Cybersecurity—It's All About Relationships

Katherine Barrett
& Richard Greene

With the list of ransomware and other cyberattacks on local government getting longer and longer, the importance of bulking up cybersecurity protection is escalating—even as COVID-19 and the country's economic downturn drain resources. In researching this column, the most repeated phrase we heard about the potential for attack was "It's not if, it's when."

While it may be possible to put off other problems, no government can afford to ignore cybersecurity. "It's not like you can say we're small and nobody will pay attention to us," said Teri Takai, co-executive director of the Center for Digital Government.

As she and fellow co-executive director Phil Bertolini told the National Association of Counties (NACo) in early March, the growing dependence on technology to link with citizens, the sheer number of devices connected to government networks, and constant technological changes all present opportunities for entrepreneurial criminals who use round-the-clock software probes to find weaknesses in government systems.

"There might be several hundred attempts in any given day," said Meredith Ward, director of policy and research at the National Association of State Chief Information Officers (NASCIO). "Someone will be knocking on your door all the time."

Still, many local governments are woefully unprepared for a cyberattack. A 2018 survey from Public Technology Institute (PTI) noted that only 35 percent of local government IT departments had a strategic plan for cybersecurity.[1] Last year, another small survey referenced in a report by PTI and the National League of Cities (NLC) revealed that 80 percent of respondents identified lack of funds as a barrier to achieving the highest possible level of cybersecurity.[2]

With limited resources, an emphasis on partnership and teamwork is growing. In January 2020, NASCIO joined with the National Governors Association to report on ways states can send cyber life preservers to local governments.[3] For example, the State of Indiana provides a cybersecurity incident response template for local governments; the State of Colorado facilitates information sharing on cyber threats; and the State of Pennsylvania works with counties to provide employee cybersecurity training.

In March 2020, NLC provided additional guidance in a report detailing cybersecurity partnerships and resources available to cities from states and other sources.[4] The report includes comprehensive 50-state information on a limited set of cybersecurity topics. It also includes information on non-governmental sources of help such as universities with cybersecurity programs.

At the county level, in addition to other efforts, this spring NACo launched its own information-sharing web resource called County TECH Xchange, which has both general and cybersecurity information.

Another invaluable national resource is the Multi-State Information Sharing and Analysis Center (usually referred to as MS-ISAC), which is run by the nonprofit Center for Internet Security. "The membership is free," said Alan Shark, executive director of PTI. "They send

Many local governments are woefully unprepared for a cyberattack.

out bulletins sometimes twice and three times a day of threats and remedies, and they have tools available at very low cost. I'm surprised how many local governments are not members."

Rita Reynolds, chief technology officer at NACo, said about a third of counties are members of MS-ISAC. "Every county should be a member," she said. There is also an affiliated Elections Infrastructure Information Sharing and Analysis Center, which is focused on election security.

A theme that carries through these efforts is the importance of fostering teamwork. "It's all about relationships and now is the time to build those relationships," Reynolds said.

In an attack, "You're not necessarily going to have the time to start making calls if you haven't already made them," said Ryan Fernandes, director of technology services in the City of Weston, Florida.

Knowing what tools have worked for other locations, what threats look like, and how others have dealt with threats means that entities don't need to reinvent solutions on an often-small budget.

Publications providing intergovernmental information about cybersecurity are just a beginning, though. Each individual government still has a lot of work to do in finding the actual resources available in its area. Although about two-thirds of states offer some cybersecurity services to local governments according to the NGA-NASCIO report, the offerings are extremely varied and in many states are not aggressively advertised. Moreover, local governments are often wary about working closely with the state government. That's why the most successful state programs emphasize the importance of building trust.

"Only 30 percent of states are formally marketing their [cybersecurity services] to local governments. So, it's no wonder that local governments don't know what states can offer. The onus is on local governments to reach out and to see what's there," said NASCIO's research and Policy Director Meredith Ward.

"Just as you did to get a job with networking lunches and phone calls, you need to do the same thing here," said Tom Ray, the chief information security officer for the City of Berkeley, California. One of the biggest resources that local government officials have, whether they're from large governments or small, is each other. "It's knowing your region and knowing the IT directors in the other cities and counties," Reynolds said.

Only 35% of local government IT departments have a strategic plan for cybersecurity

Source: Public Institute of Technology, 2018

80% of local governments cited lack of funds as a barrier to achieving the highest level of cybersecurity.

Source: National League of Cities, 2019

The majority of states spend only 1-2% of their IT budgets on cybersecurity.

Source: 2018 Deloitte-NASCIO Cybersecurity Study, 2018

Some states provide models for sharing information. In the State of Washington, the state auditor has a waiting list of about 50 local governments that have volunteered to participate in its cybersecurity audit program. This program was facilitated by a citizen initiative in 2005, which provided ongoing resources for performance audits.

In 2014, the state audit office began to use some of the performance audit money for cybersecurity audits of state agencies. In 2016, it began to do the same for local governments. The goal of the audits, which are not publicly released, is to move the cybersecurity needle for the entity. "We don't give an opinion on how secure they are, but we give them some actionable recommendations. If they implement them, they will be more secure," said Scott Frank, the director of performance and IT audits in Washington. Other states have inquired about starting similar programs.

Governments that work together gain tremendous economies of scale and an opportunity to use the experiences of one local government to help others. For example, information the Texas National Guard Cyber Incident Response Team gathered in assisting Jackson County, Texas, with a ransomware virus allowed the state to help 23 other small towns respond to a similar coordinated cyber-attack. The Texas response, which involved multiple agencies, helped resolve the attack on those towns within two weeks, without the payment of ransom, according to the March 2020 NLC report.

One of the states that has been most intensely involved with local governments is North Carolina. When Maria Thompson became the state's chief risk officer in the Department of Information Technology about five years ago, she immediately saw several local cybersecurity gaps that needed filling. This was not just in the interest of localities, but also of the state itself.

"We are one cyber ecosystem. We are all interconnected. If there was a cyber-attack against our water systems or our 911 systems, they ride on the local government infrastructure. The quicker we can share the information, the quicker we can protect the citizen data and infrastructure that we're all stewards of," Thompson said.

One unmet need that stood out was a statewide incident response or disruption plan. Local governments were already aided by a state membership association, the North Carolina Local Government Information Systems Association (NCLGISA), but Thompson said, "I don't think the local governments in the past looked to the state as a resource. They felt they were on their own."

What has also helped is a memo of understanding that has been in place for more than five years that establishes the framework with which the North Carolina National Guard supports the state on cyber missions. This enables the state to call on the National Guard for a quick response to a local cyber incident without a formal emergency declaration.

Local information technology officials serve on incident response strike teams through NCLGISA, an organization that has helped state and local managers get to know each other. Randy Cress is assistant county manager and chief information officer of Rowan County, North Carolina, and a member of the NCLGISA IT Strike Team for the eastern region of the state. "Through relationship building you achieve the same vision. You won't get it perfect the first or second time, but it's continuing to evolve and always with the focus that we're one team," he said.

Another way that North Carolina provides help to local governments is by getting the word out about new threats. The state finds out what went wrong with an individual location, and that gets sent out to members of the NCLGISA, said Tom McGrath, cyber unit manager of the North Carolina Division of Emergency Management. This way, "Other places can harden their systems against a similar attack."

North Carolina also provides assessments, for a fee, to local governments, and in this election year it is offering free assessments to counties to remediate cyber dangers in county election infrastructure. There isn't time or money to provide assessments to all the state's 100 counties, so a prioritization process is in place to move those with the greatest need to the head of the line.

Assessments are only shared with the county itself, but trends are rolled up and shared with all the counties. By wrapping up the results of their assessments and sharing lessons learned, the state avoids exposing any individual government's potential weaknesses.

Many individuals at the state level talk about the importance of building personal connections with local officials before partnering on security services. The State of Pennsylvania, for example, started participating in meetings and workshops with the County Commissioners Association of Pennsylvania several years before it launched a program to provide cybersecurity training for county employees.

The program's success had joint benefits. "When you can work together through a shared services model, there's a great ROI. We're bringing this to the counties in one shot versus every county going out and buying their own solution," said Pennsylvania Chief Information Security Officer Erik Avakian.

Pennsylvania has been able to get good costs per unit based on the large number of software licenses purchased, and this has enabled it to cover the cost of counties' web-based security awareness training and follow-up exercises to reinforce that training. Going forward, the state is looking at other services that can be shared in similar ways, and it is also expanding shared training to cities and considering ways to also include school districts.

Governments that work together gain tremendous economies of scale and an opportunity to use the experiences of one local government to help others.

A key to making this program work was the relationships that had been formed between state and county officials. Counties were included in decisions about the vendor contract, and they made their feelings known about how they wanted the training and follow-up assessments to work. One important element for counties was that the individual county assessment results would be theirs alone and not shared with the state. "The feedback from the counties was, they didn't want the state to see individual county results. The county association could see the results, but we only provided a summary that we'd share with the counties and the state," said Reynolds, who was chief information officer of the county association of Pennsylvania before joining NACo.

The vendor contract was set up the way the counties wanted. "If we had just said the state is doing this, that would not have worked," Avakian said. "We had to establish the relationship and nurture it. That's the real recipe for doing this."

As the NLC report said, "Both local and state governments are increasingly realizing that they can't shoulder the burden of cybersecurity alone."

Katherine Barrett *and* ***Richard Greene*** *are principals of Barrett and Greene, Inc. and are co-authors of the recently released* Making Government Work: The Promises and Pitfalls of Performance-Informed Management. *They are: columnists for the Government Finance Officers Association; columnists and senior advisors at Route Fifty; senior advisors at the Government Finance Research Center at the University of Illinois in Chicago; consultants to the National Association of State Personnel Executives; special projects consultants for the Volcker Alliance; columnists for IPMA-HR; and fellows in the National Academy of Public Administration. Greene has been named chair of The Center for Accountability and Performance at the American Society for Public Administration. Their website is greenebarrett.com*

[1] "What's the current status of the cybersecurity program and environment in your local government?" Public Institute of Technology (pti.org/civicax/inc/blobfetch.aspx?BlobID=23009)

[2] "Protecting Our Data: What Cities Should Know about Cyber Security," National League of Cities, 2019.

[3] "Stronger Together: State and Local Cybersecutiry Collaboration," National Association of State Chief Information Officers and the National Governors Association, 2020.

[4] Citation not yet available