Stateline

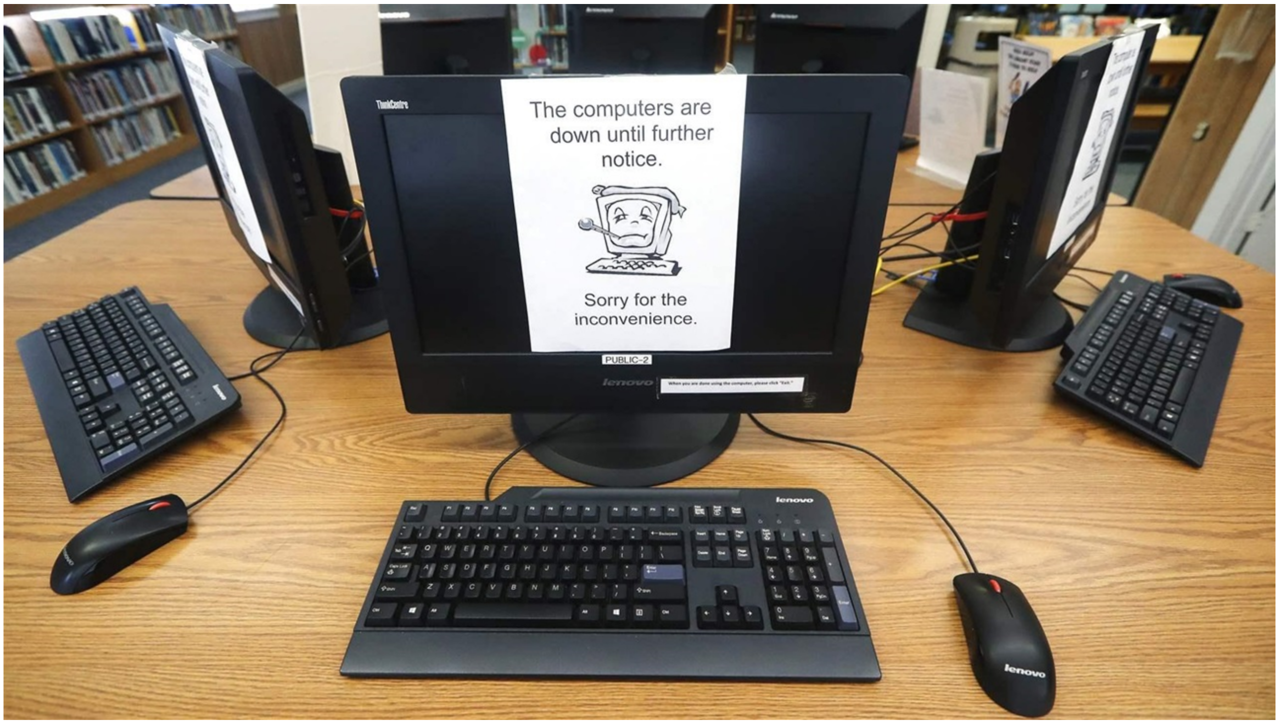
With Cybercriminals on the Attack, States Help Cities Punch Back

STATELINE ARTICLE February 4, 2020

By: Jenni Bergal

Read time: 6 min

Topics: Business of Government & Justice


The computers are down until further notice.
Sorry for the inconvenience.
PUBLIC-2
lenovo

Signs on a bank of computers tell visitors that the machines are not working at the Wilmer, Texas, public library in August, after cyberattacks crippled nearly two dozen Texas cities. Some states help local governments with cybersecurity.

Tony Gutierrez/The Associated Press

When the city of Lodi, California’s computers got hit by a ransomware attack last April, the strike disabled phone lines, forced police officers to write reports by hand and prevented workers from sending out utility bills.

City officials refused to pay the ransom of 75 bitcoins — about $400,000 — and instead turned to their cyber insurance company, which sent in a legal team and security experts to investigate and help return the system to normal.

“It took a lot of our energy and ended up consuming a great deal of time,” recalled City Manager Steve Schwabauer. “We ultimately filed a claim of about $250,000, and it’s not fully closed yet.”

State legislators later gave Lodi, a city of about 67,000, a half-million-dollar grant to upgrade cybersecurity.

> "Cybersecurity is a team sport.."
>
> **Meredith Ward, policy and research director**
>
> NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS

As cybercriminals increase their attacks against local governments — hundreds of municipalities and county agencies were hit in the past two years — some states are helping cities and counties better protect themselves.

States have offered election cybersecurity, responses to ransomware attacks that take computer systems hostage, training and other programs, according to a recent report by the National Governors Association and the National Association of State Chief Information Officers.

“It’s the right thing to do,” said Meredith Ward, the latter group’s policy and research director. “Cybersecurity is a team sport. States and local government and the private sector all have a role to play.”

But while 65% of states report that they provide some cybersecurity services to local governments, the scope varies widely. And other states aren’t doing anything to help, saying they don’t have jurisdiction over local governments or they lack money to spare.

“It’s very hard for most local governments,” said Alan Shark, executive director of the Public Technology Institute, a Washington, D.C.-based nonprofit that provides training and other support to local government information technology executives. “They lack the resources to adequately protect themselves. Yesterday’s fixes don’t work today. The cybercriminals are encouraged.”

But Shark said more states are starting to assist local governments in restoring their systems.

The states committed to collaboration are on the right track, the report by the governors’ and IT chiefs’ groups found.

Among them:

- Illinois created a program that helps local election officials improve their cybersecurity readiness and conduct risk assessments. It hired IT specialists to help local election offices beef up their security.
- Iowa is using a federal grant to offer counties cybersecurity vulnerability scanning and to pay for hardware and anti-malware tools. It also is piloting cyber projects with schools, cities and hospitals.
- North Carolina developed a partnership with the state’s National Guard and emergency management division to help local governments, school systems and community colleges recover data compromised during a cyberattack and provide training to help prevent future incidents.
- Pennsylvania partnered with the county commissioners’ statewide association to provide security awareness training and phishing exercises for all 150,000 county and state employees and contractors. Phishing victims unwittingly click on emailed links designed to get personal information, such as passwords.

“It’s about working outside your comfort zone and forging relationships,” said Erik Avakian, Pennsylvania’s chief information security officer. “We think this is really the path forward for all states. It’s something they should be looking at.”

Cyberattacks Spike

Cybersecurity remains a serious issue for state governments, as sophisticated hackers and cybercriminals are constantly scanning computer networks looking for vulnerabilities.

Those networks contain information such as Social Security numbers, birth certificates, bank account details and credit card numbers of millions of individuals and businesses.

But it’s especially hard for local governments. Just last month, for example, a small school district near Austin, Texas, with 9,600 students, disclosed that it had lost $2 million in a phishing email scam.

Local governments saw a spike in cyberattacks in 2019, and experts say it doesn’t look like they’re going to abate any time soon.

In the past 24 months, at least 370 cyber incidents affecting local governments and public safety agencies were publicly reported in 47 states, according to Aubrey Larson, a marketing manager at SecuLore Solutions, a Maryland-based cybersecurity company. That’s a 150% hike over the previous two-year period, she said.

In fact, the majority of publicized ransomware attacks in the United States last year targeted local governments, according to the report by the governors’ and state IT officers’ associations. Cities and counties provide essential services to residents and need access to their data to function effectively.

Ransomware hijacks government computer systems and holds them hostage until their victims pay a ransom or restore the system on their own.

In October, the FBI issued a public service announcement, saying state and local governments “have been particularly visible targets for ransomware attacks.”

Those attacks can be devastating.

Democratic New Orleans Mayor LaToya Cantrell declared a state of emergency in December after a ransomware attack hobbled the city. Officials had to shut down more than 4,000 computers and close municipal courthouses. The attack has cost the city at least $7 million.

Nearly two dozen Texas cities were targeted in a ransomware attack in August that led Republican Gov. Greg Abbott to order a “Level 2 Escalated Response,” which is just one level below the emergency management division’s highest alert. The state led the response and helped the cities restore their systems.

And Baltimore was hit by a ransomware attack in May that crippled thousands of computers and left workers unable to access online accounts and payment systems for weeks. City officials transferred $6 million from a parks and recreation fund to pay for cyber protections. In total, restorations and repairs cost $18 million.

Crossing Boundaries

Preventing and responding to attacks can be complicated when efforts involve jurisdictions that generally operate independently of one another.

“Some cyber incidents are truly becoming emergencies. [State and local IT officials] shouldn’t be exchanging business cards at that point,” said Maggie Brunner, cybersecurity program director for the national governors’ group. “ They should be doing it ahead of time. We’d love to see state CIOs know every single local IT director.”

In Pennsylvania, IT security chief Avakian said his agency held quarterly meetings with county IT officials to build relationships and find out about their cybersecurity needs.

“The fact that we’ve cracked this nut across jurisdictional boundaries is significant,” Avakian said.

Because of the collaboration, he said, the state was able to buy licenses for the phishing training exercise in bulk. The larger number of users lowered the cost per unit and saved the state and its 67 counties a considerable amount of money. He wouldn’t say how much.

“Now that we’ve done this, more people want to come onboard — school districts, cities,” Avakian said. “It’s kind of taken off.”

Michael Sage, chief information officer for the County Commissioners Association of Pennsylvania, called the cyber training and relationship the counties have developed with the commonwealth “a fantastic effort.”

“It has bolstered awareness and helped the counties understand where the threats are coming from, so they can stay vigilant,” Sage said. “The more we can collaborate and share, the better off we’re going to be.”

Stumbling Blocks

While some states have provided help, others have “little or no engagement with local governments,” when it comes to cybersecurity, according to the report by the governors’ and state IT officials’ groups, though the report didn’t list the states that are uninvolved.

That needs to change, they say.

“Cybersecurity is not just an ‘IT problem’ anymore,” the report said. “It is a critical business risk, homeland security and public safety threat, voter confidence issue and economic development opportunity.”

But there are impediments, said Ward, of the state IT officials’ group.

“Sometimes, states will say, ‘We don’t have jurisdiction to help local governments. That’s not our swim lane,’” she said. “Or localities will say, ‘We’re good, and we don’t need your help.’”

And Ward said some states say they don’t have the money to help local governments with cybersecurity. “They’ll say, ‘We’re just trying to keep our head above water ourselves.’”

The report recommended that states overcome those obstacles by building relationships with municipal leagues and county associations and raising awareness by holding cyber summits. States also should explore ways to save money by consulting local governments during the cyber contract planning process.

“You don’t need to have jurisdictional permission nor money to pick up the phone and call someone and build a relationship,” Ward said. “That’s something anyone can do.”

< Top State Stories 2/3 Top State Stories 2/4 >

AUTHORS

Jenni Bergal
Staff Writer
Stateline

RELATED

Topics	Business of Government, Justice
Places	Illinois, North Carolina, California, Pennsylvania

EXPLORE MORE FROM STATELINE

explore by place ▾

explore by topic ▾

About Stateline

Stateline provides daily reporting and analysis on trends in state policy.

About Stateline

Media Contact

Jeremy Ratner
Director,
Communications
202.540.6507
✉