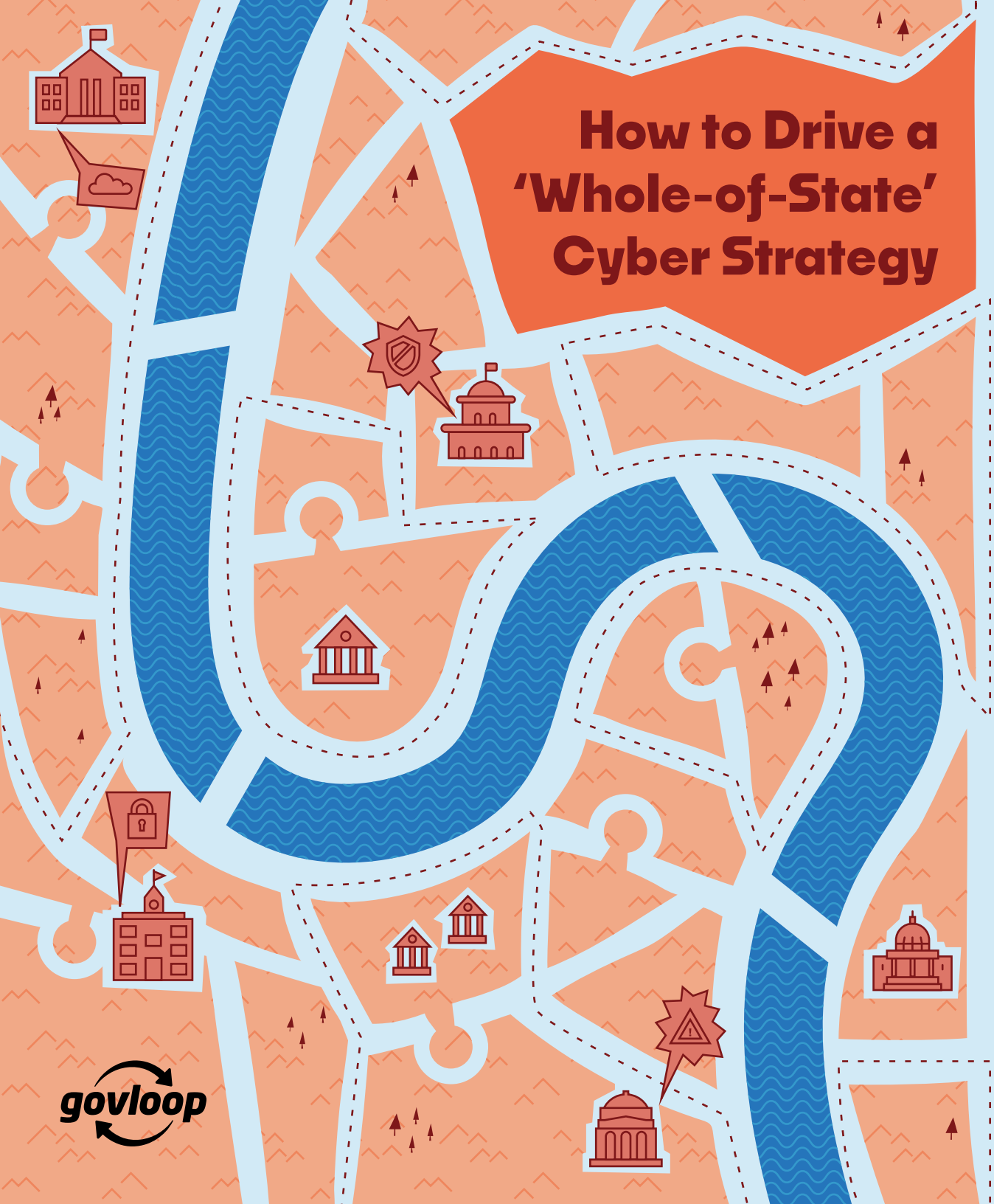


How to Drive a 'Whole-of-State' Cyber Strategy

At the state and local levels, the complexity and volume of cyberattacks is on the rise. At the same time, resources are stretched thin. In this environment, there's an urgent need for state and local governments to work together to manage risk.

A "whole-of-state" approach offers a collaborative strategy for cyber response. "At the end of the day, it's one team, one fight," said James Weaver, Secretary and State Chief Information Officer for the North Carolina Department of Information Technology.

He spoke at a recent GovLoop online training, along with Vinod Brahmapuram, Senior Director of Security for State, Local and Education at Lumen.

govloop

LUMEN®

Challenges to Effective Security

States face a number of stumbling blocks in their efforts to ensure a secure cyber environment; challenges that a whole-of-state approach can help them overcome. They include:

- **Rising digital interconnectedness:** Digital modernization creates new vulnerabilities. In the modernized IT landscape, "we are all connected," Brahmapuram said. "For example, a state health department has so much connectivity with the county and city systems. In this environment, we cannot be siloed."
- **Cyber labor shortages:** It's no secret that IT teams are shorthanded and that cyber professionals are hard to find. Building and sustaining the talent pipeline "is one of our biggest challenges," Weaver said. Agencies need a collaborative approach in order to more effectively leverage their existing personnel and technology.
- **Consistency in citizen service:** In spite of stovepipes, there's ultimately a common mission across all levels of state and local government: to serve the citizen. "The same resident is a resident of the state, a resident of the county, a resident of the city. It's the same person," Brahmapuram said. A whole-of-state approach responds to that reality, further securing citizen data.

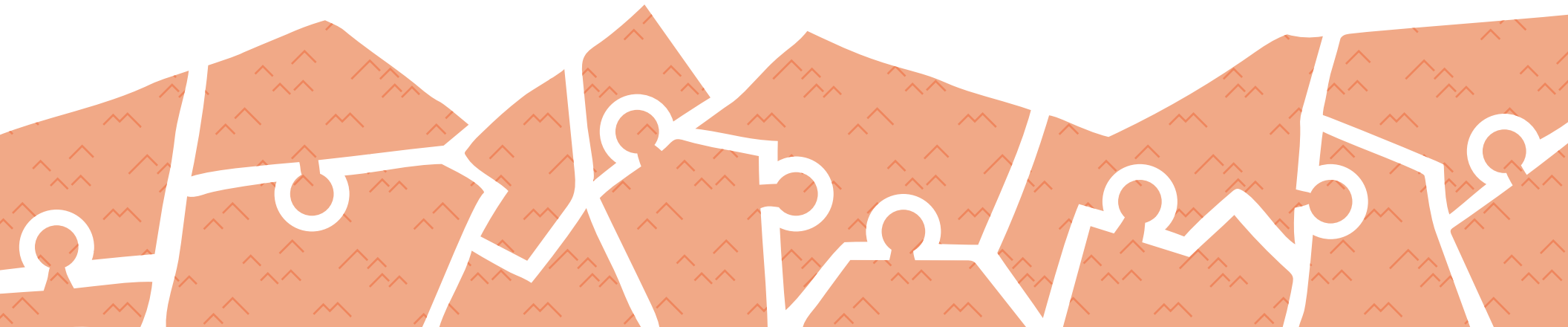
Toward a Collaborative Environment

As states look to secure data and systems in an effort to protect citizens and businesses, a "whole-of-state" strategy encourages a collaborative approach. In this model, state IT leaders team with city and county officials; they collaborate with higher education, critical-infrastructure providers, federal cyber responders and others to address cyber incidents.

North Carolina's joint cyber task force, for example, brings together law enforcement, emergency management, the N.C. National Guard cyber team and a local government IT strike team. With this approach, "we are very quickly able to pivot and provide the right level of support" in response to a cyber incident, Weaver said.

Brahmapuram said a whole-of-state strategy can be crafted in such a way that it meets the needs of diverse stakeholders, including both large and small municipalities that may be at very different places in their cyber journeys. When IT leaders work with stakeholders early in the process, they can maximize the impact of available resources for all parties.

Over time, this approach brings with it a culture shift – a pivot away from siloed thinking and toward a more cooperative mindset. "We have to marshal our resources a little bit differently than what we've done in the past," Weaver said.



Maximizing Impact

In North Carolina, a three-tiered approach helps drive effective implementation of whole-of-state cybersecurity, ensuring that resources align with needs across the state's 100 counties.

There are 40 counties in the Tier 1 category and 40 in Tier 2, representing less affluent (and hence less well-resourced) counties, with 20 counties at the Tier 3 level being the more affluent counties – those with "more capability and capacity," Weaver said.

For some Tier 1 counties, "the IT guy is probably doing three or four other things," he said. Tier 3, on the other hand, won't require as much support. "When I look at Wake County, where Raleigh is … we don't necessarily have to worry about them because they have the resources to go make things happen and get things done."

By aligning resources against need, a tiered approach helps ensure an effective whole-of-state strategy.

Key Strategies for Effective Whole-of-State

Empower Participants

Whole-of-state comes with certain risks, especially in how it may be perceived by key stakeholders. "There can be some misperceptions … where people think this is Big Brother trying to reach in," Brahmapuram said. Rather than appearing to dictate, an effective partnership will be one in which the voices of business owners help drive the process.

At its heart, cybersecurity is a business issue. "What that means is the business owners need to be empowered to make the decisions," he said. With this in mind, whole-of-state should be a collaborative effort aimed at elevating best practices, rather than just a policy pushed down from the top.

Plan for Disengagement

In cybersecurity, a whole-of-state effort works best as a targeted response mechanism, rather than as ongoing support. In North Carolina, "the joint cyber task force is not there to run day-to-day operations. It's there to resolve the incident, contain it, eradicate it," Weaver said.

That means state leaders will need to consider not just how to bring people together, but how to pull them back apart when the job is done. To address emerging cyber incidents effectively, people need to pull away from collaboration and return to their daily work. "There's a point in time where we have to disengage," Weaver said. "We have to cut that umbilical cord and bring those folks back onto the bench."

Maximizing Existing Resources

A whole-of-state approach asks state leaders and individual cyber teams to think about how they can best design their engagements for maximum benefit. To get there, it's helpful to create a roadmap that takes into account existing strengths and capabilities.

"This is about really pulling together every resource that you have, and maximizing those resources to the best extent possible," Brahmapuram said.

How Lumen Helps

Lumen combines government expertise and trusted technology in order to deliver next-gen citizen experiences. With an adaptive network, cloud-based services and built-in security, its platform can help state and local leaders build a foundation for digital transformation, with the ability to securely connect, proactively monitor and effectively defend against constantly evolving threats.

Learn more here.

How to Get Started on 'Whole-of-State'

In its 2022 cybersecurity study, conducted in collaboration with Deloitte, the National Association of State Chief Information Officers (NASCIO) lays out key actions for bringing to life a whole-of-state cyber strategy.

Advocate for a whole-of-state approach.

"Tighter collaboration with local governments and state higher education institutions provides greater security across the state," NASCIO argues, and CISOs and others will need to make that case relevant to stakeholders. Whole-of-state represents a new mindset, and top IT leaders will need to articulate and evangelize this vision in order to drive cultural change.

Explore tools to foster coordination.

Executive and/or legislative tools can help establish a whole-of-state coordination authority, such as a joint cyber task force or shared services initiatives. "CISOs can use these councils and task forces to build closer collaboration with local governments and public higher education entities," NASCIO notes.

Use federal grants to promote collaboration.

IT leaders should tap funding mechanisms that support a whole-of-state approach. For example, "CISOs can use the opportunity provided by the State & Local Cybersecurity Grant Program to build closer collaboration with local governments on cyber protections, including cybersecurity training at local government levels," NASCIO notes.

Thank you to Lumen for their support of this valuable resource for public sector professionals.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop