Palindrome Technologies

ASSURANCE | TRUST | CONFIDENCE

# Municipal Cybersecurity Risks, Challenges and Best Practices

Palindrome Technologies
100 Village Ct, Suite 300
Hazlet, NJ 07730
Tel: 844-429-2792 (844-4-CYBRWAR)
www.palindrometech.com

# Introduction

Municipalities face a wide range of cybersecurity threats against operational, financial and control systems. This challenging environment is further complicated by budget realities commonly faced by municipal institutions that can result in inadequate spending levels on technologies, personnel, and process formalization. Cyber risks therefore present substantial exposure to municipal organizations.

## *Threats*

Prevailing threats to municipalities include the vast array of threats faced by all internet-connected enterprise organizations, but also industry-specific concerns. Municipalities are therefore required to perform tech-industry standard activities to identify, control, and monitor cyber risks, but to also continuously monitor the threat landscape. While cyber-adversaries historically attacked targets of opportunities, today's attackers are more sophisticated including state sponsored actors who choose targets based on perceived value of information or computing resources that may be gained via successful breach. It is also reasonable to expect that budget-starved public organizations may be expected to lag with respect to technology adoption (therefore resulting in antiquated architecture) as well as personnel (possibly causing inadequate monitoring and maintenance).

Information on general cybersecurity threats abounds, in large part due to regulatory and industry resources and guidance, as well as a relatively robust environment for cybersecurity tools. The challenge for municipalities however is harnessing the available resources and acting upon threat information, which as mentioned may be made difficult as a result of historically low IT and cybersecurity staffing levels and budgetary constraints.

Threat and vulnerability data collected (for 4 weeks) from a cyber security study on 11 municipal networks conducted by Palindrome in 2018 revealed that, as organizations grow overtime so does their IT budget but the organization also becomes more vulnerable due to a lack of investment in Cyber Security resources.


100 Village Ct, Suite 300, Hazlet NJ 07730
Tel: **844-429-2792** (844-4-CYBRWAR)
www.palindrometech.com

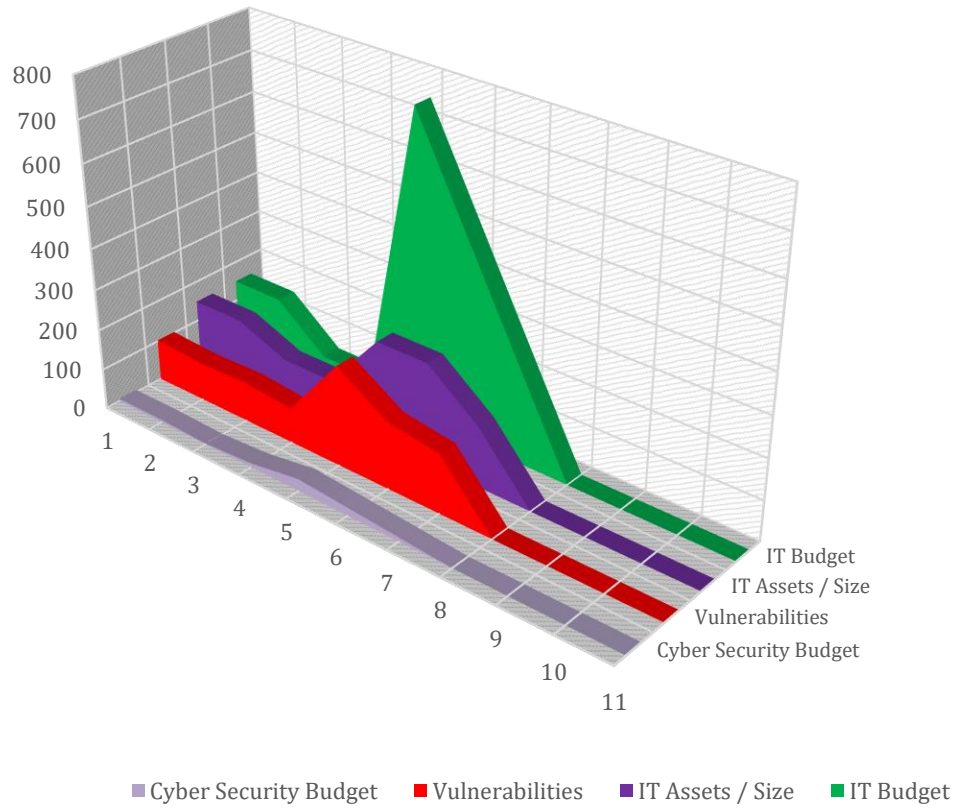


*Figure 1 Cyber Security Budget Investment and Susceptibility to attack*

Municipal-specific concerns may present the greater challenge. Information resources may actually have higher value to some attackers than traditional financial and customer information records. For example, information gathered and stored by law enforcement and judiciaries should be expected to be highly sensitive, particularly data related to criminal prosecutions that are subject to individual privacy concerns as well as confidentiality such as related to eyewitness testimony. High profile cases may draw in sophisticated, global threat actors. Threats may potentially seek to impact confidentiality, integrity (e.g. attackers modifying municipal data), and availability (e.g. attackers delete or ransom municipal data).

During the aforementioned cyber security study, participating municipalities revealed that the four major security concerns are phishing attacks, ransomware, lack of incident response plan and employees visiting inappropriate sites.


100 Village Ct, Suite 300, Hazlet NJ 07730
Tel: **844-429-2792** (844-4-CYBRWAR)
www.palindrometech.com

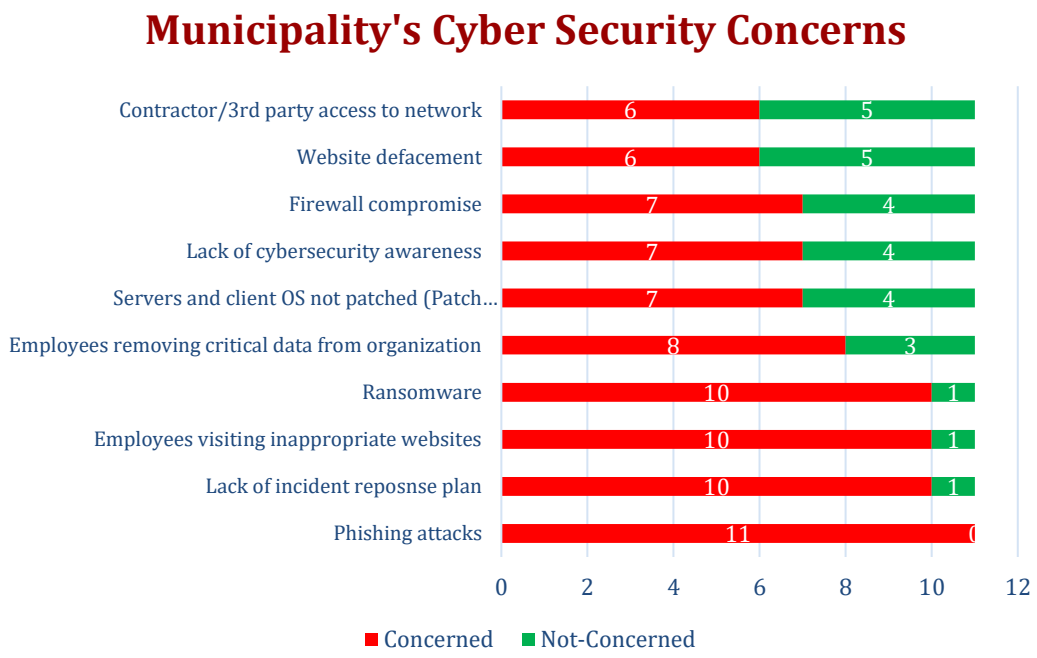


*Figure 2 Municipality's Cyber Security Concerns*

Furthermore, only 45% of the participants had an Information Security Program in place.

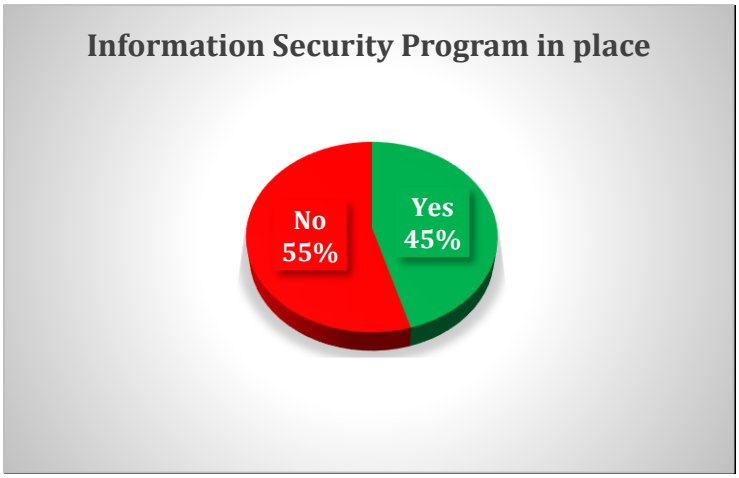


*Figure 3 Information Security Program Active Implementation*

## *Vulnerabilities*

The vulnerability profile for municipalities should be expected to lag that of other industries due to budget and personnel limitations as mentioned previously.


100 Village Ct, Suite 300, Hazlet NJ 07730
Tel: **844-429-2792** (844-4-CYBRWAR)
www.palindrometech.com

However, the combination of funding issues with staff or skill shortages magnifies vulnerability concerns. Budget pressures may force municipal enterprises to use outdated hardware and software longer than desired, perhaps even past the point when vendors drop support for older versions. It should be anticipated that all or most municipal organizations will be under some form of pressure to squeeze every bit of useful life out of technology before it can be replaced.

Vulnerabilities may also be created by a failure to successfully install and configure technologies the municipality actually is able to purchase. For example, as noted in the 2016 San Bernardino shooting, "the county government that owned the iPhone in a high-profile legal battle between Apple Inc. and the Justice Department paid for but never installed a feature that would have allowed the FBI to easily and immediately unlock the phone as part of the terrorism investigation…"[1] Therefore it is important to consider vulnerabilities beyond the simple observation of missing or outdated technology, but towards full enterprise capabilities.

Municipalities may also operate SCADA environments. An industry-wide unfamiliarity with industrial control systems can cause enterprises to avoid or simply be unprepared to observe and respond to SCADA risks. The answer of course is investment in appropriate skills and expertise as well as application of prevailing cyber standards, such as the NIST Cybersecurity Framework (CSF). The unfamiliarity of much of the tech industry with SCADA is in and of itself a vulnerability.

During the 2018 Cyber Security study the threat and vulnerability data collected revealed that overall, municipal networks that were evaluated maintain some security controls to prevent attacks against their IT assets but further improvements are encouraged.

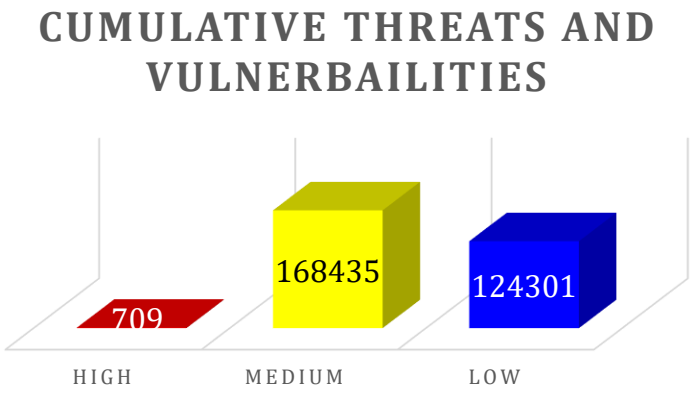


*Figure 4 Threats and Vulnerabilities data collected for 4 weeks*

[1] https://www.cbsnews.com/news/common-software-would-have-unlocked-san-bernardino-shooters-iphone/


100 Village Ct, Suite 300, Hazlet NJ 07730
Tel: **844-429-2792** (844-4-CYBRWAR)
www.palindrometech.com

To further enhance the security profile of the Municipal networks the following are recommended:

a) Establishment of an Information Security Program; Based on the data collected, 55% of Municipalities are concerned that an Information Security program is not in place.
b) Mitigate the identified vulnerabilities and ensure that systems are updated on a consistent schedule for operating system patches and other software updates.
c) Ensure that Network Security monitoring (i.e., network traffic, critical system logs) is implemented to align with government requirements and best industry practices.
d) Evaluate the use of network sharing applications (i.e., Dropbox) for sensitive data such as payroll and medical.
e) Consider instituting a robust vulnerability management process as part of the Municipal Cyber Security program

In this study, a threat constitutes an actor (external or internal) who engages in malicious activity such as network reconnaissance, credential harvesting, brute-force password attempts, phishing attacks or exploitation of a vulnerability (i.e., buffer overflow, SQL injection) to gain unauthorized access to a system or data. A vulnerability is a weakness that can be exploited by an attacker in order to gain unauthorized access to a system or data and may include, but not limited to, poor configuration (e.g., default account passwords, unnecessary services, outdated software), buffer overflows, SQL injection, Cross-Site Scripting among others.

## *Consequences*

The impact of cybersecurity incidents on municipalities can be profound, including substantial disruption to business as usual as well as very large financial losses. The 2018 malware incident experienced by the City of Allentown, Pennsylvania resulted in almost $1,000,000 in recovery costs.[2] Also in 2018, a ransomware attack against the Colorado Department of Transportation caused the department to pay Microsoft $185,000 for cyber response. [3] Loses stem not only from any ransom paid or professional response needed, but also the inability to send bills and tax notices. In August 2019, the city of Baltimore was sending out the first water bills since the attack on its systems in May and is facing an estimated 18 million in direct

[2] https://www.mcall.com/news/breaking/mc-nws-allentown-computer-virus-20180220-story.html
[3] https://www.scmagazine.com/home/security-news/government-and-defense/colorado-dot-allentown-pa-in-recovery-mode-after-costly-cyberattacks/


100 Village Ct, Suite 300, Hazlet NJ 07730
Tel: **844-429-2792** (844-4-CYBRWAR)
www.palindrometech.com

costs and lost revenue.[4] Study after study demonstrates the sophistication of adversaries in increasing as are the costs of protection, response, and recovery for enterprises.

## Best Practices

Just as NIST CSF and other industry guidance is available to municipalities, so are a wide range of technical and non-technical best practices that can improve the monitoring of threats, identification of vulnerabilities, design of adequate control strategies, and testing/validation techniques. Like in all industries, there is a base of knowledge municipalities can benchmark against and, as a result, address many cybersecurity concerns that can be directly applied by the respective enterprise. This includes best practices related to the following;

- Technology maintenance
- Software patching for operating systems and patches
- Well-designed and maintained network perimeter security
- Recurring penetration testing and vulnerability analysis
- Performance of cyber response drills
- Periodic risk assessments over information and systems
- Appropriate oversight of third-party service providers
- Employee awareness of cyber risks in areas such as sending sensitive data in unencrypted e-mail, e-mail phishing, sharing USB drives, and the use of public-cloud solutions for document sharing

More challenging, however, is recognition of risks unique to the enterprise that can stem from the nature of core processes, data confidentiality and sensitivity, and ongoing challenges in maintaining updated architecture. Challenges like these may need to be confronted using specialized technologies and perhaps external expertise.

## Conclusions

Municipal organizations face the cybersecurity threats that apply to all enterprises, but are presented with additional challenges with respect to budget and staffing that may cause considerable increases in exposure. General industry standards and guidance on cybersecurity can be applied, with special attention needed to ensure highly efficient budget processes, careful cybersecurity spending decisions, ongoing support of IT and cyber staff, and reliance on trusted external partners to help fill the gaps.

[4] https://arstechnica.com/information-technology/2019/08/ransomware-strike-takes-down-23-texas-local-government-agencies/


100 Village Ct, Suite 300, Hazlet NJ 07730
Tel: **844-429-2792** (844-4-CYBRWAR)
www.palindrometech.com

For more information please contact us:

**Peter Thermos**
100 Village Ct, Suite 300
Hazlet, NJ 07730
Email: peter.thermos@palindrometech.com
Tel: 844-429-2792 (844-4-CYBRWAR)
**www.palindrometech.com**