KnowBe4
Human error. Conquered.

WHITEPAPER

The Economic Impact of Cyber Attacks on Municipalities

WHITEPAPER: The Economic Impact of Cyber Attacks on Municipalities

Table of Contents

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 end user 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.

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 phishing attacks posed by malicious hackers.

The attacks have infiltrated foundational departments within the community, including education, law enforcement, and healthcare. Through social engineering, a single click can expose an entire database of sensitive information to the bad actors. The result of this is often millions of dollars in financial losses, along with thousands of invaluable, confidential records.

The research gathered reveals that phishing attacks cut deeper than just the financial burden of ransomware. 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.

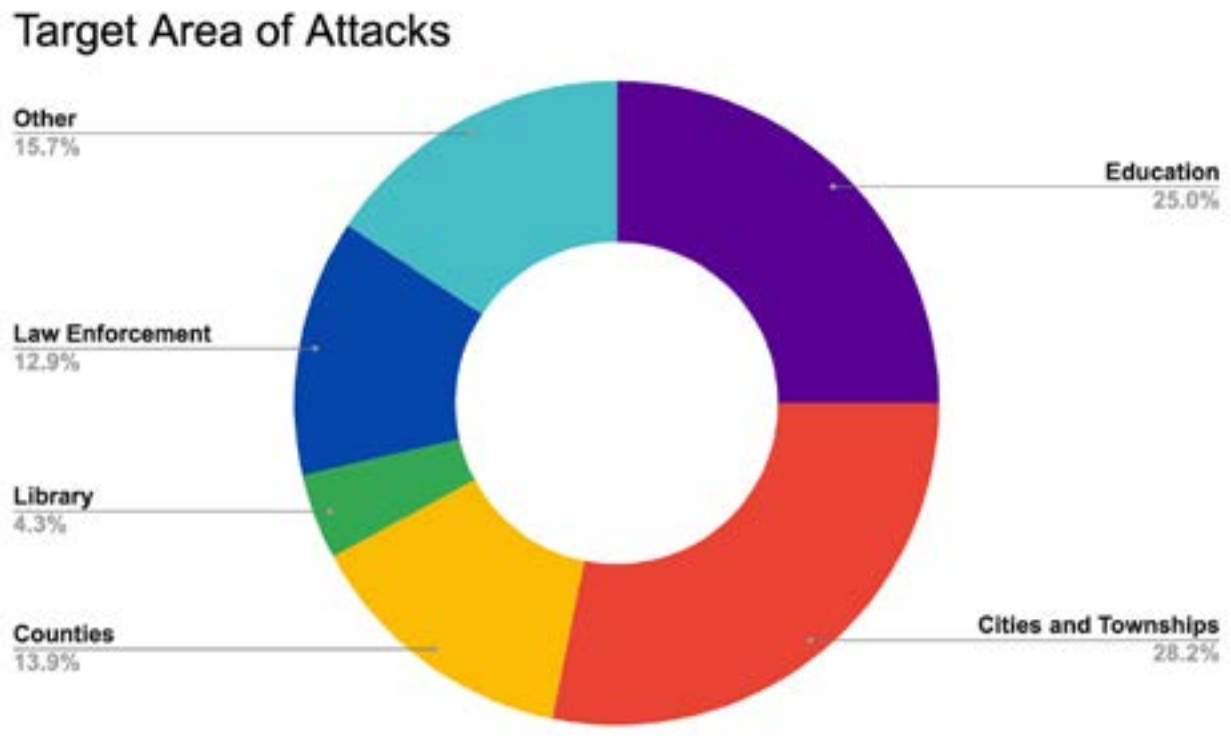
The preferred method of attack against these organizations is ransomware; a vicious malware that locks users out of their devices or blocks access to files until a sum of money or ransom is paid. If defenses fail, a city could be stuck paying the cost of a ransom or losing vital information needed to provide services to the community. From 2017-2020, the estimated reported ransom paid per event in municipalities was $125,697.

Municipalities are responsible for safeguarding sensitive information and confidential files. With such liability comes possible vulnerability. In the case of a small beach town in Florida, an uneducated click led to a cyber attack that cost roughly $600,000[1]. Cyber criminals accessed sensitive information and used it as ransom against the city of the town. With options limited, the city paid the ransom in an attempt to protect citizens' sensitive information and Personally Identifiable Information (PII).

With the increasing rates of cyber attacks on our institutions across state and local levels, 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

1 Freed, Benjamin. (2019, Oct.). Ransomware Attacks Map Chronicles a Growing Threat. State Scoop.



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, a Georgia city was hit by ransomware, with the attackers demanding $55,000 in Bitcoin. The city was not only faced with a financial burden, but sensitive information was also put at risk. This created a similar scenario to the Florida cyber attack, except the city Georgia was not willing to pay the ransom. Consequently, the recovery from the attack, which was caused by simple human error, is estimated to reach as much as $17 million[2].

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

City Population Affected	Demand (USD)	Recovery (USD)
619,493 in Maryland	$76,000	$10-18 Million
619,968 in Colorado	$51,000	$1.5 Million
523,738 in Georgia	$55,000	$17 Million
390,144 in 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.

2 Mazzei, P. (Jun. 2019. Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000. New York Times

For example, in the 14 reported ransomware attacks the state of Texas has experienced since 2016, the attacks on hospitals alone have impacted 483,000 patients and some attacks have caused nearly $20 million in total damages[3].

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."[4]

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.

As assessed by a Coveware analysis, the average downtime that results from a ransomware attack is **9.6 days**[5]. 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 ransomware 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.[6]

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.

---

3 Bischoff, P. (2020, Feb. 11). 172 Ransomware Attacks on US Healthcare Organization Since 2016 (Costing Over $157 Million).

4 U.S. Senate Committee on Homeland Security & Governmental Affairs. (2019, Jun.) Peters, Portman Introduces Bipartisan Bill to Strengthen Cybersecurity Coordination with State and Local Governments.

5 Coveware. (2019). Coveware Q2 Ransomware Marketplace Report.

6 Marine Safety Information Bulletin Commandant MSIB Number: 10-19 U.S. Coast Guard Date: December 16, 2019 Inspections and Compliance Directorate

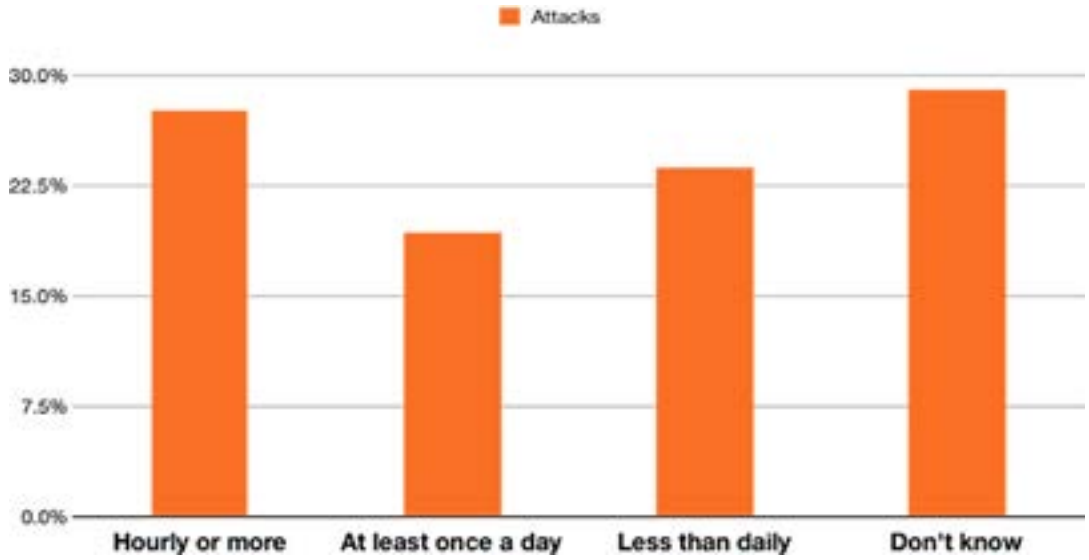
FREQUENCY/TYPES OF ATTACKS

A cyber attack is rarely a single, isolated event, but a recurring and chronic issue. In the single year between 2018 and 2019, known attacks on local governments rose 58.5%.[7]

Hackers continue to develop new methods to disable systems while extracting money and information. To understand the capabilities of cyber criminals, 10 of the most common attack types have been identified as follows:

- Ryuk (Most Common)
- CryptoLocker
- Cryptowall
- Scarab
- SamSam
- WannaCry
- Snake
- Maze
- Hermes
- Sodinokibi

The chart below outlines the typical frequency of attacks against state and local governments.



Source: University of Maryland Baltimore County[7]

In response to the threat of the financial impact, officials are beginning to recognize the tangible damage caused by 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."*[8]

Officials are still struggling to remain apprised of the cost and frequency of attacks.

Data shows that 48% of elected councilors and/or commissioners are either slightly aware or do not know the extent of the need for cybersecurity measures in the community.[7]

---

7 Donald Norris, A. J. (2018). Local Governments' Cybersecurity Crisis in 8 Charts. Baltimore: The Conversation.

8 U.S. Senate Committee on Homeland Security & Government Affairs. (2019, Nov.). Senate Passes Peters, Portman Bill to Strengthen Cybersecurity Coordination with State and Local Governments.

The chart below provides insights into government officials' various awareness levels of the need for cybersecurity. This data takes into account all levels of expertise, ranging from elected officials to average citizens to top appointed managers.

Are local government officials and staff aware of the need for cybersecurity?

Official	Not / Slightly Aware	Somewhat Aware	Moderately / Exceptionally Aware	Don't Know
Top Appointed Managers	14%	19%	61.7%	5.3%
Department Managers	21.3%	32.8%	42.3%	3.6%
Average End Users	28.7%	33.4%	34%	4%
Elected Executives	27.5%	26.5%	32%	13.9%
Staff of Elected Councilors / Commissioners	31.4%	26.3%	30.4%	11.9%
Elected Councilors / Commissioners	40.7%	26.6%	25.4%	7.3%
Average Citizens	46.9%	24.4%	8.2%	20.5%

Source: (University of Maryland Baltimore County)[9]

CHALLENGES OF ALLOCATING CAPITAL TO PREVENT ATTACKS

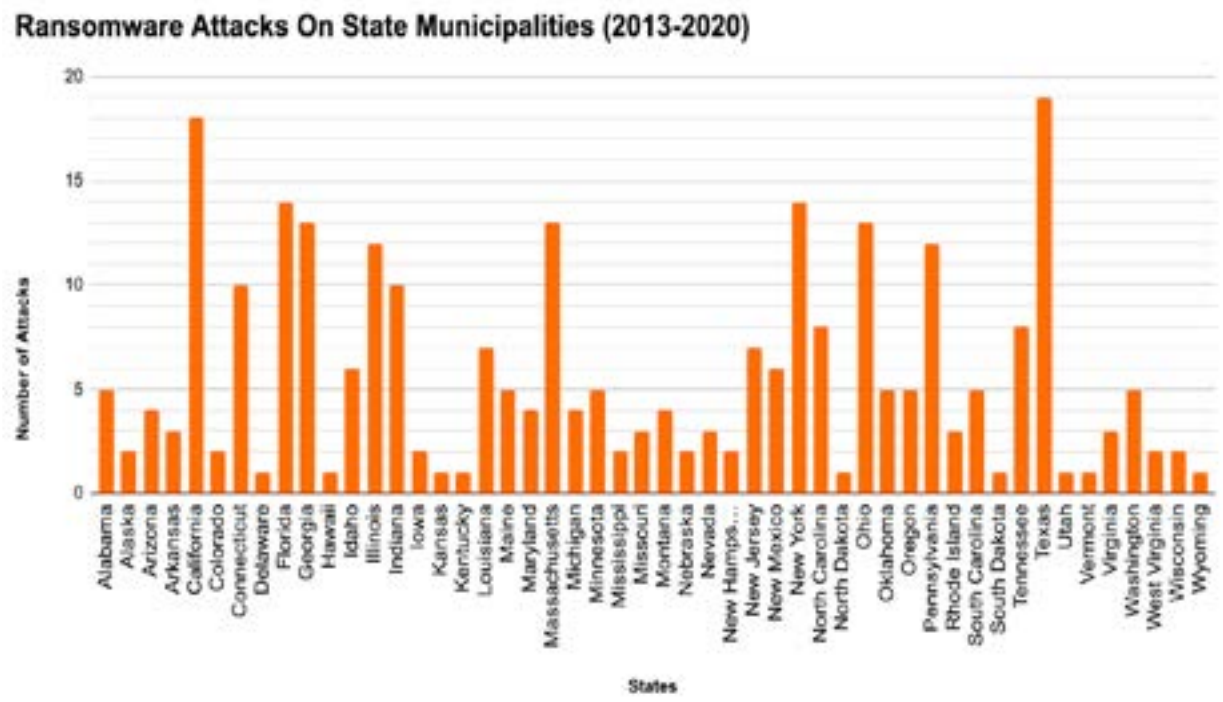
State and local government is constantly combating the challenge of financial allocation. By not funding the last line of defense, long-term damages can exceed tens of thousands of dollars. Less than half of department managers are "moderately/exceptionally aware" for the need of cybersecurity. This demonstrates that the lack of knowledge and awareness by governing officials remains a great barrier to achieving an adequately protected community.

According to a study conducted by the National Association of State Information Officers (NASCIO), about **50%** of states do not have a committed cybersecurity line-item budget. Even more concerning is the fact that **37%** of states have seen a reduction in funding or no change at all.[10] The lack of reoccurring funding translates to municipal networks and computers being put at risk to increasing cyber threats.

9 Donald Norris, A. J. (2018). Local Governments' Cybersecurity Crisis in 8 Charts. Baltimore: The Conversation.

10 Deloitte Insights. (2018). 2018 Deloitte-NASCIO Cybersecurity Study States at Risk: Bold Plays for Change.

New York District 24 representative John Katko said, “Before we have a catastrophic cyber event, we better get our act together and prioritize with more funding and more attention.”[11]



Using data from over 280 known successful cyber attacks, the chart above reveals that no state is safe from potential financial hardship.[12]

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.[12]

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.

---

11 House Committee on Homeland Security. (2019, Jun.). Cybersecurity, Infrastructure Protection, & Innovation (116th Congress) Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help.

12 Freed, Benjamin. (2019, Oct.). Ransomware Attacks Map Chronicles a Growing Threat. State Scoop.

A prime example is a ransomware attack on a 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 resulted in the debt service coverage to fall to 78%—well below the 120% required by the investors' loan agreement.[13] 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 to state and local governments:

- The average cybersecurity breach costs states between $665,000 to $40.53 million, with a median cost varying $60,000 to as high as $1.87 million.[14]
- The average ransom amount demanded by cybercriminals from 2013-2020 was $835,758.33 (USD).[15]
- 60% of states either have "voluntary" or no cybersecurity training programs at all.[16]
- 53.2% of attacks in state government are targeted towards cities and local schools across the nation.[14]

Municipalities form the backbone of civil service. By analyzing these target areas, a sweeping perspective can represent a 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 representatives, 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.

13 Mitra, Mallika. (Feb 6. 2020). Hospital's Ransomware Attack Exposes New Risk for Muni-Bond Issuers. Insurance Journal Insurance.

14 The Council of Economic Advisers. (2018, Feb.). The Cost of Malicious Cyber Activity to the U.S. Economy. White House.

15 Freed, Benjamin. (2019, Oct.). Ransomware Attacks Map Chronicles a Growing Threat. State Scoop.

16 National Conference of State Legislatures. (Published 2017- Revised Feb.2020) State Cyber Training for State Employees.

What's frightening is that a staggering 53.3% of local government institutions do not even keep track of their cyberattacks.[17]

17 Donald Norris, A. J. (2018). Local Governments' Cybersecurity Crisis in 8 Charts. Baltimore: The Conversation.

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 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 better 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

V061520