KnowBe4

State and Local Cybersecurity: Facing New Burdens Amid Rising Threats

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

052025

Table of Contents

INTRODUCTION

With the exception of a relatively small number of wealthy cities and regions, cybersecurity departments of municipalities, where they exist, are largely understaffed and underfunded. Add archaic IT infrastructure and shrinking budgets into the picture, along with troves of sensitive data sitting on the servers, and we start to see why hackers have increasingly trained their eyes on the sector.

Cybercriminals are developing new and more potent variants of ransomware, and increasing sophistication of phishing techniques with the help of AI. Unfortunately, fighting back is about to get even more difficult.

The Attackers Have the Momentum

It can be daunting to put a precise figure on the number of ransomware attacks against local and state governments. There is no standardized requirement for reporting cybersecurity incidents at the local government level, and there are many reasons, including the loss of public confidence, for officials to be reticent about calling attention to breaches of their systems. But much can be known from the trends in recent years.

In 2023 Rita Reynolds, chief information officer at the National Association of Counties told Axios that nearly seven in 10 leaders at local and state governments reported having faced ransomware attacks.[1] That same year, the FBI reported that government entities, including local and state agencies, were the third most-targeted sector by ransomware.[2]

Some of the most valuable information and trends have come from the Center for Internet Security (CIS), an upstate New York nonprofit that provides information sharing and analysis operations to government agencies and Congress. Primarily supported by the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security. CIS has a division, the Multi-State Information Sharing and Analysis Center (MS-ISAC), designed more than 20 years ago to serve as the central cybersecurity resource for the nation's State, Local, Territorial, Tribal (SLTT) governments. Its 18,000+ members include not only SLTT government agencies, but also law enforcement, educational institutions, public utilities, transportation authorities, public hospitals, educational institutions, and others. Services offered to its members include cybersecurity advisories and alerts, secure information sharing, tabletop exercises, a weekly malicious domains/IP report, real-time threat analysis, and more.

MS-ISAC also publishes the National Cybersecurity Review, a bi-annual assessment of the state of cybersecurity SLTT government organizations based on voluntary responses from its members. The report goes not only to member organizations but to U.S. government agencies and Congress.

MS-ISAC's 2022 survey, published in March 2023 and based on responses from more than 3,600 SLTT members,[3] found that malware attacks had increased by 148% between 2022 and 2023, while ransomware incidents had increased by 51%. The report documented a 313% rise in security incidents, including data breaches, unauthorized access, and insider threats.

1 https://www.axios.com/2023/05/16/ransomware-us-cities-towns-local-government-hackers
2 https://arcticwolf.com/resources/blog/notable-cyber-attacks-on-government-agencies/
3 Fox-Sowell, Sophia, "Cyberattacks on state and local governments rose in 2023," says CIS report, Statescoop, January 30, 2024

Its 2025 report, "Strengthening Critical Infrastructure / State, Local, Tribal, & Territorial Progress & Priorities," was published March 10, 2025.[4] It highlights growing cyberthreats to critical infrastructure, warns of a surge in attacks by nation-state-affiliated and criminal groups targeting state, local, tribal, and territorial (SLTT) installations, often aimed at undermining public trust. With much of the nation's critical infrastructure managed at these levels, the report stresses the urgent need to build more resilient systems, improve threat intelligence sharing, and strengthen coordinated incident response efforts to protect vital services and maintain national security, saying:

> In every community across America, services on which small business owners and working Americans rely face unrelenting attacks to our critical infrastructure. These attacks on our critical infrastructure, when successful, have significant and costly direct impacts on government services and undermine Americans' confidence in our nation's ability to defend itself.
>
> U.S. State, Local, Tribal, and Territorial (SLTT) organizations are the defenders of much of the nation's critical infrastructure that keeps everyday life moving forward. SLTT organizations are uniquely positioned to address local threats and collaborate with federal entities to share actionable intelligence. Their involvement is crucial in national security efforts, particularly in enhancing cybersecurity and emergency communications. Moreover, critical infrastructure owned by the private sector is almost universally dependent on the proper functioning of SLTT critical infrastructure.
>
> Safeguarding this infrastructure is a national imperative as its destruction or disruption would severely impact national security and economic prosperity for the individual, locally, and nationally.

4 "Strengthening Critical Infrastructure / State, Local, Tribal, & Territorial Progress & Priorities," MS-ISAC, March 10, 2025

The Unique Challenges

Local governments in particular are amorphous entities. They include not only the networks within city offices, but also public libraries, the police and fire departments, municipal courts, parks and recreation, housing, and more.

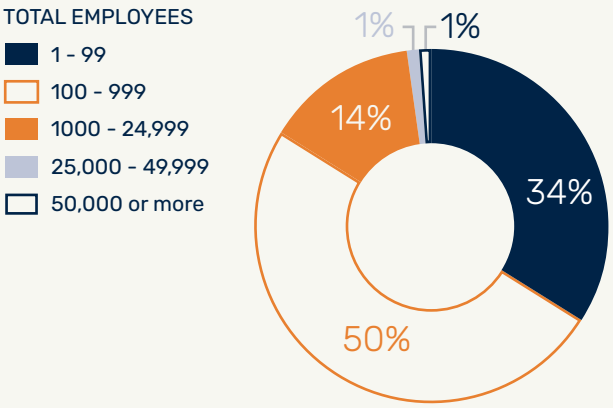
Funding for their IT Departments comes from annual budgets that require buy-in from local politicians or federal grant programs. While cyberattackers seem to evolve on a dime, the funding of municipal IT Departments is a long process not quickly adaptable to rising or urgent threats.

Most local governments have small teams (see below), many of which are expected to not only monitor and respond to threats, keep their systems updated and patched, but also provide tech support to employees and even residents.

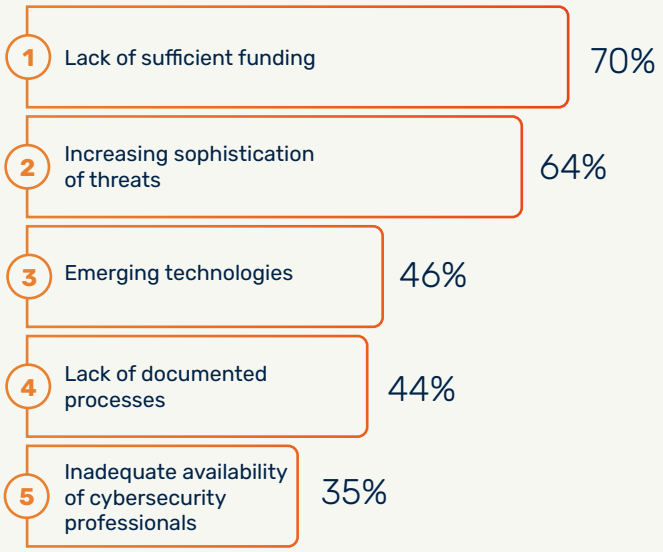
In September 2024, the Center for Internet Security released a summary report based on a survey of 4,210 SLTT government organizations. Of those, the bulk of the participants were from local governments:

PEER GROUP: **XX** | STATE: **48** | STATE AGENCY: **490**
LOCAL: **3609** | TRIBAL: **22** | TERRITORIAL: **6**

In a telling portrayal of the sector, more than 80% of participants reported their organization had less than five employees dedicated to cybersecurity, including organizations with up to 24,999 employees:



Participants, the report says, have consistently identified the same top five security concerns since 2015:



Per the report:

With a lack of security staffing, it is difficult to begin assessing and implementing an appropriate cybersecurity program. The current lack of staffing and capability demonstrates a need for managed services and low-resource, low-maintenance resources, tools, and services that can be used without creating more effort for the SLTT partner.

Economic Impact and Lost Production

Direct recovery costs of a cyberattack include ransoms paid, forensic reviews, and help required to rebuild servers and workstations. Secondary, but often more substantial costs stem from downtime losses, including lost revenue and lost productivity, loss of reputation and loss of confidence on the part of customers and/or investors.

On March 18, 2025, Comparitech released a report based on a study of 525 attacks on government agencies including 911 dispatch centers, sheriff's offices, city councils, and utilities.[5] The report put the average ransom per attack at $872,656, costing $458 million in total. But the ransom costs for these attacks pale next to the cost of downtime and lost services, which averaged more than double that figure at $1.09 billion, largely due to disruptions to key infrastructure and services. "Government employees," it notes, "are often left stranded without their systems and have to resort to pen and paper. In some cases, organizations may be able to restore lost data using backups, but in many cases, they are forced to either pay extortionate ransom demands or make the costly decision to rebuild their systems from scratch."

On March 18, 2025, *The Record*[6] illustrated just a slice of four states under cyberattack, and the toll on police stations, school districts, courts, and more. In Kansas, Atchison County offices were closed and services restricted after an attack impacted the county's computer network. Cleveland, Ohio, was just three weeks out from a cyberattack that had brought down its systems. Its court system, which had been closed for a week by the attack, had still not recovered, hampering dozens of trials. Workers did not have computer access and had been forced to do many tasks by hand. The court's website was still down, and they were unable to conduct background checks.

At the same time, in New England three other U.S. municipalities were dealing with cyberattacks, including two school districts in New Hampshire and Connecticut's Derby Police Department. Strafford County, home to 133,000 people, had been struggling with communication systems outages for three days due to an attack that a prosecutor working on an attempted murder trial called "debilitating."

EXAMPLES

NOVEMBER 1, 2024 THE HOUSING AUTHORITY OF THE CITY OF LOS ANGELES (HACLA)

Cactus ransomware gang claimed it stole 861 gigabytes (GB) of data that included personal information, backups, financial documents and more.

NOVEMBER 1, 2024 SAN JOAQUIN COUNTY, CALIFORNIA, SUPERIOR COURT

Nearly all of digital services knocked offline due to a cyberattack, including all of the court's phone and fax services, websites containing juror reporting instructions, the e-filing platform, credit card payment processing and more. Some jurors scheduled for this week were excused.

NOVEMBER 3, 2024 CITY OF COLUMBUS, OHIO

A ransomware attack resulting in the theft of 6.5 TB of information from the city of Columbus, Ohio, exposing the information of more than 500,000 current and former residents. Stolen data contained emergency services data, access to city cameras and more.

NOVEMBER 7, 2024 WASHINGTON'S COURTS IN THE COUNTIES OF THURSTON, MONROE, RENTON, PUYALLUP, BAINBRIDGE, KING, PIERCE, WHATCOM, AND LEWIS

Outages impact Washington state courts after 'unauthorized activity' detected on network.

NOVEMBER 13, 2024 CITY OF SHEBOYGAN, WISCONSIN

Series of technology outages confirmed from hackers gaining "unauthorized access" to city's network.

NOVEMBER 27, 2024 CITY OF HOBOKEN, NJ

City shut down its government, closed city hall and local courts in ransomware attack.

5 Bischoff, Paul, "Ransomware attacks on US government organizations have cost over $1.09 billion," Comparitech, March 18, 2025.
6 Greig, Jonathan, "Municipalities in four states are struggling with cyberattacks limiting services," *The Record*, March 18, 2025.

An hour away from Strafford, the Pelham School District had warned parents that it was still "facing technological issues" caused by a cyberattack. Teachers were using "printed materials, offline digital resources, and previously downloaded materials, to continue delivering lessons." They asked parents to be flexible with assignments, report cards and progress reports.

Costs can continue for months following an attack. On August 24, 2024, the Port of Seattle, which runs Seattle-Tacoma International Airport, several parks, container terminals and more, suffered an attack from the Rhysida ransomware gang. The attack knocked out the airport's Wi-Fi, leaving employees using dry-erase boards for flight and baggage information, and some airlines manually sorting through bags. Encryptions and the resulting system disconnections took down port services like "baggage, check-in kiosks, ticketing, Wi-Fi, passenger display boards, the Port of Seattle website, the flySEA app, and reserved parking." Eight months later, on April 4, 2025, the Port announced that it was sending breach notification letters to 71,000 Washington residents whose personal information had been stolen in the attack, including names, dates of birth, Social Security numbers, driver's licenses, ID cards, and medical information.

Other costs are virtually immeasurable. In July 2024, the Rhysida hacker group exfiltrated three terabytes (TB) of data from the city of Columbus, Ohio. After unsuccessfully attempting to extort $1.7M in Bitcoin from the city, the attackers released the data onto the dark web.[7] Apparently, the three TB was just 45% of the stolen data, the rest having been sold. In August, the city warned that the published data included information on victims and witnesses stolen from the local prosecutor's database.[8] City Attorney Zach Kelin acknowledged that there were "probably people that are out there that are maybe trying to escape an abuser, that are trying to escape a situation that could be violent for them."

EXAMPLES

NOVEMBER 27, 2024 TEXAS CITY, MINNEAPOLIS AGENCY

RansomHub operation took credit for damaging attacks on the city of Coppell, Texas, and the Minneapolis Park and Recreation Board.

JANUARY 5, 2025 SOUTH PORTLAND PUBLIC SCHOOLS IN MAINE AND RUTHERFORD COUNTY SCHOOLS

South Portland Public Schools in Maine said it was forced to take its network down after a cyberattack was discovered, and Rutherford County Schools said on December 27 that it had been dealing with a "network and systems disruption" since November 25.

JANUARY 8, 2025 WINSTON-SALEM, NORTH CAROLINA

Residents were not able to pay their utility bills online after a post-Christmas cyberattack knocked the city's systems offline.

FEBRUARY 12, 2025 SAULT TRIBE IN MICHIGAN

Ransomware attack knocked many of the tribe's critical services offline, and impacted "multiple computer and phone systems across tribal administration, including the casinos, health centers and various businesses."

FEBRUARY 26, 2025 CLEVELAND MUNICIPAL COURT

'Cyber incident' shuts down Cleveland Municipal Court for three days.

MARCH 25, 2025 UNION COUNTY, PENNSYLVANIA

Personal information from 40,000 Union County, Pennsylvania, residents was stolen during a ransomware attack on government systems. Affected information appeared to be mostly related to individuals involved with County law enforcement, court related matters, and/or other County business.

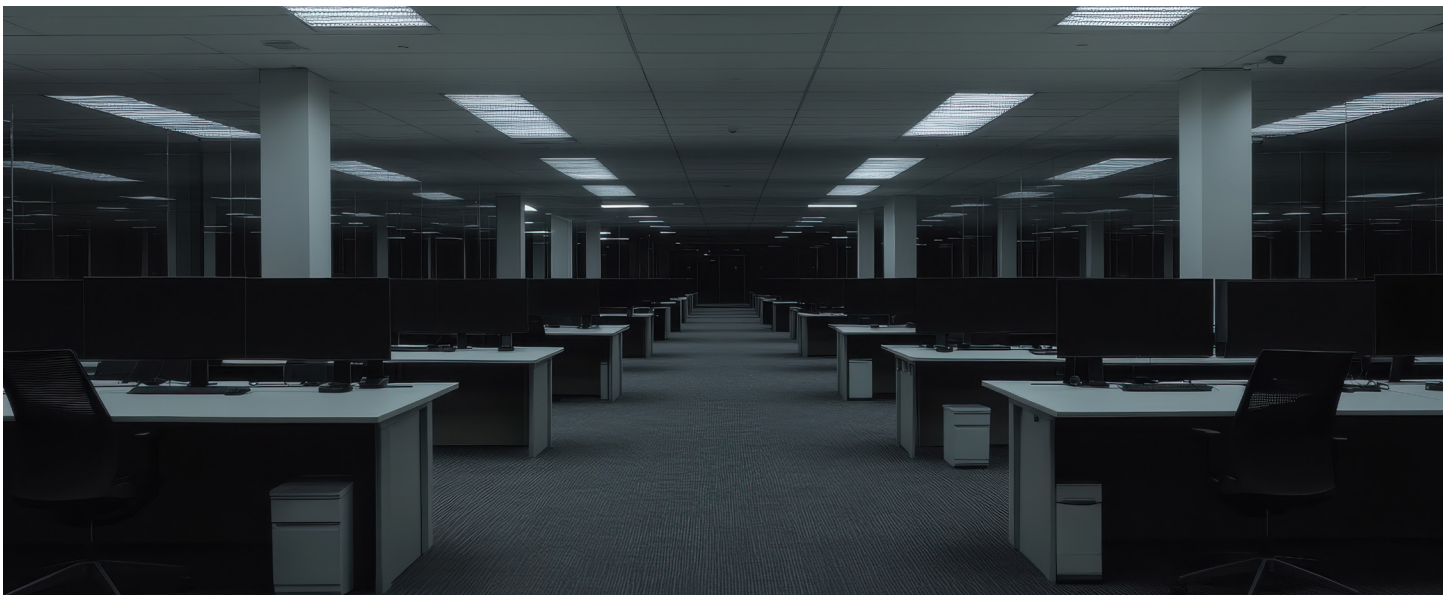
Source: Cyber Management Alliance

7 Bush, Bill, "Hackers release reams of stolen Columbus data on dark web," *Columbus Dispatch*, August 8, 2024
8 Greig, Jonathan, "Columbus officials warn victims, witnesses after ransomware leak of prosecutor files," *The Record*, August 19, 2024

A Tectonic Shift in the Landscape

In February 2025, amid other massive government layoffs under the new administration, CISA terminated hundreds of workers, approximately 10% of its workforce. The layoffs followed the firing of 130 probationary CISA workers in mid-February.

On March 11, CISA axed $10 million in funding for CIS, funds that were supporting both MS-ISAC and the Elections Infrastructure Information Sharing and Analysis Center. It simultaneously terminated its partnership with CIS to run the two info sharing and analysis centers (ISACs). In a statement regarding the cuts, a CISA spokesperson said that the work of MS-ISAC and EI-ISAC "no longer effectuates department priorities."[9]



The Next Steps

The axing of MS-ISAC will have profound effects on an already overtaxed and increasingly threatened sector. As adversarial nation states increasingly target state and local governments, the loss of services has potentially disastrous consequences on the sector of government most responsible for the maintenance of key elements of the country's critical infrastructure, including power, water, hospitals, schools, and more.

Speaking to *Recorded Future News* on March 12, Tim Harper, a former election administration official who now works for the Center for Democracy and Technology said the EI-ISAC and the MS-ISAC provide real-time threat-sharing and response coordination that election offices cannot replicate by themselves.

Losing that coordination leaves towns and counties to fight nation-state hackers on their own, he explained.

An option to reduce this risk is the formation of a new ISAC operating on a global level, in the model of existing Health-ISAC, IT-ISAC, and Food and Ag-ISAC, which are global private sector non-profit organizations operating at least partially funded with dues from members.

On the level of the local government offices, finding low cost and effective programs to continue protecting both systems and citizens has become not just vital, but a matter of mitigating serious risk to the nation's infrastructure.

9 Greig, Jonathan, "CISA cuts $10 million annually from ISAC funding for states amid wider cyber cuts," *Recorded Future News*, March 12, 2025,

The Essential Role of Security Awareness Training

Whether it is a hacker looking to pick up some ransom money, or an adversarial nation state working to undermine the security of American infrastructure, all cyberattackers need to find a way in.

The most common entry point (found in 70-90% of malicious hacking instances[10]) involves a human misstep, usually involving social engineering and, more specifically, phishing. This is not new. Since the beginning of computers, social engineering has been the number one way, by far, for bad actors to accomplish malicious hacking. Social engineering is someone (or a group) fraudulently posing as someone (e.g., friend, boss, etc.), something (e.g., police, tax authority, etc.) or some well-known brand (e.g., Microsoft, PayPal, your bank, etc.) the user trusts, and using that trust to get them to perform an action harmful to their company's (or government agency's) best interests. They are usually tricked into providing confidential information like login details, download a boobytrapped document, run malware, etc.

Each year, KnowBe4 analyzes the online behavior of users to determine a baseline of how many individuals, without security awareness training, are susceptible to clicking on fraudulent links in phishing emails. For its 2025 Phishing by Industry Benchmarking Report, KnowBe4 analyzed the behavior of 14.5 million users across various industries and sizes. The baseline statistics indicate a "Phish-prone Percentage™" (PPP) of 33% of users; in other words, more than one out of three computer users tested were likely to click on a bad link in a phishing email.

The sector had lower initial PPP ratings than the global average — 25.1% for operations with 1-249 employees, 26.8% for 250-999 employees, and 29.1% for 1000+ employees. The good news is that consistent and comprehensive cybersecurity awareness training works. According to the study, 90 days into an integrated approach of educational content and simulated phishing tests changed the outcomes noticeably, with the PPP in government organizations dropping to 19.3% in small organizations, 18.6% in medium sized organizations, and 17.9% in organizations with more than 1,000 employees.

After one year of cybersecurity awareness training, the PPP dropped even more significantly; for small organizations it dropped to 4%, for medium sized organizations, 3.7%, and for large organizations, 4.4%.

10 Grimes, Roger, "70% to 90% of All Malicious Breaches are Due to Social Engineering and Phishing Attacks," Security Awareness Training Blog, KnowBe4, March 31, 2025

Conclusion

It is evident that state and local government entities are facing a perfect storm of challenges: understaffed and underfunded cybersecurity departments, aging IT infrastructure, increasingly sophisticated threat actors, and now, the dismantling of crucial federal support systems.

The data is clear and concerning:

Ransomware attacks against local and state governments have **increased by 51%** in recent years

Malware attacks surged by 148% between 2022 and 2023

More than 80% of SLTT organizations operate with **fewer than five dedicated cybersecurity employees**

The **average ransom per attack has reached $872,656**, with total costs often exceeding $1 million per incident when including downtime and recovery expenses

The recent elimination of vital federal support such as the termination of MS-ISAC and EI-ISAC funding impacts the collective defense mechanisms these organizations previously relied upon. This leaves already vulnerable municipalities to face sophisticated, often nation-state-backed threats essentially on their own.

However, effective countermeasures remain available. Comprehensive security awareness training can reduce an organization's PPP from approximately 33.1% to just 4.1% after one year of implementation. This represents a cost-effective strategy that targets the primary attack vector—human error—which accounts for 70-90% of successful breaches.

The creation of a security culture across the sectors has accelerated and has become imperative. Effective cybersecurity training that addresses human risk management will prove to be a cost effective and powerful tool to meet the rising demands.

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit **www.KnowBe4.com**

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

KnowBe4

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