ATTACKERS TARGET GOVERNMENT

Public sector responds with new tools and growing cybersecurity sophistication.

Cyberattacks against governments, already a top concern for public sector IT professionals, took an ominous turn in August, when the Texas Department of Information Resources reported that 22 Texas cities had been attacked simultaneously by a single source.

Most of the targets were smaller, rural cities, according to the department, which in late August was leading recovery efforts in coordination with multiple state and federal agencies. Experts immediately pointed to the attacks as a new permutation in government's ongoing war with cyber crooks.

"What's unique about this attack and something we hadn't seen before is how coordinated this attack is," said Allan Liska, a threat intelligence analyst with security firm Recorded Future, in an interview with NPR shortly after the incident. "It does present a new front in the ransomware attack. It absolutely is the largest coordinated attack we've seen."

This latest ransomware evolution comes at a time when governments already face intensifying cybersecurity challenges.

States and localities have become a favored target for attackers, according to security experts. A new report from security firm Barracuda Networks says there have been more than 70 ransomware attacks on state and local governments in 2019, representing almost two-thirds of all publicly reported attacks this year.

In addition, new computing models are broadening and complicating the task of safeguarding government data and IT systems. The rise of mobility, increasing use of edge computing and IoT-connected devices, and migration to cloud platforms and services all expand the cyber threat landscape for public agencies.

New Attention on Risk

These and other factors are pushing states and localities toward more sophisticated cybersecurity approaches, including growing adoption of risk management tools, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework. These tools help agencies understand vulnerabilities, focus protection efforts on their most critical systems and implement security best practices.

Thanks to the risk management trend, cyberattacks increasingly are viewed as a business threat instead of a technology problem. As a result, cybersecurity is getting more attention from political leaders and agency management — and governments are responding to cyberattacks as they would other large-scale emergencies.

For instance, former Colorado Gov. John Hickenlooper declared an emergency last year when a ransomware attack impacted financial systems at the state's Department of Transportation, which processes around $100 million in monthly payments. Hickenlooper's executive action, thought to be the first in response to a cyberattack, enabled the state to use the same resources and processes that are triggered after a major natural disaster.

Louisiana Gov. John Bel Edwards took a similar approach this year when attackers hit several local school districts in his state, mobilizing the Governor's Office of Homeland Security, Louisiana State Police and National Guard, statewide Office of Technology Services, and academic and private sector experts. And Texas Gov. Greg Abbott ordered a "Level 2 Escalated Response" after the August coordinated ransomware attack in his state — the second-highest level of Texas' four-step emergency response protocol.

Growing attacks on local governments are also prompting more states to share cybersecurity resources with cities and counties. Michigan, for example, recently launched a CISO-as-a-Service program where state security experts provide maturity assessments and implementation plans for counties and cities.

"A few years ago, states started developing incident response teams, but states are now starting to say, how do we engage with locals before an incident," said Maggie Brunner, a program director for the National Governors Association (NGA), during a recent *Government Technology* webinar.

The NGA is working with states to strengthen their cybersecurity partnerships with local governments, she said. “States, having the cyber expertise that they do, are in a great position to create these economies of scale.”

More Powerful Technologies

Along with new techniques and partnerships, governments are implementing sophisticated new technologies for cyber protection.

“Many of the technology tools and services that governments are buying now have some level of artificial intelligence capability built into them,” says Teri Takai, executive director of the Center for Digital Government (CDG). “You can’t deal with the number of cyber threats on an ongoing basis without it.”

Results from CDG’s 2018 Digital States Survey show broad adoption of cybersecurity technologies such as intrusion prevention, security patch enforcement and data encryption enforcement systems. States also are deploying emerging security solutions like microsegmentation, security policy orchestration and application visibility.

Many of these tools automate security processes and procedures, helping ensure that software vulnerabilities are quickly patched and equipment is properly configured. They can also scan for unusual activity, enabling agencies to detect potential intrusion into systems and data.

Like states, city governments also have broadly adopted intrusion prevention and patch management systems, as well as tools to monitor and analyze threats to endpoint computing devices, according to CDG’s 2018 Digital Cities Survey.

The surveys also make it clear that government agencies continue to struggle to attract cybersecurity professionals into public service. State and city respondents both ranked cybersecurity as their biggest technology workforce need. The talent shortage is driving growing use of security services by government agencies.

A Continuing Challenge

Takai says the current spike in government-focused cyberattacks puts public sector CIOs and CISOs in a stronger position to argue for more security resources.

“The good and bad of it is that, as a CIO, I would be much more cautious and I would also be looking to highlight where I might need funding,” she says. “And in highly decentralized organizations, security can be a powerful argument for adopting an enterprise view of technology to decrease vulnerability.”

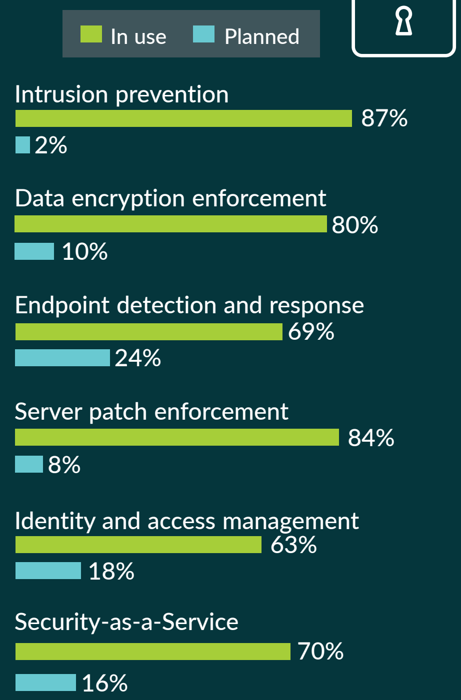
Even as states and localities have increased their sophistication around cybersecurity, these efforts must continue to expand and evolve. Indeed, one looming issue for CIOs and chief security officers is making sure advanced security tools can function together.

“The challenge is integrating these individual products into an enterprise framework now,” says Takai, “and understanding the cybersecurity architecture of the future.”

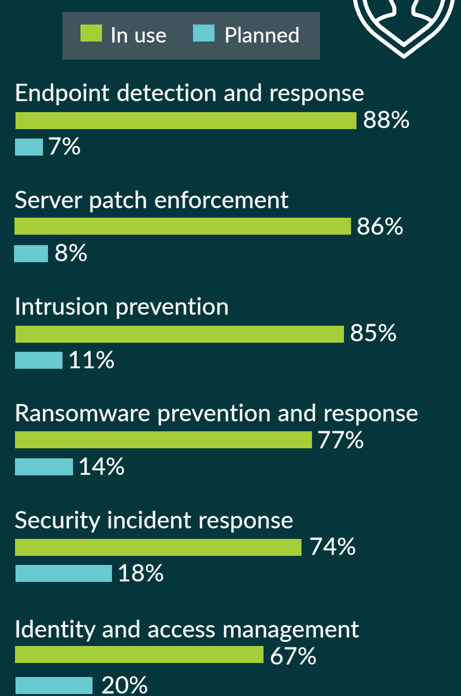
Addressing these issues and strengthening security capabilities will remain a top priority for CIOs — and increasingly their bosses — as cyber threats proliferate.

“I think we’re entering an epidemic stage,” said Alan Shark, executive director of the Public Technology Institute, in a recent interview with the *Washington Post*. “The bad actors have been emboldened.”

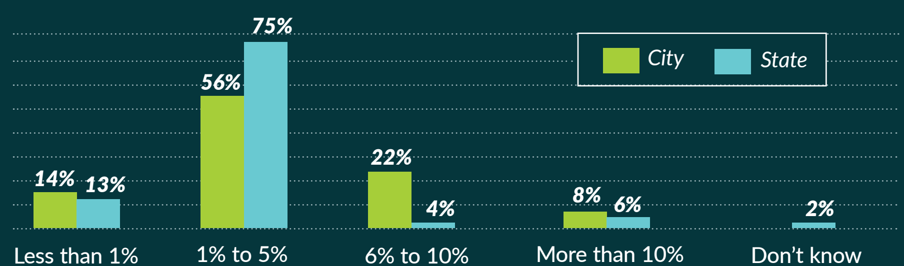
State Cybersecurity Measures and Initiatives



City Cybersecurity Measures and Initiatives



Percentage of Technology Budget Spent on Cybersecurity



Source: CDG 2018 Digital States and Digital Cities Surveys