To fend off hackers, local governments get help from states

December 12 2017, by Jenni Bergal, Stateline.org

The city of Mill Creek, Wash., has only 55 full-time employees and just one of them—James Busch—is responsible for handling information technology and cybersecurity. He worries about the growing sophistication of hackers and cybercriminals and the city computer network's vulnerabilities.

So when the Washington State Auditor's Office started offering local governments a free, in-depth evaluation of their cybersecurity systems, Mill Creek, a city of about 20,000 near Seattle, jumped at the chance in 2015.

"It was something we couldn't afford on our own," Busch said. "It was a great opportunity for us to see where we needed to improve."

Local governments, especially smaller cities, counties, police agencies and school districts, often don't have the resources to evaluate their cyber defenses or deal with cyberattacks. Yet just like states, their networks contain vast amounts of information about residents and businesses, such as Social Security, bank account and credit card numbers.

Some local governments say they can't necessarily rely on states for cyber aid because many are busy trying to deal with their own cyber preparedness. But some states, including Washington, Michigan and Virginia, have decided to extend help to the locals. They're providing training, sending in experts to uncover security vulnerabilities, or lending

a hand if a local government has been hit in a cyberattack.

"There's a growing awareness that the key to states being more prepared is ensuring that municipalities and counties are also improving their awareness," said Timothy Blute, a program director of the National Governors Association's homeland security division.

Local government chief information officers have become increasingly concerned about hackers. Just this week, hackers targeted Mecklenburg County, North Carolina, with ransomware and demanded $23,000 to unlock the affected data. County officials refused to pay and said it would rebuild the applications from scratch. But hours after that announcement Thursday, the hackers struck again.

Nearly a third of local government IT officers reported a spike in cyberattacks during the past 12 months, according to a 2016 survey by the International City/County Management Association.

Less than half of the local governments had a formal cybersecurity policy or standard, and only a third had a formal, written recovery plan for breaches, the survey found. IT officers cited the inability to pay competitive salaries and a lack of cyber staff and funding as serious barriers to achieving the highest level of cybersecurity.

State IT departments historically have focused their cyber efforts on their executive branches, and often don't have the relationships or infrastructure to provide cyber aid to local governments, said Alan Shark, executive director of the Public Technology Institute, a Washington, D.C.-based nonprofit that provides professional development and consulting services to local government IT executives. "The locals don't have much faith that they'd get a lot of help."

One option for local governments victimized in a cyberattack, Shark

said, is the Multi-State Information Sharing and Analysis Center, a federally funded group that tracks cybersecurity issues for states and local governments.

The center can offer assistance, either remotely or in person, and help identify how a virus or attack occurred, how to prevent it from spreading, and how to get the system back to normal, said vice president Brian Calkin. This year, the center has assisted about 90 local governments that were attacked.

Michigan is one state that's trying to change that image for local governments. It is the only one that has created a volunteer team of highly trained cybersecurity experts from the public and private sectors who can provide local governments technical assistance if they get hit by a cyberattack or data breach.

And in May, Michigan launched a one-year pilot program designed to help local governments identify their biggest cyber vulnerabilities, create a plan to fix them, and then put solutions into practice. "Cybersecurity is a concern for everyone no matter what size you are," said Rajiv Das, Michigan's chief security officer. "If the counties are cyber secure, it helps us when we exchange data with them—and vice versa."

Michigan's pilot started with five local governments and has since added four more, Das said. The program has cost the state Department of Technology, Management and Budget about $200,000, most of which pays for a consultant to work with the locals.

While the pilot is free for local governments through April 2018, participants will need to fund the program themselves after that, Das said.

Virginia also helps local governments strengthen their cybersecurity by

making available a National Guard cyber brigade of experts to test IT vulnerabilities.

"This allows them to get an outside set of eyeballs to see what they've done and what they need to do to make them safe," said Virginia Secretary of Technology Karen Jackson.

Jackson said nearly a dozen local governments have participated in the program, which is free for them but is costing the state about $150,000. It started last year and will run through June 2018, unless it is renewed.

In Georgia, officials plan to offer local governments training through the Georgia Cybersecurity Workforce Academy, which started last year to teach state IT security employees how to build a secure cyber program and respond to an attack. Next year, that training will include local governments, said Stanton Gatewood, Georgia's chief information security officer.

"The states have a duty to help the local governments," he said. "We're all in the same boat so why not mobilize and protect and defend each other?"

Washington state started offering local governments independent audits of their cyber defenses three years ago.

The reviews by contractors and state auditors and IT security specialists assess a system's vulnerabilities, perform technical tests to see if it can be penetrated, and recommend improvements. The audits take six months to two years and cost the state $150,000 to $300,000 each.

Funding comes from a 2005 voter initiative that allotted a bit of Washington's sales tax revenue to the auditor's office to conduct performance audits for local governments. The office later expanded the

mission to include cybersecurity audits.

So far, two cyber audits, including Mill Creek's, have been finished, and 10 are ongoing, according to program manager Peg Bodin.

As a result of his city's audit, Mill Creek IT manager Busch said, officials there have developed new cyber policies and now require cyber training for every employee.

The lessons learned came in handy. Just a few weeks after the training, Busch said, the city got phished "big time." But an employee who received the phony email, which looked as though it came from a colleague, didn't open it and instead reported the incident.

Having an independent assessment also can be useful politically, Busch said.

"We can use it to go back to elected officials and say we need to upgrade and put in security measures," he said. "It helps lend some credibility and some oomph behind what you're saying, especially when you're a one-man shop."