SECURITY

More Than a Year After Atlanta Ransomware Attacks, Cities Remain Vulnerable

Government experts say state and local governments often lack the resources, skilled personnel and mindset to combat cyberattacks.

by Steve Zurier

Latest Articles

NASCIO Midyear 2019: How Ohio Government And State Schools Work Together On IT Initiatives

NASCIO Midyear 2019: How To Navigate The Role Of 'CIO As A Broker'

NASCIO Midyear 2019: 5 Essential Traits By Extraordinary CIOs

NASCIO Midyear 2019: Utah Prioritized Inventory Visibility After Critical Medicaid Data Breach

Steve Zurier is a freelance technology writer based in Columbia, Md.

More than a year ago, the SamSam ransomware attack took down multiple municipal systems in Atlanta. The city will pay up to **$17 million** to repair the damage, *The Atlanta Journal-Constitution* reports. The municipality responded by hiring Gary Brantley as its new CIO and pledging a multimillion-dollar effort to **modernize and protect the city against future cyberattacks**.

Atlanta has been moving forward, but other cities also recently suffered ransomware attacks. Recent cases include Albany, N.Y., Del Rio, Texas and Greenville, N.C.

So, what's going on at municipal governments?

Alan Shark, executive director of the Public Technology Institute, says **municipal governments remain more vulnerable to cyberattacks than their counterparts in the corporate sector**, where large corporations have invested heavily in cybersecurity since the Target breach in late 2013 that exposed the data of 41 million of the retailer's customers.

"I think municipal governments are much more vulnerable," Shark says. "Governments don't pay as well, so they find it hard to attract and keep good people. They also **don't invest in the hardware and the training**. And senior managers are from a different generation, they have to realize that there's no longer an option — **they have to invest in cybersecurity**."

3 Steps Cities Can Take to Evade Cyberattacks

NETWORKING

Risk vs. Reward with Internet of Things Deployments

DATA CENTER

Disaster-Ready State and City IT Systems Weather the Storm

Shark offers several steps cities can take to combat ransomware and other cyberattacks.

First, they should **have a third-party organization come in** and execute a risk assessment. Governments need much better visibility into where they are vulnerable and need to identify the critical data they need to protect. Too often they don't know how much data they have and where it's stored.

Second, local governments should **hire a CISO who has full-time responsibility for the security operation**. He says security has become too big a job for the CIO or IT department manager to handle.

Third, local governments need to **obtain cyber insurance**.

"With all the attacks, cyberinsurance is getting tougher to get; city governments need to look into this," Shark says.

To prevent ransomware attacks, Shark adds, cities also need to **step up cyber awareness training with the municipal workforce and sharpen their backup strategies**. He advises that governments isolate data backups from application backups. For example, he says data should get backed up sequentially on a daily, weekly and monthly basis, while applications should get backed up separately over the cloud.

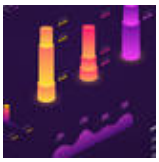
"By isolating the data from the applications, governments can get a better view of where the problems may come from and what needs fixing," Shark says.

VIDEO: *These are the cybersecurity threats that keep state CISOs up at night.*

Good Practices and Processes Required to Secure Networks

Cory Fleming, senior technical specialist for the International City/County Management Association, adds that city governments have to put good practices and processes in place, including insurance.

Trending Now



IT Managers Should Take Advantage Of Dynamic Graphics

IT Managers Can Facilitate Good Decisions With Strong Data Visualization

Public Safety Agencies Weigh Storage Requirements In The Face Of Video Demands

How 5G Networks Will Benefit State And Local Agencies

"Some municipal managers **still question why they need to carry liability insurance for cybersecurity**," Fleming says. "Many managers believe they are too small to be of interest to hackers. But less secure systems just make the hacker's job easier. And like in the case of Atlanta, systems could go down for weeks and run millions of dollars to repair. Governments need to take proactive steps and purchase insurance so that if they are hit by hackers, it's not taking down the budget."

Fleming points out that in a report ICMA released with Microsoft last year, the association laid out some of the barriers municipalities faced in developing more effective cybersecurity operations. Survey respondents cited the following as severe or somewhat severe barriers to improving cybersecurity at their organizations:

- **58.3 percent** cited the inability to pay competitive salaries for cybersecurity personnel
- **53 percent** cited an insufficient number of cybersecurity staff
- **46.5 percent** cited a lack of adequately trained cybersecurity personnel
- **52.3 percent** cited a lack of funds for cybersecurity

ICMA's Fleming adds that municipal governments have to **broaden their cybersecurity awareness efforts**.

"I was preparing a presentation for a local city managers' group in the Midwest, and the person organizing the program said we didn't need to cover cybersecurity because most municipalities have an IT department," Fleming says.

In fact the organization found, as part of the ICMA study, that the level of awareness training outside the IT department was lacking. When asked about the level of cyber awareness training, **71.4 percent** of those surveyed never offered cyber security awareness to citizens, **61.9 percent** never offered such training to contractors and **50.1 percent** never offered cyber awareness training to local officials.

"That's just the point," Fleming says. "Governments can't leave cybersecurity just to the IT staff — it's everyone's job."

SPAINTER_VFX/GETTY IMAGES

More On

LEADERSHIP POLICIES TRAINING

ANTI-MALWARE THREAT PREVENTION

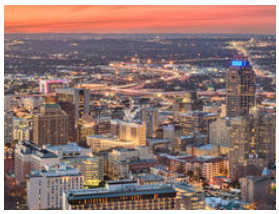
Related Articles

Security

How a Windows 10 Migration Boosts Agencies' Cybersecurity

Security

Ransomware Wreaks Havoc on Small Town, USA



Security

San Antonio Plans to Open Cybersecurity Center

SPONSORS