KnowBe4
Human error. Conquered.

The Economic Impact of Cyber Attacks on Municipalities

The Economic Impact of Cyber Attacks on Municipalities

Table of Contents

Cyber Attacks on Municipalities 2

The Average Financial Loss 3

Denial of Services 4

Frequency/Types of Attacks 5

Challenges of Allocating Capital to Prevent Attacks 6

The Decline of Economic Investment in Municipalities 6

Conclusion 7

CYBER ATTACKS ON MUNICIPALITIES

Cyber attacks continue to have a massive economic impact on state and local governments across the U.S. Local government institutions have become a growing soft target, and they struggle to combat the highly sophisticated attacks posed by malicious hackers. While the tools attackers use once in the victim's network are quite sophisticated, getting into the network in the first place is often done with low-tech phishing emails. The attacks have infiltrated foundational departments within the community including education, law enforcement, city operations and healthcare. Through social engineering, a single click can expose an entire database of sensitive information to the bad actors or allow bad actors to hold the entire network hostage. The result of this is often millions of dollars in financial losses, along with the theft of thousands of invaluable confidential records.

KEY FINDINGS

The data reveals that state and local governments are struggling to keep their heads above water. The weakest areas include a lack of support from top officials, "inefficient" to "no user end training at all," and "too many network/IT systems". The answer is not just to have great IT systems, but to have personnel who are trained to recognize the threats, giving the IT department support in creating a human firewall.

The research gathered reveals that phishing attacks cut deeper than just the financial burden of ransomware or a Business Email Compromise (BEC) attack. Other losses include sensitive data and information, Denial of Services (DoS), and the broken trust of citizens and stakeholders. The credibility of government institutions is jeopardized, causing even greater inflation of resources used to overcome such damaging fiscal setbacks.

The preferred method of attack against these organizations is ransomware; a vicious malware that locks users out of their devices or blocks access to files until a sum of money or ransom is paid. If defenses fail, a city could be stuck paying the cost of a ransom or losing vital information needed to provide services to the community. In 2020 alone, ransomware attacks against U.S. government organizations impacted 71 million people and carried an estimated price tag of $18.88 billion in downtime and recovery costs.

Municipalities are responsible for safeguarding sensitive information and confidential files. With such liability comes possible vulnerability. In November 2020, Delaware County, Pennsylvania, was hit with an email that triggered a ransomware event that forced them to pay a $500,000 ransom. This cost did not include the cost of downtime or the costs of remediation, which often runs into the millions of dollars.

With the increasing rates of cyber attacks on our institutions across the state and local level, a deep dive into the data revealed the massive economic impact broken down into five target areas of focus:

- The average financial loss from state and local governments
- The denial of service to citizens due to financial loss
- The frequency/types of attacks and the risk of recurring attacks
- The challenge of allocating capital to prevent attacks
- The decline of economic investment in municipalities

Publicized Ransomware Attacks By Industry

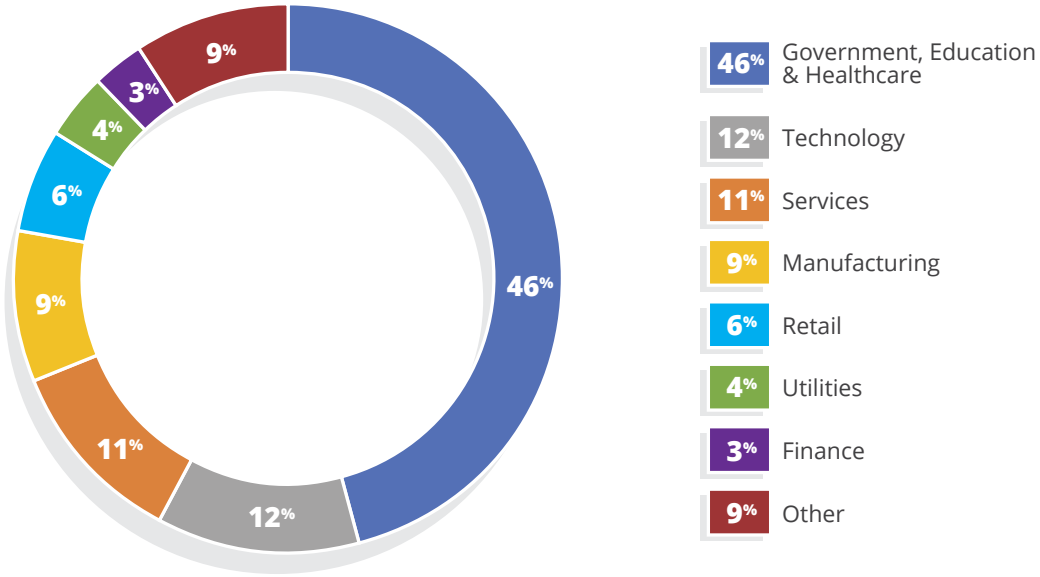


Figure 1: 2021 Publicized Ransomware Attacks by Industry

THE AVERAGE FINANCIAL LOSS

Municipalities are ideal targets for cyber criminals, as they provide many essential services to citizens. These services require a financial infrastructure that is supported largely by taxpayers and the federal government.

In 2018, Atlanta, Georgia was hit by ransomware, with the attackers demanding $55,000 in Bitcoin. The city not only faced a financial burden, but sensitive information was also put at risk. In this case, the city of Atlanta was not willing to pay the ransom. Consequently, the recovery from the attack, which was caused by simple human error, is estimated to have reached as much as $17 million.

Cities Refusing to Pay Ransom Demand Compared to the Average Recovery Cost

City, State	Demand (USD)	Recovery (USD)
Baltimore, Maryland	$76,000	$10-$18 Million
Denver, Colorado	$51,000	$1.5 Million
Atlanta, Georgia	$55,000	$17 Million
New Orleans, Louisiana	Unknown	$7-$10 Million

Once a ransomware attack occurs and a ransom is demanded, there is no escaping the fiscal costs. The city or state is left to either pay the ransom or to pay the recovery cost. In both scenarios, sensitive information will be lost, and the municipality will be compromised.

For example, in the 19 reported ransomware attacks that the state of Texas has experienced between 2016 and 2020, the attacks on hospitals alone have impacted 1,200,619 patients.

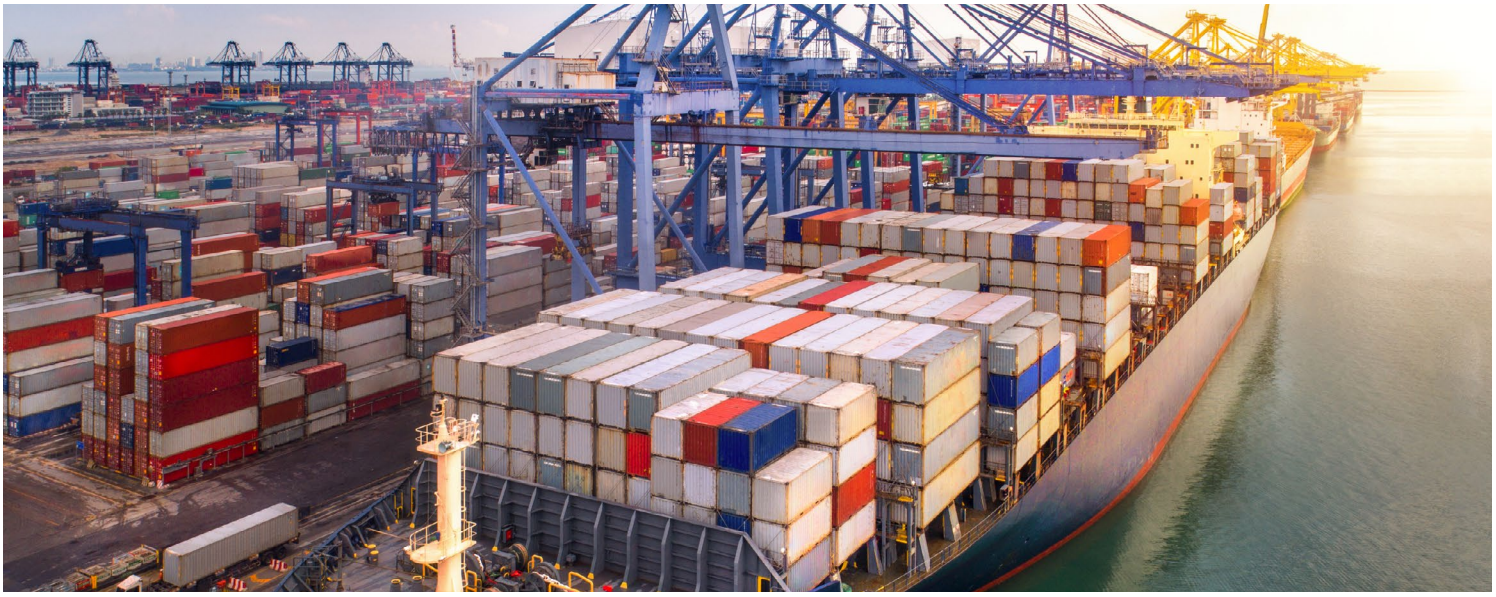
As Senator Gary Peters of Michigan (D) said, "State and local governments are responsible for safeguarding everything from election systems to an increasing amount of sensitive personal data – from social security numbers and credit card information to detailed medical records."

DENIAL OF SERVICES

Among the many types of malicious malware, hackers prefer ransomware because it locks users out of their devices or blocks access to files until a sum of money or ransom is paid. Ransomware attacks cause a Denial of Service (DoS), downtime, data loss, and possible intellectual property theft.

In addition to the direct monetary impact, the downtime caused by ransomware can be extremely disruptive. In Q3 of 2021, Coveware reported that on average, organizations face 22 days of business interruption. During this period of lockdown, the city's necessary services and vital information can no longer be accessed or operated. Examples of such services or information can include, but are not limited to:

1. Public safety (law enforcement, firefighters, hospitals)
2. Public utilities (electricity, sanitation)
3. Information services (tax services, real estate transactions, marriage licenses)
4. Maritime cargo (shipping cargo)



Maritime cargo is a critical component of the transportation of goods throughout the United States. In a report by the U.S. Coast Guard, a Ryuk ransom attack in 2019 caused significant damage to a Maritime Transportation Security Act (MTSA) facility. In order to be classified as an MTSA facility, critical assets and infrastructure must be present and identified, thus making it an ideal target for phishing attacks. The hacker(s) extracted critical files, including encrypted data containing process operations,

cargo schedules, and records. What is usually a high-volume traffic facility, halted operations during a 30-hour lockdown period. Without necessary cybersecurity measures in place, federal/municipal information and operations are at risk for a possible DoS attack. High-risk infrastructures need trained end users who are capable of identifying and reporting phishing emails. These end users will act as a last line of defense to prevent future attempts to attack the facility.

In response to the threat of financial impact, officials are beginning to recognize the tangible damage caused by cyber attacks. As Senator Rob Portman of Ohio (R) said, "Hackers with malicious intent can and do attack state and local cyber infrastructure consistently. Sometimes, state and local governments need some additional help or expertise to mitigate these threats." Officials are still struggling to remain apprised of the cost and frequency of attacks.

FREQUENCY/TYPES OF ATTACKS

A cyber attack is rarely a single, isolated event, but a recurring and chronic issue. In 2020, there were at least 2,354 U.S. governments, schools and healthcare facilities impacted by ransomware.

According to Accenture, from January to August of 2021, these five ransomware variants made up 75% of observed attacks, with REvil/Sodinokibi topping the list:

- REvil/Sodinokibi
- Hades
- DoppelPaymer
- Ryuk
- Egregor

Changes Due to the Pandemic

According to a Deloitte/NASCIO study, the COVID-19 pandemic has added to the challenges that CISOs in the government face. While adequate funding has always been a significant challenge, the workforce shifted to working from home in a dramatic fashion. Prior to the pandemic, the study showed that of survey respondents from 51 states and territories, 52% had said that less than 5% of staff worked remotely. During the pandemic, 35 states had more than half of their employees working remotely and nine states said they had more than 90% remote workers.

This move to remote working has strained the already short-handed IT and security staff, and changed the nature of much of the work, including the use of technologies that existing staff had little experience deploying or securing. To help deal with this shortage, 69% of states plan to augment staff with contractors or consultants, and 51% plan to contract with a managed security services provider.

The Deloitte/NASCIO report also stated that only 40% of CISOs said they felt only somewhat confident that their state information assets are adequately protected from cyber attacks targeting local government and public higher education entities.

CHALLENGES OF ALLOCATING CAPITAL TO PREVENT ATTACKS

State and local governments are constantly combating the challenge of financial allocation. By not funding the last line of defense, long-term damages can exceed tens of thousands of dollars.

According to a study conducted by the National Association of State Information Officers (NASCIO), only 18 states have a cybersecurity budget line-item. Even more concerning is the fact that only 16% of states reported a budget increase of 10% or greater since 2018. The lack of recurring funding translates to municipal networks and computers being put at risk to increasing cyber threats.

New York District 24 representative said, "Before we have a catastrophic cyber event, we better get our act together and prioritize with more funding and more attention."

THE DECLINE OF ECONOMIC INVESTMENT IN MUNICIPALITIES

Failure to account for the negative consequences results in reduced confidence of stakeholders. It's simple: businesses can fold following cyber attacks; however, governments cannot. Maintaining the confidence of citizens and stakeholders is essential to a municipality's credit analysis. Potential investors have increased confidence when a municipality yields a strong cybersecurity defense program/policy. This reaffirms that their sensitive information and investments are generally at a lower risk to being lost in a potential cyber attack.

Municipalities frequently attempt to protect their credibility from investors by not fully disclosing details of a cyber attack. After analyzing reported attacks on local governments since 2013, 64% refused to disclose the amount requested from hackers and 30% refused to disclose if a payment was made.

But why not report the attack when the financial loss can be this worrisome and damaging?

Essentially, government entities fear losing investment confidence from potential stakeholders and the trust of their citizens.

A prime example is a ransomware attack on Pleasant Valley Hospital in West Virginia. The attack on the hospital resulted in a recovery cost of $1 million, shaking their investors' confidence. The massive remediation expenses caused the debt service coverage to fall to 78% – well below the 120% required by the investors' loan agreement. As a result, the hospital was obligated to send a notice to their municipal bondholders about the attack and its stress on their financial operations.

CONCLUSION

Below is a list detailing the greatest economic threats of cyber attacks and the potential impact they could have on states, local governments and municipalities :

- The average ransomware payment was $570,000 in the first half of 2021 (https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/)
- It is estimated that ransomware attacks cost the U.S. economy approximately $20 billion per year (https://axio.com/insights/cyberattack-strikes-us-critical-infrastructure/)
- The average ransom amount demanded by cybercriminals in the first half of 2021 was $5.3 Million (USD). (https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/)
- 53.2% of attacks in state government are targeted toward cities and local schools across the nation. (https://statescoop.com/ransomware-attacks-map-state-local-government/)

Municipalities form the backbone of civil service. By analyzing these target areas, a sweeping perspective can represent the true cost of cyber attacks.

The lack of funding for cybersecurity initiatives is detrimental. The need for legislation is important, but the need for training is crucial. Legislation is simply not enough; it acts as a superficial and temporary fix to a long-term, persistent problem. Without initiatives like cybersecurity awareness training, our governmental representatives and state and local employees are vulnerable to social engineering attacks. This is a matter of state and national security, one that should not be overlooked or ignored.

KnowBe4 offers a Ransomware Hostage Manual that can help municipalities learn what to do to better protect themselves from ransomware and how to mitigate if they do become a victim of it. Also, our free ransomware simulator tool called "RanSim" will provide a look at an organization's effectiveness of their existing network protection.

Additional Resources

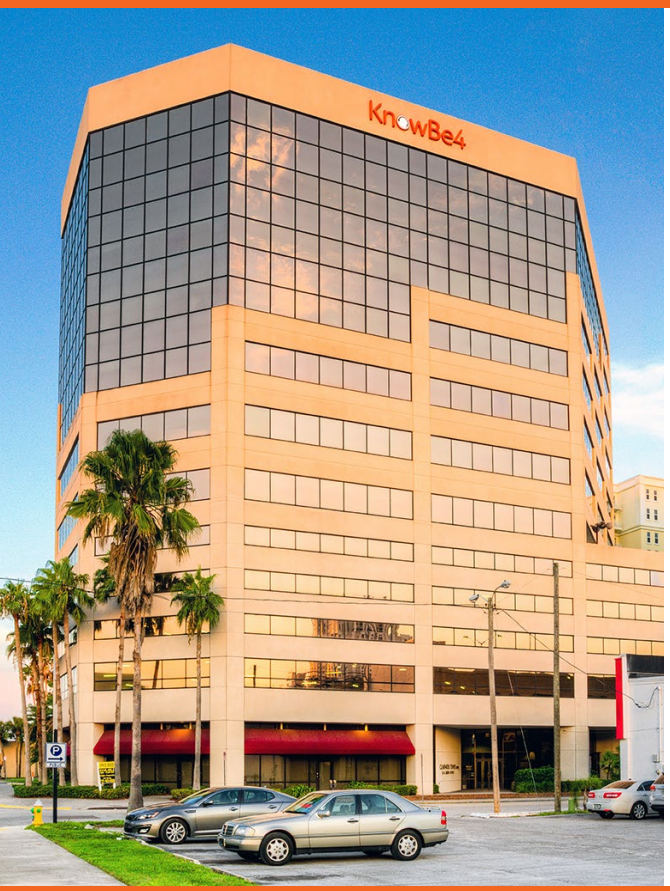
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01C05K01