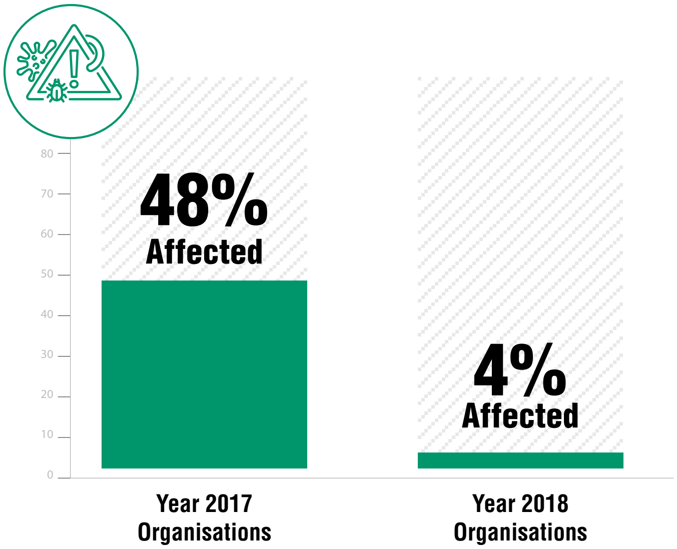
Section 3

Why are Municipalities Being Targeted?

While ransomware attacks on municipalities have earned a fair number of headlines in 2019, the truth is that ransomware attacks are on the decline overall. As noted by [Computer Weekly:]



> *While ransomware dominated the malware landscape in 2017, affecting around 48% of organisations at the height of its popularity, the Check Point researchers said the past year saw a sharp decline in the use of ransomware, with only 4% of the world's organisations affected by ransomware attacks in 2018.*

If ransomware attacks have dropped off so much, why are municipalities being targeted so heavily by them?

In the USA Today article, Lee McKnight, a cybersecurity expert and associate professor at Syracuse University's School of Information, posited a potential explanation. According to professor McKnight, "It happens again and again to municipal systems that don't have all the latest software, the latest protections or the highest-paid IT staffs." Many municipalities have to operate on a tight budget, restricting their options in the face of cyberattacks.

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.

How Much Should Your Municipality be Spending on Cybersecurity?

So, when asking, "How much should my municipality be spending on cybersecurity?" it can help to consider:

Your Overall Operational Budget

How much room is in the budget to accommodate new cybersecurity spending in the first place? It's important to nail down this detail before creating grand plans to update and upgrade every asset on the network with the latest and greatest solutions.

Your Municipality's Network Assets

What assets are on your network, how many authorized users do you have, and what level of access does each person need? Answering these questions can help you better plan your cybersecurity budget.

What Assets and Information are Mission Critical?

Of the assets on your network, which ones absolutely need to function at all times, and what would the impacts be for their loss? Knowing this can prove to be especially crucial for optimizing your cybersecurity strategy and picking the best tools to meet your needs.

What are My Single Points of Failure?

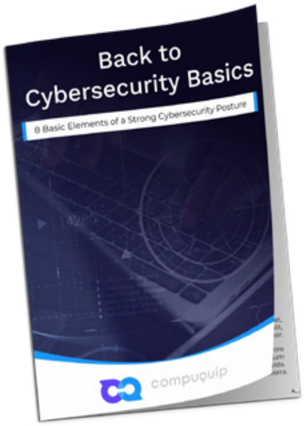
Are there any assets on the network that, if they failed, would bring your municipal operations to a grinding halt? If so, creating backup systems that can take over for these assets when they fail is a must. This is a key part of your disaster recovery planning.

Taking all of these into account can be crucial for creating a comprehensive budget for your city or county's cybersecurity needs.

Are You Ready to Partner with an MSSP Who Cares about Your Needs?

You can reach out to our Chief Information Security Officer (CISO), Michel Ramirez today to learn more about Compuquip and how to perfect your cybersecurity strategy. Or, you can contact us at:

CONTACT US TODAY



Back to Cybersecurity Basics

8 Basic Elements of a Strong Cybersecurity Posture

compuquip

Back to Cybersecurity Basics

8 Basic Elements of a Strong Cybersecurity

Download Now

Email: info@compuquip.com

Phone: 789-641-5437

Address: 2121 Ponce De Leon Blvd. Suite 530
Coral Gables, FL 33134

Follow us on: