# Small Cities, Big Threats: Cyber Risk in Municipal Governments

Addy Moran
*Pacific Northwest National Laboratory Pacific*
Richland, WA
0000-0001-6922-5011

Ford Powers
*Pacific Northwest National Laboratory Pacific*
Richland, WA
0009-0005-9571-3576

Ashley Billman
*Pacific Northwest National Laboratory Pacific*
Richland, WA
0000-0003-1444-1360

Christian Perry
*Pacific Northwest National Laboratory Pacific*
Richland, WA
0009-0003-0342-1724

***Abstract*—Small town governments were once thought to be at a lower risk from cyber threat actors due to their geographical isolation and small digital footprint. The past few years has shown that to be definitively false, with several different threat actors successfully attacking local municipalities, ultimately causing disruptions to critical services, monetary loss, and privacy breaches. With the now ubiquitous presence of the internet, the reality is small city governments are at the same, if not even higher, overall risk of being attacked as large entities. For small municipalities and organizations, there may not be much opportunity to invest additional resources into cyber security due to staffing concerns and limited budgets. This paper will discuss how, while it may seem the overall risk of a cyberattack is lower because these organizations are "small fish", the probability and impact of an attack are just as high, if not higher in some circumstances, than large, high visibility organizations.**

***Keywords—small municipalities, threat analysis, cyber security, threat actors, low budget***

## I. INTRODUCTION

Cyberattacks have become a popular avenue for criminals to promote chaos, make a political stand, make an income, among other reasons. We define cybersecurity risk as the combination of the probability of an attack occurring and the resulting impact of the attack (see the Fig. 1). Cybersecurity risk is difficult to predict because there could be many different motivations and goals behind an attack[1]. While all organizations must balance this risk, small municipalities have a unique cyber risk profile, driven by the criticality of the services they are responsible for but restricted by their limited overall budgets.

It is a common occurrence to see cyber security breaches and ransomware in the news, such as the 2013 Target data breach costing the company more than $18.5 million [2] and a current ransomware attack, targeting a multi-state health care system, ultimately shutting down imaging capabilities, urgent care services, and outpatient blood draw for more than a month [3]. While those two breaches were on large organizations and are not holistically reflective of the impact on all organizations or municipalities, IBM estimates a data breach, on average, costs $4.45 million [4]. While this would be a hinderance to even the largest companies and communities, this could prove catastrophic for small communities and organizations whose yearly budget is less than $4 million. Even though smaller communities may not be as newsworthy as large ones, it does not mean their overall risk is any less. It could be argued that smaller municipalities and organizations are more likely to be the victim of a cyberattack, because an attacker can reasonably assume they have less personnel available and less defenses in place. The impact of a successful cyberattack isn't reduced either, as small municipalities need to provide emergency services, water, electricity, and other government services in the same way large municipalities do. Depending on the municipality, a cyberattack could cause even more damage. For example, it would be catastrophic if the only hospital in Nome, Alaska was attacked (the only hospital in a two hundred mile radius) and could no longer help patients (compared to the eighteen hospitals in and surrounding Los Angeles). A cyberattack could cause extreme hardship on a municipality not only immediately impacting the resident's livelihood, but could also lead to death if emergency services, clean water, or electricity were to be disturbed.

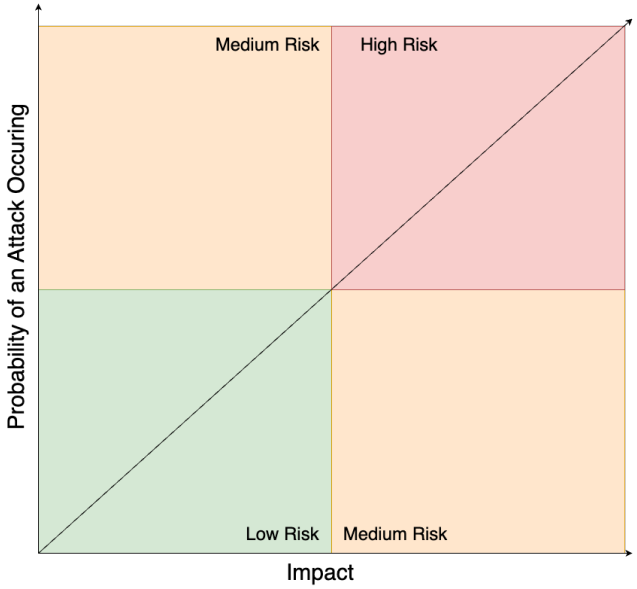


Fig. 1. Risk matrix defined by the connection between the impact of an attack and the probability of an attack happening.

## II. SMALL COMMUNITIES: HIGH RESPONSIBILITY, LOW RESOURCES

As an example, a large municipality such as New York City, New York has a population of 8.335 million people as of July 2022 [6] and a yearly budget of $107 billion [7]. A small city in New York[2] has a population of approximately 1,000 people and an annual budget of $4.1 million. That's about 0.11% of New York City's population and about 0.004% of their budget. Both municipalities must provide life-supporting services such as emergency services and crime support, water and other utilities, road maintenance and public transportation. If an attacker chose to attack New York City's government systems, they could impact millions of people, 8,335x more people than attacking the smaller city. However, the attackers would be battling against the New York City's Office of Technology & Innovation (OTI)[3] which boasts 24/7 cybersecurity monitoring and a partnership with over one hundred agencies. Comparatively, the smaller town has no mention of cybersecurity on their website. While New York City has many more people relying on the government's infrastructure, if there was no heat to the one thousand residents and tourists in a New York winter, a thousand people potentially dying is still too many. Due to the increasing frequency of attacks on small municipalities, the FBI released the following Private Industry Notification (PIN) on March 30th, 2022:

> The FBI is informing Government Facilities Sector (GFS) partners of cyber actors conducting ransomware attacks on local government agencies that have resulted in disrupted operational services, risks to public safety, and financial losses. Ransomware attacks against local government entities and the subsequent impacts are especially significant due to the public's dependency on critical utilities, emergency services, educational facilities, and other services overseen by local governments, making them attractive targets for cyber criminals. Victim incident reporting to the FBI between January and December 2021 indicated local government entities within the GFS were the second highest victimized group behind academia [5].

### A. Threat Landscape

There are endless possible attack vectors that could be used to gain access to a small municipality's infrastructure. Some common entry points to a small municipality's system are: exploiting unpatched hardware or software, cracking insecure passwords, spear phishing, and gaining physical access to the facilities. These initial entry points could potentially lead to an attacker deploying a form of malware or ransomware (for financial gain or to promote chaos), releasing and selling sensitive information on the government and residents, and many other malicious actions. Based on the infrastructure, the impact of these attacks can be exacerbated due to lack of network segmentation (a.k.a "flat networks") and lack of affordable tools and trained personnel. See Appendix Table I for a detailed view of the potential threats, consequences, and potential mitigation strategies.

*1) Initial Entry Points:* Malware[4] can be very damaging to an infrastructure, often leaving data unreachable and resources unavailable. There are many ways malware could be deployed on a system; cracking insecure passwords, exploiting unpatched hardware or software, gaining access to a physical location, and spear phishing being some of them.

If cyber security has not been on the forefront of a municipality's discussions and decisions and the importance not emphasized to their employees, many avoidable gaps could be exploited. Such as proper password security. If passwords are not changed on a recurring basis or they are not of a secure complexity, an attacker could easily crack the password of an employee and gain access into the infrastructure.

Another opportunity an attacker may utilize to gain access to the system is exploiting unpatched hardware or software. Due to small budgets and many priorities, it is often easy to decide not to upgrade hardware or software if it still works. However, depending on the age of the hardware or software and the manufacturer, those devices may reach their End-of-Life (EOL) and the manufacturers may stop releasing security patches. These vulnerabilities are relatively easy for an actor to find using tools like Exploit-DB[5], where it will scan a system and provide the attacker with a list of exploitable vulnerabilities/CVEs[6] based on the manufacturer and firmware/software version.

Due to the nature of small municipalities, many facilities operated by the small municipality have public access (i.e. court house, in-person utility payment services). If a malicious actor visited one of these buildings there is often an opportunity to join the WiFi[7] or to use a tool like a Rubber Ducky[8] on a public computer or a computer at the front desk, which could create a reverse shell or pull sensitive files.

Phishing "is a form of social engineering that uses email or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity" [16]. Spear phishing is a type of phishing that targets an individual using key information about them (or their organization) [16]. According to the Swiss Cyber Institute "95% of all attacks on enterprise networks are the result of successful spear phishing" [9]. Due to government regulations and policy, some information must be published such as elected officials, working hours, operating sites, services provided, and budget and financial information. In addition, social media has become a prominent tool in politics, making it easy to find in-depth information on officials through their personal websites, social media accounts, and election campaign material. This information on the government entity and elected officials, makes a spear phishing campaign more likely to be successful because the attackers can make the emails very detailed and accurate.

After the initial entry to the network, one of the most common attacks used against municipalities and organizations (regardless of size) is ransomware. Ransomware is defined by CISA as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then

demand ransom in exchange for decryption" [11]. Ransomware used against a municipality could shut down the emergency services or utilities (water, electricity), could encrypt hospital records, or could freeze financial transactions. The attacker would require a payment before giving access back, often threatening to permanently delete or lock the files or systems if a payment is not received in a certain amount of time. Since municipalities and government entities are often required to release operating budgets and expenditures to the public, this information helps a malicious actor make an educated ransomware payout value, increasing the likelihood of payment.

2) Exacerbating Factors: There are certain factors that are particularly common in small municipalities or organizations that either make a cyber attack more likely to be successful or to be more harmful. Specifically having a "flat network" and a lack of funding for tools, dedicated cyber staff, and recurring training.

Small municipalities manage several systems and sub-systems for their local populace, and while these might be separate networks, if they don't, a threat actor could utilize the connections local government systems have to extract greater impact against the community. An example of this would be traditional Operational Technology (OT) systems, like water utilities and power distribution. Depending on the expertise of the staff, time available for setup, and the initial infrastructure decisions, it is not uncommon to see the OT network alongside the IT network. This type of network is considered "flat" because there is no segmentation of services. While this is a straightforward, easy-to-implement and maintainable solution, it introduces the risk that if an attacker gained access to the IT network it could immediately manipulate the OT network (or vice versa). This would allow an attacker to be very destructive to numerous networks in a very short amount of time.

Of the state-of-the-art tools used in cyber security, Splunk is one of the most popular Security Information and Event Management (SIEM) tools, used by companies like Papa John's, REI Co-Op, Puma, and Nasdaq. At the time of this writing, licenses start at $1,500 per GB per year. Based on an anonymized small municipality which has around 10 GB of traffic per day, Splunk monitoring would cost around $5,475,000 per year. This municipality has an annual total revenue of just over $4.4 million. This does not include any labor or hardware cost for running a Security Operations Center (SOC), let alone any of the other expenses the municipality requires to run (like utilities, public safety services). This prohibitively high expense severely limits small communities the opportunity to use Splunk and many other commercial-of-the-shelf (COTS) tools that increase network monitoring and overall security. While there are either free or more cost effective tools similar to Splunk (like the Elastic Stack[9]) there is usually a trade off between the up-front cost of the tool and the hardware and labor cost to setup and maintain these tools, making the decision non-trivial [8].

Due, in part, to the shortage of cyber security personnel in the industry, even the municipalities with available budget for security staff are finding it difficult to compete against the private industry. Not only do they need to offer competitive pay and benefits, many of these municipalities are in remote areas, forcing potential employees to either commute or relocate, compounding the problem when trying to acquire and keep well trained cyber personnel. This often leads to the current reality, where employees must wear multiple "hats". These employees are often responsible for multiple domains, for example, one staff may be in charge of both the IT/tech support and the cyber security across the organization. This could also look like one part time staff dedicated to maintaining a system and another part time staff dedicated to maintaining another. Staff being spread thin like this makes it difficult to prioritize security on all the systems the organization manages. This potentially leads to a cyberattack getting found very late (if ever).

For similar budget reasons, small municipalities struggle to find resources to train their staff (especially the staff that are in non-technical roles) on security best practices, such as how to identify a phishing email and good password and system hygiene. The lack of training opportunities and quality resources increases the likelihood of successful attack campaigns, and subsequently, increases the likelihood of a successful compromise. It has been found that "97% of users cannot identify a sophisticated phishing email" [9] and that investing in the employees' training "reduces the likelihood of cyber-incidents occurrence" [13].

### *B. The Consequences of a Breach*

Regardless of how an attacker gained access to an infrastructure, the consequences would directly impact the livelihood of their residents. This includes privacy concerns (HIPAA/PII information, credit card information from utility payments), physical safety concerns (loss of emergency services, decreased security at prisons), and health safety concerns (no electricity, unsafe or no water). In 2021, the Centre for Counter Fraud Studies and Cybercrime Awareness Clinic explored the impacts of Computer Misuse Act offenses in the United Kingdom which included testimonies from the victims on their financial, health, psychological and emotional states after the attack. They found the impact from being very minor for some individuals, to very severe for others, some comparing their experience to rape. Some of the victims said they "felt powerless, angry, violated in a way, very angry and angry" and that "Yes, there [are] more important things than money, but there's all different feelings that go into it, from the isolation, from the betrayal, from hopelessness" [14].

Direct examples of cyberattacks and the consequences on the municipalities were included in the FBI PIN [5] mentioned above, specifically:

- In January 2022, a ransomware attack disabled county jail surveillance cameras, deactivated automated doors, among other things, forcing the county to shut down the systems and close public offices for a period of time.

- In January of 2021, a ransomware attack stole data on the election, financial information, jail management files, dispatch, and assessment files.

911 call dispatch and emergency response systems are typically managed by Emergency Communication Centers (ECCs) or Public Safety Answering Points (PSAPs). ECCs serve as the first point of contact for individuals in need of emergency services, including police, fire, and medical assistance. ECCs rely on local government networks for various functions, including call routing, database access, and communication with first responders. These systems are often integrated into the broader municipal network infrastructure to ensure operations. In the event of a network breach this system could be degraded or disrupted, affecting emergency communications.

Local government data has lots of opportunity for privacy violations. For example, if the 911 dispatch/emergency response systems were infiltrated, Personal Identifiable Information (PII) and Health Insurance Portability and Accountability Act (HIPAA) records may become available. In 2016 Banner Health was victim to a data breach that disclosed protected health information for 2.81 million consumers. The data breach specifically resulted in the following HIPAA violations: "the lack of an analysis to determine risks and vulnerabilities to electronic protected health information across the organization, insufficient monitoring of its health information systems' activity to protect against a cyber-attack, failure to implement an authentication process to safeguard its electronic protected health information, and failure to have security measures in place to protect electronic protected health information from unauthorized access when it was being transmitted electronically". As a result of these violations, Banner Health paid $1.25 million dollars to the impacted [10]. Another potential privacy concern is if the sheriff or background check database[10] gets infiltrated and modified, potentially leading to the creation of arrest warrants of innocent residents or removing arrest warrants for criminals. Even if the local government doesn't host the background check server within it's network, a threat actor could abuse permissions within the network to make queries against and get access to the database.

If an attacker wanted to promote panic, desperation, or cause injury and death, they could manipulate traffic lights or traffic monitoring systems to increase vehicle wrecks or disrupt first responder services. As mentioned, disruption to utility services could also prove deadly, especially if air conditioning (AC) was unavailable in Texas in the summer, if heat was unavailable in Montana in the winter, or if the water treatment plants were disabled, making the water unsafe to drink or unavailable all together.

### C. Caveats

This paper is based on an anonymized organization and the risks described are not guaranteed to apply to all small municipalities nor is it a comprehensive representation of the risks a small municipality may face. For example, one additional risk not applicable to the anonymized organization used for the core of this paper, is public gun ownership records. The State of California maintains a database that "contains information on individuals who have purchased or transferred firearms legally and all known firearms associated with each individual"[11]. While not specifically applicable to small municipalities, depending on how the state-wide database is maintained and updated in each municipality, there may be the opportunity to maliciously modify the database to either remove records from the list or change someone's status to be "prohibited" and therefore having the guns removed from their possession. Another example of a variation to the potential risk analysis is from the power grid perspective. Depending on the municipality, the power grid may be managed by the city, county, state, or privately, which may increase or decrease a municipality's risk.

## III. CONCLUSION

While it may seem that small municipalities may not be noticed by a malicious actor, that does not mean their risk is less. Due to smaller budgets, it is harder to defend (due to cost of tools, resources, and personnel) and the impact on both the residents and the government entity itself is the same as a large municipality or organization. It is of utmost importance that these municipalities receive the support they need, through funding, education, and opportunities to better protect their livelihood. This paper provides an overview of potential attack vectors and the consequences of such but does not discuss how to help protect these communities, specifically in the argument of how to get more funding. An article posted by CSO Online provides a viewpoint on how some municipal CISO's have navigated this issue [17] and the "What Credit Unions Must Know to Combat Cyberattacks in 2022" paper published in the Credit Union Management journal is a good resource to learn ways to better secure small organizations [18].

## REFERENCES

[1] Steven Wertheim. (2019, December). "The Willingness Not to Believe". The CPA Journal, vol. 89:12, pp. 86+, link.gale.com/apps/doc/A611548130/GBIB?u=pnnl&sid=bookmark-GBIB&xid=29a6a0f0 (retrieved 11 September 2023).

[2] Reuters. (2017, May 24). "Target Settles 2013 Hacked Customer Data Breach For $18.5 Million". Reuters. https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031 (retrieved 6 September 2023).

[3] Rebecca Carballo. (2023, August 5). "Ransomware Attack Disrupts Health Care Services in at Least Three States". The New York Times. https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html (retrieved 30 August 2023).

[4] IBM. (2023). "Cost of a Data Breach Report 2023". IBM. https://www.ibm.com/reports/data-breach (retrieved 30 August 2023).

[5] FBI. (2022, March 30). "Ransomware Attacks Straining Local US Governments and Public Services". Department of Justice Federal Bureau of Investigation. https://www.ic3.gov/Media/News/2022/220330.pdf (retrieved 30 August 2023).

[6] U.S. Census Bureau. (n.d.). "QuickFacts: New York city, New York". Census.gov.

https://www.census.gov/quickfacts/fact/table/newyorkcitynewyork/PST045222 (retrieved 6 September 2023).

[7] New York City Council. (n.d.). "The City Budget". nyc.gov. https://council.nyc.gov/budget/ (retrieved 6 September 2023).

[8] Pearl Kim. (2020, June 24). "3 Things to Consider About COTS vs. Open Source Software". GovLoop. https://www.govloop.com/3-things-to-consider-about-cots-vs-open-source-software/ (retrieved 6 September 2023).

[9] Swiss Cyber Institute. (2021, September 1). "27 Phishing Attack Statistics You Probably Didn't Know". Swiss Cyber Institute. https://swisscyberinstitute.com/blog/cybersecurity-facts-phishing-statistics/ (retrieved 7 September 2023).

[10] U.S. Department of Health and Human Services. (2023, February 2). "HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking". hhs.gov. https://www.hhs.gov/about/news/2023/02/02/hhs-office-for-civil-rights-settles-hipaa-investigation-with-arizona-hospital-system.html (retrieved 6 September 2023).

[11] CISA (n.d.). "Stop Ransomware". CISA. https://www.cisa.gov/stopransomware (retrieved 10 September 2023).

[12] CISA (n.d.). "Malware Tip Card". CISA. https://www.cisa.gov/sites/default/files/publications/Malware_1.pdf (retrieved 11 September 2023).

[13] Mattia Caldarulo, Eric W. Welch, Mary K. Feeney. (2022). "Determinants of cyber-incidents among small and medium US cities". Government Information Quarterly, vol: 39:3, DOI: 10.1016/j.giq.2022.101703. Available: https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000363 (retrieved 11 September 2023).

[14] Mark Button, Dean Blackbourn, Lisa Sugiura, David Shepherd, Richard Kapend, Victoria Wang. (2021). "From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom". Telematics and Informatics vol: 64, DOI: 10.1016/j.tele.2021.101675. Available: https://www.sciencedirect.com/science/article/abs/pii/S0736585321001143 (retrieved 11 September 2023).

[15] D. W. Woods and L. Walter. (2022). "Reviewing Estimates of Cyber-crime Victimisation and Cyber Risk Likelihood". 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, pp. 150-162, DOI: 10.1109/EuroSPW55150.2022.00021 (retrieved 11 September 2023).

[16] CISA. (n.d.). "Phishing". CISA. cisa.gov/sites/default/files/publications/Phishing%20General%20Security%20Postcard_6.24.2021_508cV2.pdf (retrieved 11 September 2023).

[17] Cynthia Brumfield. (2023, March 6). "Municipal CISOs grapple with challenges as cyber threats soar". CSOOnline. https://www.csoonline.com/article/574621/municipal-cisos-grapple-with-challenges-as-cyber-threats-soar.html (retrieved 9 September 2023).

[18] F. H. Hannafan. (2021). "What Credit Unions Must Know to Combat Cyberattacks in 2022," Credit Union Management, vol. 44:12, pp. 14-17. Available: https://www.proquest.com/trade-journals/what-credit-unions-must-know-combat-cyberattacks/docview/2601608656/se-2 (retrieved 11 September 2023).

## Notes

1. There has been significant research invested in determining a repeatable process to estimate the likelihood of the cyber risk [15].
2. The city name was intentionally excluded to prevent any unintentional damage.
3. https://www.nyc.gov/content/oti/pages/cybersecurity
4. CISA defines malware as "short for 'malicious software,' includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data" [12].
5. https://www.kali.org/tools/exploitdb/
6. https://cve.mitre.org/
7. Some municipalities have a separate public wifi, but some don't, allowing the attacker immediately access to the network.
8. https://shop.hak5.org/products/usb-rubber-ducky
9. https://www.elastic.co/elastic-stack
10. A collection of arrest records shared amongst small city governments and the law enforcement system and is subject to the Criminal Justice Information Services (CJIS) Security Policy.
11. https://oag.ca.gov/ogvp/apps-database

# APPENDIX

TABLE I. THREAT ANALYSIS OF SMALL MUNICIPALITIES

| **Threat to Small Municipality** | **Explanation** | **Consequences** | **Potential Mitigation Strategies** |
|---|---|---|---|
| Ransomware Attack | Published budgets can allow an attacker to make an educated ransomware payout value, increasing the likelihood of success. | Loss of access to data or systems, potentially resulting in loss of life (if system was core utility or emergency services), financial loss (if ransomware is paid) | Backup of data and emergency systems, allowing a replacement system to be used in case of system failure or lock out. |
| Spear Phishing Attack | Published information on websites and social media can lead to a more successful spear phishing attack. Lack of training may also contribute to a successful attack, specifically if employees don't understand what to look for and the consequences. | Allows access into the IT network, if the infrastructure is "flat" could lead to more harmful consequences such as pivoting from the IT network to the OT network and disabling services. | Enforce mandatory (and recurring) training (can look to free resources/training material). |
| Lack of Password Hygiene | If good password hygiene (frequent password changes, password complexity/length requirements) is not mandated, it could allow an attacker to crack the password on any number of systems. Potentially to service accounts or people of high access (i.e. a mayor). | Loss of access to data or systems (if the attacker locks the accounts), financial loss (if the attacker threatens access or data leaks unless paid), loss of life (if the attacker disrupts critical services such as emergency management services, water filtration system, electricity) | Develop and enforce mandatory password changes and password complexity requirements. |
| Outdated Software/Hardware | If municipalities can't afford to upgrade software or hardware and they reach their end of life (EOL), there may not be patches available, leaving critical gaps easily found by attackers. | Attacker getting access to system, and if the system was "flat", potentially pivoting between the IT and OT networks. | Make upgrading software and hardware a priority during budget discussions. |
| Network Access through Physical Facility | Most municipalities have physical locations (for the resident's to pay bills, get resources, etc.) many of these facilities often have WiFi available and public computers. | An attacker may get a direct connection into the network with critical infrastructure/information, allowing them to deploy malware, gain access to sensitive files, etc. | Utilize a separate public WiFi with a wired-only internet connection or password-protected WiFi for employees and critical systems. Disable USB support on systems. |
| Supply Chain Attacks | Between staffing shortages, cost of labor and tools/services, hiring 3rd party companies is common. | While a cyber attack to the 3rd party organization is often not preventable, the impact could be just as severe as if the attack was on the municipality itself. | Invest in a repeatable process to investigate 3rd party companies/vendors and appropriately determine and decide if the risk is acceptable before integrating into the infrastructure. |