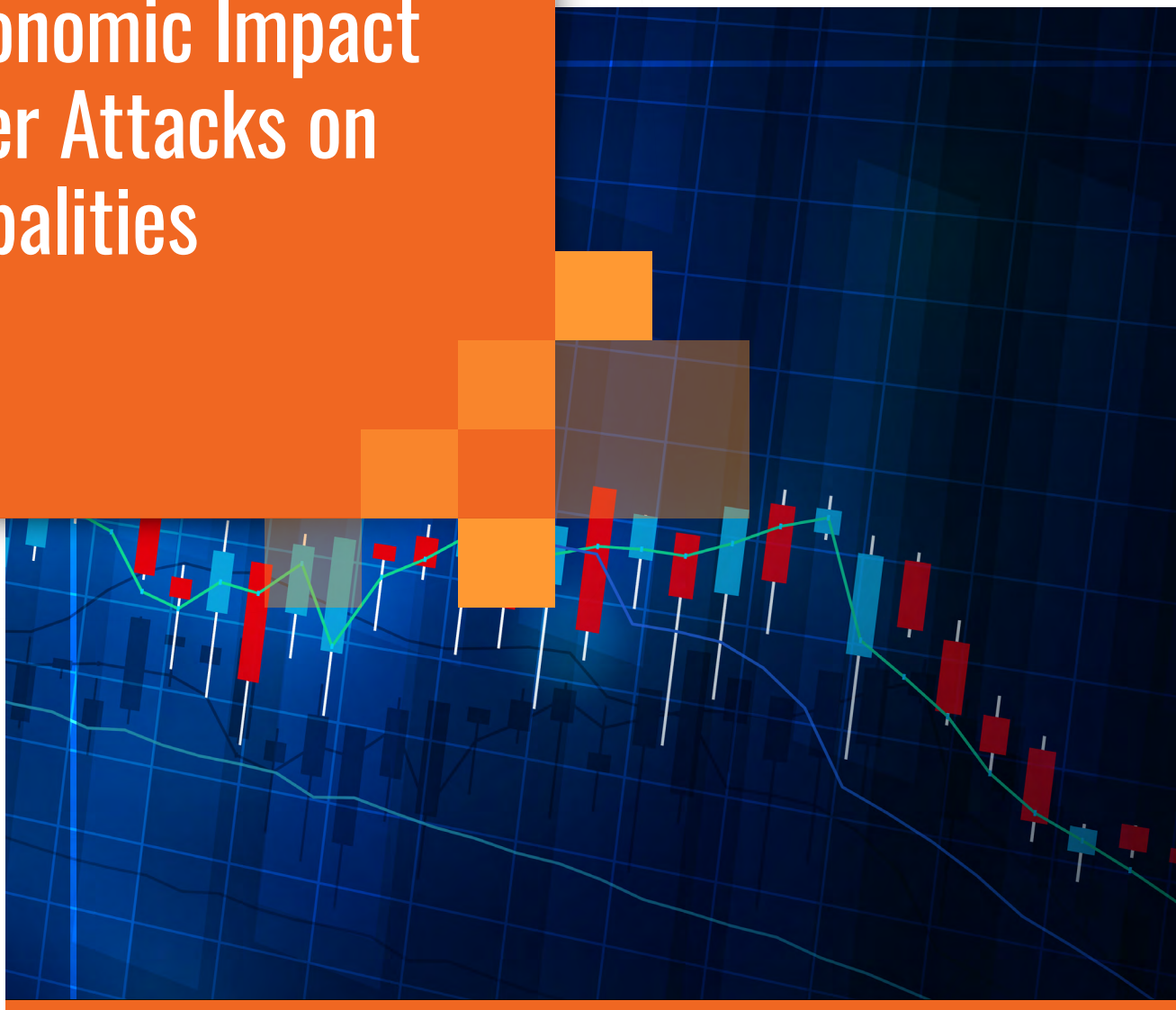
KnowBe4
Human error. Conquered.

The Economic Impact of Cyber Attacks on Municipalities



The Economic Impact of Cyber Attacks on Municipalities

Table of Contents

CYBER ATTACKS ON MUNICIPALITIES

In March 2022, the FBI issued a stark warning to local U.S. governments and public services: ransomware attacks against regional and local governments were disrupting operational services, posing risks to public safety, and generating financial losses. The impact of these attacks, it said, are "especially significant due to the public's dependency on critical utilities, emergency services, educational facilities, and other services overseen by local governments."[1] Within the government sector, local government entities had become the second highest victimized group behind academia.

Larger organizations and agencies with access to greater resources, including states and transit systems, have demonstrated stronger readiness to deal with attacks. But regional and local governments struggling with weak security planning, lax risk prevention, and poor response and recovery, have been left vulnerable to attack. Adding these conditions to the volume and sensitivity of data on their servers, which include records and operations of law enforcement, city operations, healthcare, and education, as well as Personally Identifiable Information (PII) such as passport numbers, social security numbers, bank accounts, private health information and even mental health evaluations, the costs of a cyber attack are potentially far higher than in the private sector. In the eyes of the hacker community, this makes them more likely to pay the ransom. These factors are compounding to make regional and local governments increasingly attractive soft targets for malicious hackers.

Smaller administrations and agencies may also be less familiar with the mechanism for reporting to and accessing support from law enforcement and specialist security vendors, meaning that the true impact of ransomware will continue to be under reported and in a high percentage of cases, victims will not receive the support they need.

School districts demonstrated a lower level of cyber risk preparedness than other governmental sectors. Relative to their local government peers, districts trail in key metrics such as MFA use and data backups. Risk management practices such as red team testing are mostly out of reach for cost reasons, with only 9% of districts conducting them.

According to Moody's[2], which began tracking school districts in 2018, the rates at which school districts are targeted has increased "exponentially." School cyber breaches most often result in unauthorized access to student and teacher data, leaving individuals vulnerable to future misuse of this information, particularly through identity theft. These attacks have at times resulted in school closures or delayed openings.

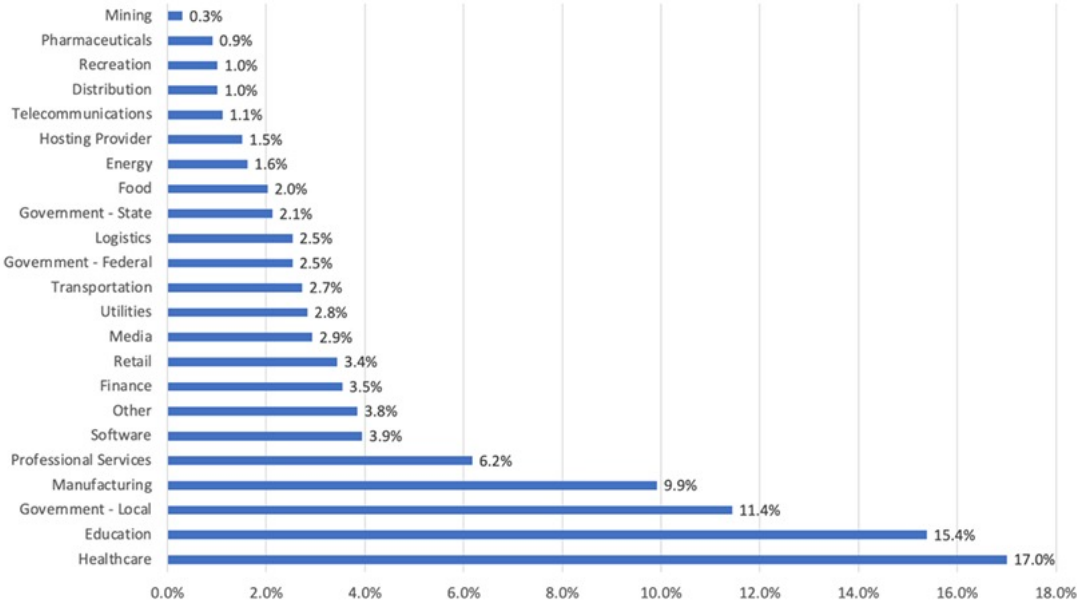
Like attacks in the private sector, though the tools attackers use once in the victim's network are increasingly sophisticated, getting into the network in the first place is often done with low-tech phishing emails. Through social engineering, a single click by an unaware user can expose an entire database of sensitive information to the bad actors or allow bad actors to hold the entire network hostage.

Due to the damage to the trust placed in them by their communities, local agencies stand to lose considerably more from a single click than organizations in the private sector. When these are added to tangible financial losses, and the greater allocation of resources required to overcome the attack, the losses from one attack can amount to millions of dollars.

---

[1]https://www.ic3.gov/Media/News/2022/220330.pdf
[2]https://www.moodys.com/researchdocumentcontentpage.aspx?docid=PBM_1268980

DISTRIBUTION OF DESTRUCTIVE RANSOMWARE EVENTS BY INDUSTRY SECTOR: JANUARY, 2023[3]



RANSOMWARE ON THE RISE

While attacks against regional and local governments are often unreported, data gathered from disclosure statements, press reports, the dark web, and third-party information feeds[4] shows that a minimum of 106 ransomware attacks in these sectors were reported in 2022, an increase from 77 attacks in 2021. Forty-four universities and colleges and 45 school districts operating 1,981 schools were similarly impacted by ransomware in 2022, nearly double the 2021 figure of 1,043 schools.

One of the largest attacks in 2022 was against the Glenn County Office of Education (GCOE) in California, which serves eight school districts. On May 10, GCOE was struck by an attack that knocked the internet, voice-over-internet phones, emails and financial software offline for GCOE, the school districts and many of the schools. After having claimed to have deleted all backups and locking the agency's software, the Quantum ransomware gang initially demanded a $1 million ransom. After two weeks of negotiations, GCOE reportedly paid a $400,000 ransom to Quantum. Notifications were sent to current and former students as well as teachers notifying them of the theft of names, social security numbers and other personal information[5].

In November 2022, a single attack on Miller County, Arkansas' mainframe affected endpoints in 55 counties. Though no data was exfiltrated, offices including the county treasurer, the county clerk, courthouses and the county judges' offices were forced to go offline or temporarily close for more than two weeks.

The Housing Authority of the City of Los Angeles, or HACLA, provides affordable housing to more than 19,000 low-income families across Los Angeles. The agency maintains more than 6,300 units of public housing where tenants can pay rent using their bank account or credit card information

[3]https://www.riskrecon.com/report-five-lessons-learned-from-ransomware-attacks
[4]https://www.emsisoft.com/en/blog/43258/the-state-of-ransomware-in-the-us-report-and-statistics-2022/
[5]https://www.databreaches.net/scoop-glenn-county-office-of-education-paid-400k-ransom-after-ransomware-attack/

through the HACLA online payment portal. HACLA oversees the city's Section 8 housing voucher program, which provides subsidies to more than 43,700 households renting apartments or houses and maintains hundreds of thousands of applications for vouchers.

On December 31, 2022, hacker group LockBit claimed responsibility for a ransomware attack on the agency, posting images of purported HACLA databases containing 15 terabytes of stolen data, saying they would publish the data on the dark web if their payment demands were not met.

It was the second major cyber attack on a Los Angeles city agency in less than four months. In September 2022, the Los Angeles Unified School District — the second-largest school district in the U.S. — was hit by the Russian-speaking Vice Society ransomware group. The incident occurred over Labor Day weekend, a time when there would be fewer workers around to notice unusual network activity. When the school district refused to pay the ransom, the ransomware group published hundreds of gigabytes of data stolen during the attack, including personal records, health records and evaluations of students.

BEC (BUSINESS EMAIL COMPROMISE)

According to the 2022 IC3 Report[6], BEC attacks were one of the two most lucrative forms of cyber attacks in 2022, generating a total of $2,742,354,049 in losses across sectors, an increase of $346m from 2021, and $875m from 2020. State and local governments are particularly vulnerable.

Government transparency laws require that government operating information be made publicly available, allowing cybercriminals to acquire information on agency leadership, vendor relationships and associated contractors, and making it possible to tailor attacks directly to the victims. Records can expose other vulnerabilities, including a lack of cybersecurity training, allowing them to identify the agencies and personnel they can most easily compromise.

BEC attacks have also targeted accounts used for pension funds, payroll accounts and contracted services, losses of which can impact government operations as well as government employees, citizens and vendors.

Between November 2018 and September 2020, when the FBI began diligently tracking BEC attacks against state and local government organizations, there had already been millions of dollars lost to the scams. Losses from individual BEC attacks during the time period had ranged from $10,000 to $4m. These included Erie, Colorado, which in 2019 electronically sent $1 million to a fraudulent account after an impersonator changed the payment preference method for the primary contractor on a local bridge project from check to electronic transfer. In 2019, Ocala, Florida, fell victim to a spear phishing email that looked like it came from a construction firm working on a new terminal at the city's airport. The city lost more than $740,000. In January, 2020, hackers stole $2.6 million from the government of Puerto Rico through a BEC attack. In 2020, losses from BEC attacks on state and local governments totaled nearly $1.9bn.[7]

The chances of success of BEC, phishing and spear phishing rose during the pandemic, with remote government workers potentially even more likely to click on phishing links. A State, Local, Tribal, and Territorial (SLTT) assessment last year by the Cybersecurity and Infrastructure Security Agency (CISA) revealed a click rate of nearly 14%.

[6]https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[7]https://www.ic3.gov/Media/News/2021/210318.pdf

The easing of pandemic restrictions, however, has not slowed the rise of BEC attacks. The attacks increased across all sectors by 175%, with an 81% surge in 2022[8]. Ninety-eight percent of employees failed to report the threat. Government employees were the target of almost half of all phishing attacks last year.[9]

A CrowdStrike report released in early 2023 tracked the sale of stolen information to "threat actors" and found that the sale of compromised credentials from the government sector were among the top 10 sectors advertised by access brokers in 2022.[10]

IMPACT

The economic impact of cyber attacks on regional and local governments can be 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

KEY FINDINGS

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 strong and secure IT systems, but to have personnel who are trained to recognize the threats, giving the IT department support in creating a human firewall.

THE AVERAGE FINANCIAL LOSS

Many, old-school SAT programs fail to account for something called the knowledge-intention If paid, the ransom amount represents only about 15% of the cost of recovery. Ransomware attacks on state and local governments last an average of 7.3 days. Down time alone generates an average loss of $64,645.[11] Additional costs include data loss, the cost of rebuilding systems, reputational loss and new security implementations.

According to IBM's latest data breach report, in 2022, across sectors, the average cost of a ransomware breach was $4.54 million, not including the cost of the ransom itself. Targets that suffered 'destructive' attacks, where cybercriminals sought to use malware to destroy data, saw even higher expenses, with an average cost of $5.12 million.[12]

[8]https://abnormalsecurity.com/blog/28-of-bec-attacks-opened-by-employees
[9]https://www.lookout.com/documents/threat-reports/us/lookout-rise-in-mobile-phishing-in-pubsec.pdf
[10]https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf
[11]https://www.checkpoint.com/industry/government-state-local-security/
[12]https://www.blackfog.com/the-true-cost-of-ransomware-attacks/

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, or both. In all scenarios, sensitive information will be lost, and the municipality will be compromised.

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. 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. Within that sector, those classified as Maritime Transportation Security Act (MTSA) facilities, which house critical assets and infrastructure, are particularly ideal targets for phishing attacks. 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. 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.

FREQUENCY/TYPES OF ATTACKS

There are 1.7 million ransomware attacks every day, which means 19 ransomware attacks every second. Cybersecurity Ventures predicts that by 2031, ransomware will cost victims $265 billion annually, and it will attack a business, consumer or device every 2 seconds.[13]

The most commonly observed ransomware variants in Q4 2022 were:[14]

Rank	*Ransomware Type*	*Market Share %*	*Change in Ranking from Q3 2022*
1	Hive	13.8%	+1
2	Black Basta	12.2%	+1
3	BlackCat	10.6%	-2
4	Royal	8.9%	New in Top Variants
5	Phobos	6.5%	-1
6	Quantum	4.8%	New in Top Variants
7	Diavol	3.2%	New in Top Variants
7	LockBit 3.0	3.2%	New in Top Variants

In 2022, three new variants - Vohuk, ScareCrow, and AESRT - were identified by Fortinet[15] as rapidly proliferating across all sectors in multiple countries. All three target Windows systems.

This is a rapidly changing landscape. **In the first half of 2022,** the FortiGuard Labs team documented 10,666 new ransomware variants compared with just 5,400 in the second half of 2021, a nearly 100% increase. The growth is primarily attributable to attackers taking advantage of ransomware-as-a-service (RaaS) on the Dark Web. The increase is expected to continue into 2023.

Recent cases have also revealed two novel features of ransomware operations in 2022: increasing dwell time and aggression. In a municipal emergency service incident, SecurityScorecard determined that the attacker spent 90 days in the victim system prior to detection.[16] According to experts, this reflects a broader trend. Longer dwell times may suggest that actors hope to make more informed decisions about what data they can monetize.

In one municipal emergency response case, for example, attackers disabled the victim's anti-virus software to avoid detection. They then spent some of their 90-day dwell time attempting further vertical and lateral movement, perhaps in hopes of breaching more lucrative targets. From the emergency service, they tried to access the internal systems of other local government bodies, including city hall, and launched DNS poisoning attacks from the infected system.

Ransomware groups have been observed taking increasingly aggressive steps to exert pressure on victims to pay ransoms, including contacting those whose PII has been stolen, and in recent incidents,

[13]https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031
[14]https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments
[15]https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-vohuk-scarecrow-and-aerst-variants
[16]https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments/

contacting friends and family members of executives of affected organizations to exert additional pressure on the victims.

METHODS OF DISTRIBUTION

1. **Human error.** Eighty-two percent of all data breaches are causes by human error[17], primarily resulting from **phishing** and **spear phishing**,[18] with attackers impersonating a reputable entity with the aim of deceiving the target into revealing sensitive information or installing malware. Phishing and spear phishing are most commonly accomplished by email, with about 3.4 billion phishing emails sent every day, but can also be carried out with text messages, social media apps and phone calls.
2. **Compromised credentials,** which can be obtained by phishing but may also be purchased on the dark web, or obtained by brute force attacks. **Once compromised login credentials are used,** attackers may deploy malware immediately. They may also move laterally within the network and prepare the environment to maximize impact of an attack.
3. **Exploit kits** are toolkits that detect and exploit known security vulnerabilities in client-side software, including the operating system, browser and other applications. Once detected, the exploit kit automatically deploys targeted malware.
4. **Compromised managed service providers** (MSPs) take advantage of the fact that MSPs remotely manage the IT infrastructure of multiple clients allowing cybercriminals to gain access to the MSP's client base with one hit.
5. **Pirated software.** Illegal, and a common source of malware. Used for delivering keyloggers, ransomware, trojans, backdoors, cryptojackers, adware and more.

CHALLENGES OF ALLOCATING CAPITAL TO PREVENT ATTACKS

You must remember that your security awareness program and content are the visible face of your State and local governments are constantly combating the challenge of financial allocation, a challenge that has left cybersecurity chronically underfunded in many states, even in those that have been frequent targets of ransomware actors. Most state cybersecurity budgets are between 0% and 3% of their overall IT budget. In the private sector, that figure is more than 10%, according to the National Association of State Chief Information Officers (NASCIO).

According to a study conducted by 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. By not funding the last line of defense, long-term damages can be extensive.

[17]https://www.verizon.com/business/resources/reports/dbir/
[18]https://www.emsisoft.com/en/blog/43733/how-does-malware-spread-top-5-ways-malware-gets-into-your-network/

There are exceptions that may point to a shifting and more hopeful landscape. In December 2021, the State of Virginia suffered an attack of "extremely sophisticated malware" that temporarily locked up the state legislature's computer systems. In response to the attack, the Virginia House inserted a line item in its state budget bill for $150 million to cover cybersecurity over the next two years.[19]

THE DECLINE OF ECONOMIC INVESTMENT IN MUNICIPALITIES

Businesses can fold following cyber attacks. Governments cannot. Maintaining the confidence of citizens and stakeholders is essential to a municipality's credit analysis, and vulnerabilities or a hindered ability to rapidly respond to attacks reduces the confidence of stakeholders and threatens credit standing.

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,[20] 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?

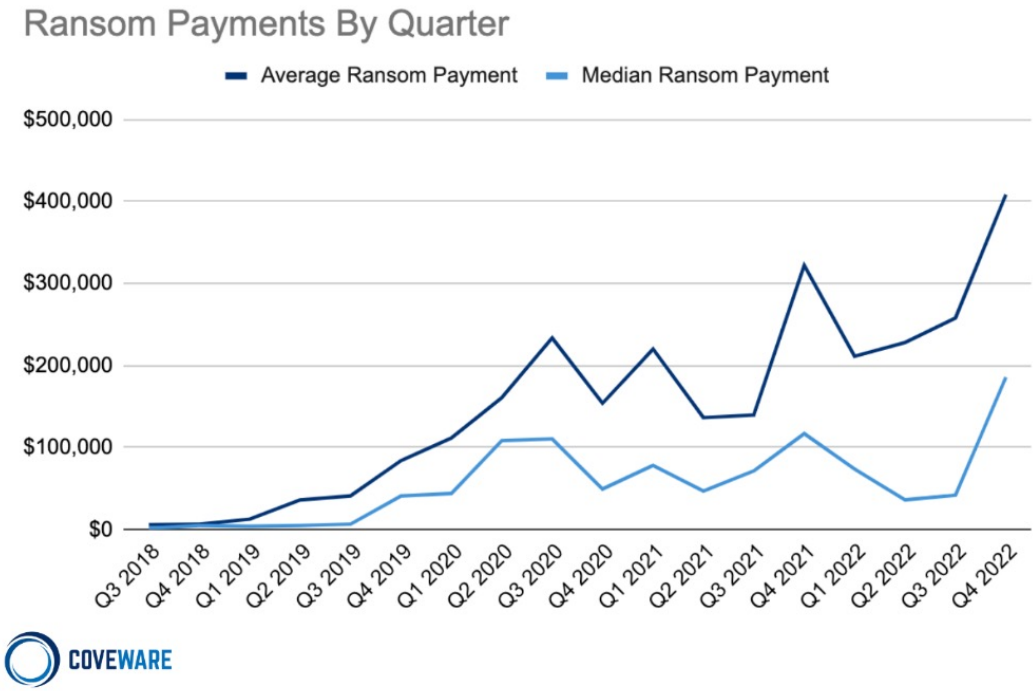
Essentially, government entities fear losing investment confidence from potential stakeholders and the trust of their citizens.

A prime example is a ransomware attack on Pleasant Valley Hospital in West Virginia in 2020.[21] 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.

[19]https://richmond.com/news/state-and-regional/govt-and-politics/rocked-by-ransomware-attacks-virginia-makes-cybersecurity-a-priority-in-budget/article_279aa723-cc76-5c3f-a74f-a9726a06692d.html

CONCLUSION

- While ransomware and BEC attacks have increased in the state and local government sector, over the last four years, ransom payments across all sectors have fallen dramatically, from 85% of victims in Q1 of 2019, to 37% of victims in Q4 of 2022. On an annual basis, 41% of victims paid in 2022 versus 76% in 2019. This can be attributed to enterprises investing substantially more in security and incident response planning. A heightened appreciation for existential risk of a ransomware attack has substantially increased funding to enterprise security and incident response teams. These advances, however, are not reflected in state and local government sectors.
- Perhaps in an attempt compensate on the part of the attackers, the average ransom payments in the last quarter of 2022 surged 58% over the previous quarter to $408,644 while the median payment skyrocketed 342% to $185.972 over the same period.[22]



- It is estimated that ransomware attacks cost the U.S. economy approximately $25 billion per year.
- 53.2% of attacks in state government are targeted toward cities and local schools across the nation.[23]

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 significantly more 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.

[20]https://statescoop.com/ransomware-attacks-map-state-local-government/
[21]https://www.insurancejournal.com/news/national/2020/02/06/557539.htm
[22]https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments
[23]https://statescoop.com/ransomware-attacks-map-state-local-government/

Additional Resources

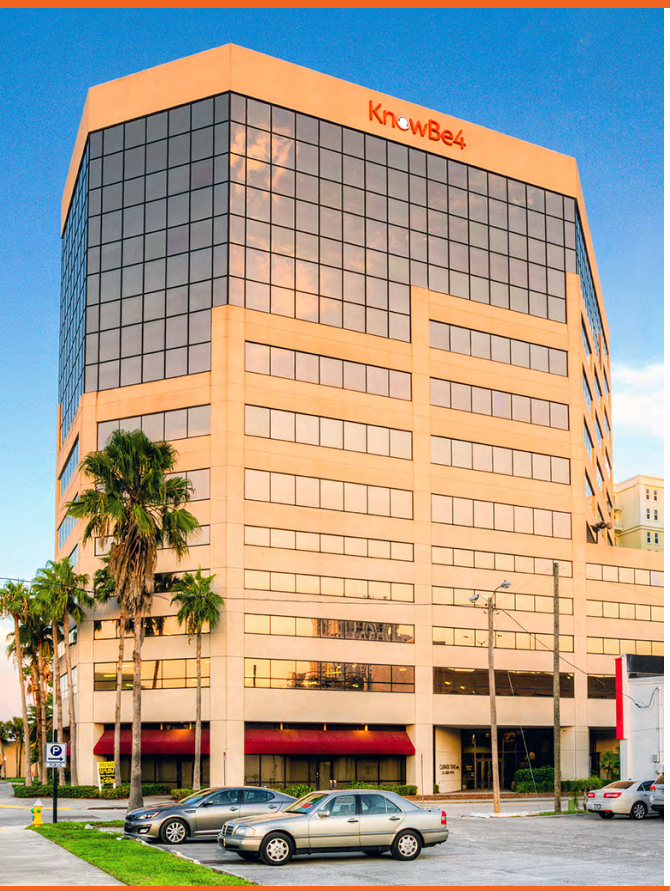
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

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 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

01D03K01