Table Of Contents

Section I

Introduction

City managers (and their deputy managers) have a lot to worry about when it comes to cybersecurity. In the face of ransomware, phishing attacks, and other cyber threats, municipal systems are considered, by some, to be "soft targets."

As a city manager or deputy manager, it may be up to you to put the right cybersecurity tools in place to protect your city's systems from attack. However, before you can optimize your municipality's cybersecurity architecture, it's important to know more about the threats that it faces.

Of the various cyber threats that target municipal and state organizations, ransomware continues to be one of the most pervasive and damaging. For example, according to a report by CNN, "Riviera Beach officials voted to pay their requested ransom of 65 bitcoin, close to $600,000, to hackers who disables the city's online services in late May." However, it isn't the ransom money that is proving damaging to municipalities—it's the disruption caused by a sudden loss of access to key information systems.

As noted in the CNN report, "Complete recovery of a city's systems can take up to several weeks and cost cities millions more than the agreed ransom – a combined cyberattack on Atlanta and Newark cost more than $30 million in damages."

> *"In the face of ransomware, phishing attacks, and other cyber threats, municipal systems are considered, by some, to be "soft targets."*

Section 4

How Much Should Your Municipality be Spending on Cybersecurity?

If budgets are a constraining factor on cybersecurity, then isn't spending more on network security crucial for preventing ransomware attacks and other cyber threats from damaging the municipality?

The answer is "yes and no" at the same time.

> ***....cybersecurity is not a device, and blindly adding new tools can waste money without producing comparable results.***

While pouring more money into a city or county cybersecurity budget can make it easier to acquire new cybersecurity tools and to beef up security staffing, simply throwing money at the problem doesn't guarantee an effective solution. After all, while a strong network security strategy might use various cybersecurity tools, cybersecurity is not a device, and blindly adding new tools can waste money without producing comparable results.

Section 5

Which Cybersecurity Tools Should I Invest in?

When it comes to prioritizing cybersecurity solutions for a municipal government setting, the advice for how to choose the right tools is not too different from what it would be for a midsized business:

> ***Investigate what your biggest cybersecurity threats and vulnerabilities are and start there!***

This often requires an asset audit, risk assessment, and vulnerability assessment to properly identify both security vulnerabilities and the types of attackers your municipality will face. After running these assessments and creating a comprehensive report that ranks your vulnerabilities according to likelihood of occurrence and level of potential impact, you should be able to effectively prioritize the security tools that will provide the biggest return on investment for your budget expenditures.

> ***"... setting up extra protections to prevent malware from being uploaded to your network's assets and creating a remote data backup of your mission-critical files and resources would be a high priority"***