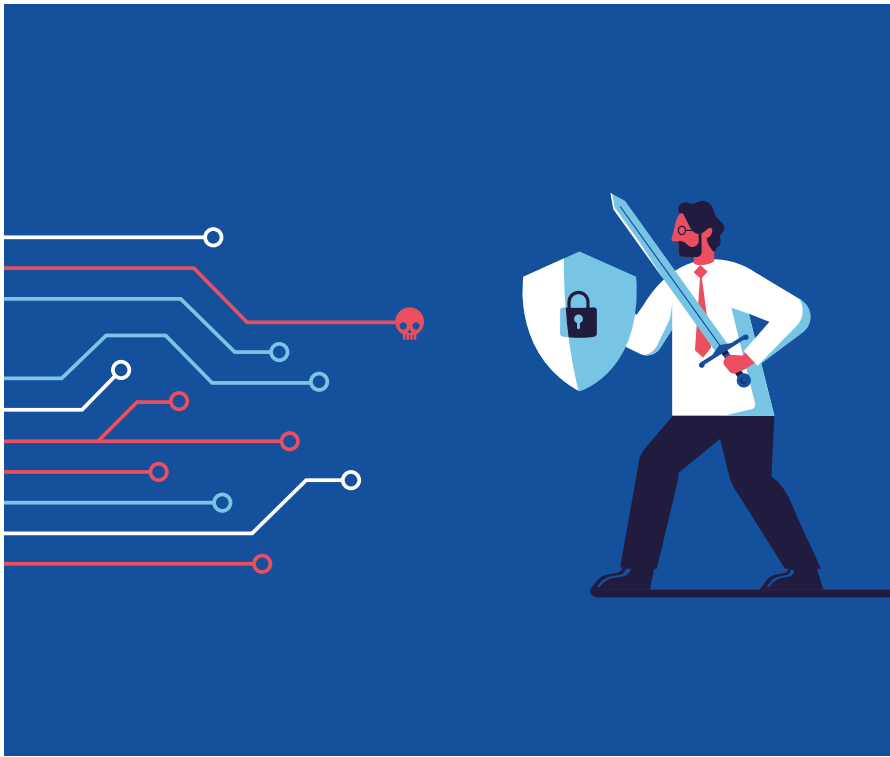




PERSPECTIVE

Fighting Cyber Attacks in Local Governments

BY KATHERINE BARRETT AND RICHARD GREENE

In the evolving world of cybersecurity, a host of new concerns and funding challenges are emerging. Artificial intelligence (AI) has given cybercriminals a powerful new tool—for example, the ability to make phone calls with voice impersonations of government leaders. But with these threats comes an expansion of state, local, and regional government collaboration.

The 2026 NASCIO-Deloitte Cybersecurity Study includes a survey of chief information security officers (CISOs) that highlights rising cyber-attack challenges—at a time of decreasing

resources. The survey includes an unsettling update to the list of threats that state and local governments face. While knowledge and attention to precautions are rising, 65 percent of state CISOs voiced concerns about the increased sophistication of attacks, compared with 29 percent in 2022.

At GFOA's 2026 annual conference, Steffanie Dorn, deputy county manager of finance in Greenwood County, South Carolina, emphasized that the trauma of a successful attack affects everyone in government. It damages productivity, diminishes residents' trust, and introduces a

host of managerial complications if government computers are temporarily disabled.

The issue goes far deeper than just IT staffers, as employees throughout government need ongoing training to reduce the risk that they'll enable a cyber attack by clicking on a dangerous link that can lead to exposure of private information or activate a virus. Departments must also be wary of easy access to internal administrative systems where private information can be compromised. This goes beyond concerns about providing unnecessary access to current employees, but to former workers whose passwords have not been deactivated—a common finding in state and local audit reports.

Growing concerns

While AI offers new tools for governments to use in dealing with cybersecurity, it also provides a powerful tool that works against government interests. AI enables attacks that are larger in scope and harder to detect than before. AI also changes the risk level for small governments, making it easier to scale a cyber-attack to many governments simultaneously.

At the same time, costs are rising, and budget worries are escalating. In 2022, 25 percent of state CISOs said the lack of a sufficient budget was a barrier that their states face in addressing cybersecurity challenges. That rose to 35 percent in 2024 and to 59 percent in 2026.

Worries also stem from federal funding cuts and uncertainty about future funding. One factor is a federal drop in cyber staff following DOGE cutbacks in 2025. Another is the 2025 move to fee-based membership for the Multi-State Information Sharing and Analysis Center (MS-ISAC), which was no longer receiving subsidies from the federal government. This member-guided organization works with "U.S. state, local, Tribal, and territorial (SLTT) government organizations" to provide "actionable threat intelligence and services ... to protect mission-critical systems."

That additional fee is particularly painful to small, under-resourced governments. If a small government doesn't pay the fee, reactive help may still be available, "but if you're not a paid member, it's very likely that you're not getting the daily updates and that kind of constant monitoring," said John Matelski, chief information officer (CIO) at the National Association of Counties.

The percent of CISOs who said they were "not very confident" or "not confident at all" rose from 35 percent to 63 percent between 2022 and 2026 when asked about the protection of information assets from cyberthreats "within local government and public higher education," according to the NASCIO-Deloitte survey.

State and local cybersecurity grant success and future prospects

One way governments are addressing this problem is through greater regional collaboration. As localities share more information with one another, more entities are teaming up to fight cyberattacks, according to Matelski.

The focus on regional resources emerges both from increased attention from the Cybersecurity and Infrastructure Security Agency and from MS-ISAC, which is run by the nonprofit Center for Internet Security. The State and Local Cybersecurity Grant Program, which was launched under the 2021 Infrastructure Act, also helped encourage states to work actively with local governments through grant funding focused on the development of greater local cybersecurity capacity.

That \$1 billion four-year initiative has been administered by states with the provision that 80 percent of the money would go to local governments, either through direct sub-grants to local applicants or the provision of services by the state itself.

While funds are still available through September 2026, the program's continued existence is uncertain, along with critical details such as the length of duration, amount

of funding, and potential changes in process or goals. In November 2025, the U.S. House of Representatives signaled its desire to keep the program going by a voice vote, but a Senate decision remained in committee at the beginning of July 2026.

According to the NASCIO-Deloitte survey, about a fifth of states have been moving toward a "whole-of-state approach" to cybersecurity, with a "growing interest in centralized state support for the cybersecurity efforts of local governments, public education and critical infrastructure."

New Hampshire is a good example of how a state with many small and often under-resourced towns and cities used the grant money to provide services that meet governments "where they are" in terms of their needs, reported long-time CIO Denis Goulet, commissioner of the New Hampshire Department of Information Technology. That approach, he said, has been more efficient than doling out the nearly \$15 million in grants the state received over four years to individual local applicants.

Through a contract with a New Hampshire nonprofit called Overwatch Foundation, the state has offered what it calls four "In a Box" programs. One has the goal of moving towns and cities to the use of a ".gov" domain name, which offers greater security through umbrella protections that come from both the federal government and the state. Another is focused on protections for K-12 schools, and the other two are aimed at drinking and wastewater systems.

Building relationships

One of the key points Goulet made is the importance of building relationships. As the state CIO with the second longest tenure, he was already seeking grants from the U.S. Department of Homeland Security through the New Hampshire Department of Public Safety several years before the pandemic. At the time, he joined the department's grant committee, and later, he said, New Hampshire became

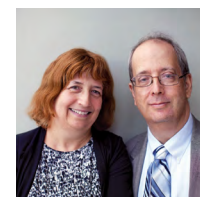
the first state to receive an SLCGP grant, which Homeland Security administered along with FEMA. "It wasn't an accident that we had the relationship. Relationships require building. We work to build them," he said.

While sufficient funding is absolutely needed to fight cybercrime, political and managerial leadership is also crucial. In Arapahoe County, Colorado, CISO Nikki Rosecrans describes herself as "very extroverted" and believes that's a major advantage in her job.

Colorado also has focused on the needs of local governments, and Rosecrans is an active participant in the monthly cybersecurity meetings hosted by the Secretary of State's Office and the Colorado Office of Information Technology. "Those are a crucial key to being able to exchange and share information," she said, adding that she is also involved in the Colorado Government Association of Information Technology and the Colorado Security Group, which is made up of members from both the private sector and government.

About a year ago, Rosecrans also started forming the Arapahoe County Cybersecurity Consortium, inviting cities within the county to participate in a quarterly information exchange. This has led to a new intergovernmental agreement between the county's seven cities, which was signed by the Board of County Commissioners on June 29, 2026. That will mean participating in joint planning, response exercises, and the sharing of training and cybersecurity resources.

"We're all faced with limited resources," Rosecrans said. "We recognize the need to be able to lean on each other. Our sister cities are just as important to Arapahoe County as we are to them." ■



Katherine Barrett and Richard Greene are principals of Barrett and Greene, Inc.