MUNICIPAL CYBERSECURITY: HOW TO PREPARE AS CYBERCRIMINALS GO HYPERLOCAL

By **Kevin Larson** | Senior Cyber Defense Manager of Security Intelligence

As the Department of Homeland Security recently noted, "state and local governments are rich targets for cyber adversaries and the frequency of attacks is accelerating." And yet most government entities struggle to keep up with cybersecurity's ever-changing landscape.

Last year alone the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) reported ransomware attacks against nearly all the 16 U.S. critical infrastructure sectors. Towns and cities were hit hard, too, according to several reports. Emisoft, a cybersecurity company, found that at least 77 local and state governments were hit with ransomware — a type of malicious software that can lock access to accounts, servers, and systems — in 2021.

With most states only spending about one to three percent of their overall IT budgets on cybersecurity, according to a study from Deloitte and the National Association of State CIOs, it's clear that the public sector needs to step up — and get serious about protecting information technology (IT) assets.

The good news is that towns, cities and counties have strategies they can use to mitigate the risks, according to the Cyber Readiness Institute And they don't require lots of money, staff, or technology They simply require a better understanding of how ransomware attacks occur and which policies can best protect data.

Ransomware Attacks on Municipalities

Today, however, the attacks on municipal governments continue with no end in sight. In early 2022, for example, a Florida city was hit with a ransomware attack that took down city computer systems. In August 2022 a local sheriff's system was taken down. This affected the city's ability to process criminal arrests, according to a report. These cities are not alone. A recent study found that 44 % of all ransomware attacks were against municipalities. One of the reasons, is that cybercrime is no longer limited to professional hackers or international espionage coming from China and Russia.

Most states only spend 1-3% of their overall IT budget on cybersecurity **despite at least 77 local and state governments being hit with ransomware in 2021.**

Source: Cybersecurity and Infrastructure Security Agency

Citizens™

The average cybersecurity breach costs U.S. states between **$665,000 to $40.5 million**

Source: KnowBe4, The Economic Impact of Cyberattacks on Municipalities Report

Threat actors are turning into businesspeople who are selling credit card and personal information. It's creating an environment where anyone can go buy anything online and you don't have to be a hacker with professional coding skills to be able to purchase or use a compromised credit card.

The financial cost is high, especially for governments, cities and states. According to a report from KnowBe4, a security awareness training and simulated phishing platform, ransomware alone cost U.S. government agencies about $19 billion in recovery costs and downtime in 2020. Local cities have reported millions of dollars in ransomware costs including paying ransoms, retooling systems and missed revenue.

There are other costs as well. Constituent trust suffers when cities are hacked, especially when cybercriminals threaten to release — or do release — personally identifiable information into the world. The human cost includes the time spent by employees mitigating breaches and service outages instead of working on other projects.

How to Avoid Becoming a Statistic and Protect Your Organization from Cyberthreats

Ransomware isn't the only cyber threat municipalities are facing. The Institute for Defense & Business, a nonprofit research and education institute, reported the top five threats in the public sector as being state-sponsored attacks, ransomware, phishing attacks, hacktivists, and improper usage and internal attacks. It can be difficult to protect against each of these crimes individually since there's no way to predict when and where cybercriminals will strike.

Municipalities may think that if they have antivirus and other security software in place they will be safe from cyberattacks, but this isn't the case. Sometimes, hackers can get into a system by exploiting a weak password or finding ways into a system that lacks multifactor authentication — an authentication method that asks users to provide more than one proof of identification to log in.

The key is making sure that systems, processes and people are being proactive. There's only so much that the fraud tools can do. You also need to have good

State-sponsored attacks

Ransomware

Phishing attacks

Improper usage

Internal attacks

Source: Institute for Defense and Business

processes in place. This includes common sense security measures such as making sure software is updated and patched and educating employees so they don't fall victim to phishing emails. Employees need to know that they should not click on, respond to or deal with any emails that they aren't expecting. The key is to be weary of emails that you're not expecting and report them if they seem suspicious. It is often better to ignore an unexpected email than open it and respond, as attackers will use tactics to trick the user into either opening a malicious attachment or link or providing personal information. If someone is really trying to get a hold of you, they'll figure out some other way.

Employees should also have clearly defined remote work policies so they know what they are and aren't allowed to do with work equipment and the types of networks they are allowed to connect to. Even with antivirus software installed it's easy for hackers to gain access to a system that's connected to an unsecured public Wi-Fi network. Likewise, employees shouldn't let anyone use their devices.

From an IT perspective, policies are also important. Managers should strive to hire the right talent, put regular cybersecurity training and testing on the calendar, and potentially hire outside firms to do penetration testing and employee testing to find potential vulnerabilities. Start by identifying "the crown jewels of your organization", your most vulnerable or sensitive information, and then strengthen security around that.

Everyone should also understand how easy it is for cybercriminals to gain access to systems and resources and be alert at all times. Recently, a cybercriminal intercepted a check and changed the address of payment so that when the municipality paid a monthly bill to a vendor, it went to the criminal's address instead of the rightful party. To avoid a similar situation happening to you, you first must know your customers and suppliers. You should have the right processes and education in place to be sure that your employees can confirm and verify information, especially for things like address changes.

IT staff should work with local, state, and federal law enforcement to keep up to date on the latest security issues, work with banks and other outside vendors to implement solutions that thwart hackers, and pass along all of that information to employees, vendors, and partners.

To learn more about IT security and fraud, go to Citizens Bank's fraud protection page. Keep up with technology, maintain the best technology you can, and have good internal practices. All of this can go a long way in keeping your organization safe.

Key Takeaways:

- Organizations must understand how simple it is for cybercriminals to perpetrate attacks and assume a proactive stance.
- Keep software and hardware patched and up-to-date.
- Create clearly-defined work policies and conduct cybersecurity training for employees and contractors.
- Implement solutions and services that can help you find and respond to cyberattacks.

Kevin Larson is the Senior Cyber Defense Manager of Security Intelligence at Citizens and maintains over 12 years of Intelligence and cybersecurity experience from his time in the military and private sector.

Find more articles, industry insights and interactive experiences on the latest corporate finance, risk, cash management and M&A trends at: citizensbank.com/insights

©2022 Citizens Financial Group, Inc. All rights reserved. Banking products and services are offered by Citizens Bank, N.A. Member FDIC. Securities, products and services are offered through Citizens Capital Markets, Inc., and/or JMP Securities LLC, Members FINRA, SIPC. Citizens is a brand name of Citizens Bank, N.A.