounts for former employees/officials have been removed from all systems.	☐	☐
Multi-factor authentication (MFA) is enabled for email and system administrators.	☐	☐
Administrator passwords are stored securely and available if needed in an emergency.	☐	☐

3. System Updates and Maintenance

Item	Yes	No
Computer and server updates are being applied regularly.	☐	☐
Website platforms and plugins are patched and monitored.	☐	☐
Personal devices used for municipal work follow the same security expectations.	☐	☐

4. Backup and Recovery

Item	Yes	No
Backups are being made regularly.	☐	☐
Backups are stored offline or in a protected cloud location.	☐	☐
A test restore was completed successfully within the last 60 days.	☐	☐

5. Vendor and IT Support

Item	Yes	No
A designated point of contact exists for IT and cybersecurity coordination.	☐	☐
The municipality knows who to call during a cyber incident.	☐	☐
The vendor/IT agreement clearly states responsibilities for updates, security, and response.	☐	☐

6. Emergency and Public Communication

Item	Yes	No
The municipality has a cyber incident response plan, even if simple.	☐	☐
Printed copies of critical contact information exist for use during outages.	☐	☐
Staff understand who is authorized to communicate with the public if systems are disrupted.	☐	☐

If any items are marked “NO”

- Assign the task to a specific person, and
- Set a target date for completion

Plan Owner: _____

Next Review Date: _____