A **CENTER FOR DIGITAL GOVERNMENT** WHITE PAPER | TANIUM

4 Pillars of a Whole-of-State Approach to Cybersecurity

Introduction

A proactive, collective approach to cybersecurity — known as a "whole-of-state" strategy — breaks down silos and brings together multiple levels of government and education for a stronger defense. Coordinating governance and combining resources improves how governments share information, respond to incidents, fill workforce skills gaps and standardize cybersecurity tools.

Simply put, whole-of-state is "the way of the future," according to the Center for Internet Security.[1] The organization cites benefits including shared risk, economies of scale, consistency of service and streamlined visibility into the threat landscape.

Every organization has unique needs and goals. But successful whole-of-state strategy implementation is built on four main pillars:

Pillar 1: Information sharing
Pillar 2: Incident response
Pillar 3: Workforce development
Pillar 4: Tool standardization

The Whole-of-State Strategy

Policy, Funding, Support

Information sharing	Incident response	Workforce development	Tool standardization
• ISAC/ISAO • NIST/CIS/IS0 • Communication platform • Stakeholder input	• Cyber reserves • Regional SOCs • National Guard • Fusion centers	• Ongoing training • Virtual CISO • K-12 and higher education programs • Internships	• Security awareness training • MFA

Governance, Implementation, Validation

1

Pillar 1:
Information sharing

Prompt reporting of cyber threats, vulnerabilities and attacks on an organization allows other agencies and jurisdictions to prepare, prioritize and respond proactively. Collecting and assessing data over time can also help entities understand overall trends and prepare for the future.

"Whether or not you participate in any of the other pillars, do the information sharing," says Jennifer Pittman-Leeper, whole-of-state strategist for Tanium. "At a minimum, just talk. Get to know the folks who are trying to keep other levels of government safe."

> "At a minimum, just talk. Get to know the folks who are trying to keep other levels of government safe."
>
> *Jennifer Pittman-Leeper, Whole-of-State Strategist, Tanium*

Success story

The **NORTH DAKOTA** Joint-Cybersecurity Operations Command Center (J-CSOC) is the first mechanism in the United States to enable direct state-to-state sharing of cyber threat intelligence. Member states can exchange threat information and mitigations in real-time, provide early warning of threat actor activity, conduct multistate tabletop exercises and more.

"The J-CSOC is an innovative multistate project that is of critical importance," says North Dakota CISO Michael Gregg.[2] "If one state is being attacked, the others will most likely be targeted next. This allows us to rapidly exchange threat information to protect the state of North Dakota before it impacts our citizens."

Information sharing costs little to nothing. Organizations need a communication platform, a way to share indicators of compromise (IOCs) broadly and a strategy to mature information-sharing capabilities over time.

Use a real-time communication platform. Organizations must be able to rapidly share information with each other in the event of an incident or as part of an ongoing dialogue. Email is too slow. A comprehensive communication platform that facilitates internal and external conversations lets people share and organize information. Ideally, the platform should include phone, videoconferencing and chat messaging as well as task management, file sharing and other capabilities.

Participate in information sharing and analysis organizations (ISAOs). Sharing IOCs with the federal Multi-State Information Sharing and Analysis Center (MS-ISAC) and state ISAOs helps disseminate information more widely. These resource centers also publish advisories, provide incident response and remediation support, and publish best practices for improving cybersecurity.

Embrace automation. Automation is vital to keep pace with today's threats. Automated responses to threat intelligence can begin with simply ingesting IOCs from MS-ISAC. Over time, organizations can add security information and event management (SIEM) tools and security automation, orchestration and response (SOAR) capabilities.

Take action

Start meeting with people.

Involve everyone. Learn what they need and let them be part of the solution. Remember to include public information officers, vendors and nonprofits such as the National Cybersecurity Center.

"Go talk to people where they are instead of having them come to you," says Arizona CISO Ryan Murray.[3] "We've found that physical road shows, where we go around the state, have been incredibly successful."

Identify your existing communication platforms.

If most stakeholders are already using a specific tool, standardize that platform rather than using several or adopting something new.

2

Pillar 2:
Incident response

Whole-of-state incident response encompasses a range of roles and activities. In some cases, an organization may simply need advice or an objective assessment of a particular course of action. In other cases, an organization may not have the resources or experience to respond to an incident on its own, so it requires the full participation of other partner jurisdictions.

"The sooner you can react as a collective to contain an incident, the quicker you can get back to business — and the less damage and overall risk you have as a state," says Pittman-Leeper.

Whole-of-state incident response is most effective when the collective engages with all stakeholders, includes outside resources and regularly practices incident response plans.

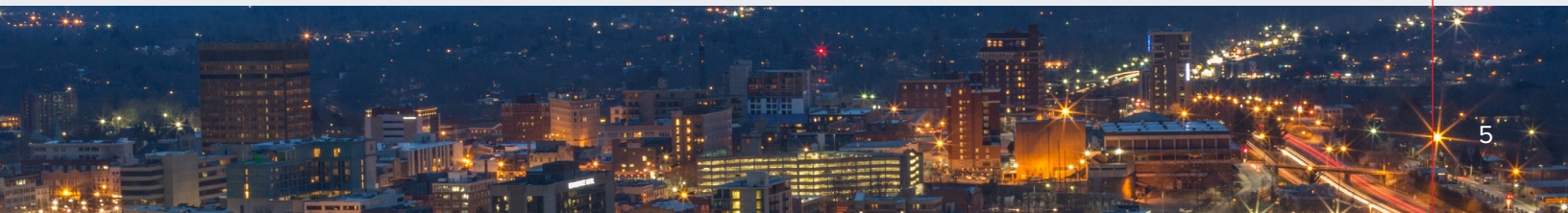
Engage all stakeholders in planning and practicing incident response. In addition to IT and cybersecurity teams, involve executives, critical infrastructure teams, public safety organizations, public information officers, risk managers and general counsel. States may also want to include their cyber insurance providers.

Success story

NORTH CAROLINA'S whole-of-state approach to cybersecurity includes mandatory incident reporting for all state and local government entities, data sharing through its ISAO and incident response through its Joint Cybersecurity Task Force, formalized by Gov. Roy Cooper in a May 2022 executive order.[4] Comprising the state departments of Information Technology and Emergency Management, the N.C. National Guard and the N.C. Local Government Information Systems Association's IT Strike Team, the Joint Cybersecurity Task Force has long provided cybersecurity support to any government entity in the state as well as K-12 public schools and community colleges.[5]

The task force's work ranges from repairing local government software to monitoring and protecting digital infrastructure for state elections. National Guard soldiers are also on call to lend subject matter expertise, resources and "boots-on-the-ground" support in the event of an incident.

"We have provided support across the entire state through the task force and our whole-of-state approach," says State Chief Risk Officer Torry Crass. "Cybersecurity is a combined effort. No entity can go at it alone, and we cannot underestimate the value of information sharing, collaboration and interpersonal relationships. They are critical in preventing and responding to cyber threats."



Get help from outside resources, including:

- **Fusion centers.** This is a collaborative effort of multiple agencies or disparate teams. It gathers, analyzes and shares threat-related information to support faster, better-informed incident detection, prevention, investigation and response than a lone SOC can provide. Every state has at least one fusion center; some regions have many.

- **National Guard incident response teams.** Many National Guards across the country have full cyber incident response teams that can mobilize quickly to serve as first responders during an incident at the local, regional or state level.

- **Private-sector cyber reserves.** These cybersecurity professionals work in the private sector and sign up to be part of an organization's cyber reserve program. If an incident occurs, the organization can call on these individuals for additional help or expertise.

- **Regional SOCs.** Texas, for example, has partnered with its community colleges and universities to provide SOC support to local municipalities.[6] The SOC monitors activity, alerts a municipality of suspicious activity and helps it respond in the event of an incident. In return, students in the participating colleges and universities get real-world experience with tools and incident response.

Practice and regularly update your incident response plan. Even the best incident response plan has gaps and cannot prepare organizations for all contingencies.

"We live in a new world, and we have new threats coming in," says Pittman-Leeper. "At some point, the bad guys will make it through, so you must have a plan and practice it regularly."

Incident response drills should include both internal staff and external partners such as critical infrastructure teams and public safety agencies so everyone knows exactly what to do in an emergency. Plans and drills should cover how and when each group will communicate, what the appropriate communication channels are, and what data can be shared in those channels.

Take action

Identify all potential outside resources in advance. This includes fusion centers, SOCs, National Guard, and cyber reserves. Determine their roles and limitations and where they would fit into incident response. Pre-screen and clear them before you need them. Build an incident response plan from there.

"Figure out what your state or local rules are regarding working with outside entities," says Pittman-Leeper. "Establish memorandums of understanding and non-disclosure agreements well before you're in the middle of an incident."

3

Pillar 3:
Workforce development

Cybersecurity needs grow more complex every day. Governments find it increasingly hard to keep up with demand. According to the National Association of State Chief Information Officers (NASCIO), more than 60% of CISOs report gaps in competencies among their staff.[7]

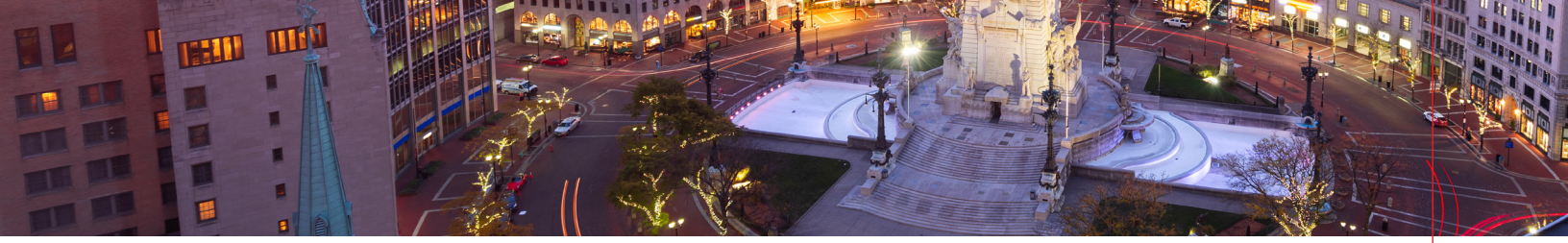
Whole-of-state workforce development strategies augment existing cybersecurity teams to meet current demand. They also help prepare qualified cybersecurity professionals for the future. The key to whole-of-state workforce development is to have a long-range vision and to be creative about collaborations that advance that vision.

Partner with K-12 and higher education to build a talent pipeline. By working together with K-12 systems and higher education institutions, organizations can ensure the workforce of the future has the right cyber skillsets.

Success story

INDIANA has developed a work-based learning program to reskill adults and prepare the next generation of IT workers. Launched in 2019, the statewide program is a joint effort between the Indiana Office of Technology (IOT) and the Indiana Department of Workforce Development. It reskills adults from occupations as varied as truck drivers and food production supervisors to work in operational IT and cybersecurity positions.

To overcome traditional barriers to hiring, the program shifts the focus from degree requirements for hiring to skills requirements for technical roles. IOT hires workers from the program to support security operations, enterprise resiliency, security-as-a-service, identity and access management, and more.[8] With paid on-the-job learning, 51 apprentices have been hired into the program and 28 have graduated.[9]



"You can't wait until a person's in college to get them thinking about a career in cybersecurity," says Pittman-Leeper. "We need to reach students when they're in grade school and make them aware of career options and career paths."

Organizations should also work directly with higher education institutions to make sure their cybersecurity and IT curriculums align with real-world needs and students have relevant skillsets when they complete a program.

Share and borrow talent. Smaller entities don't always need — or have the budget for — a full-time person to handle specialized tasks or act as a CISO. They may be able to pool resources and share someone's skillsets and expertise.

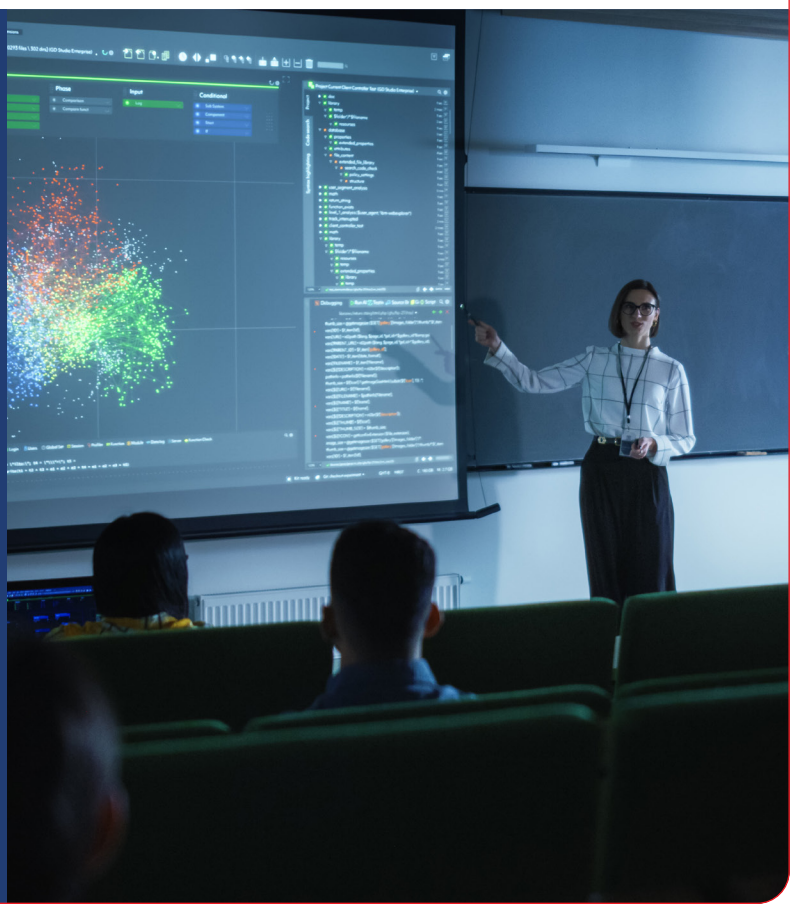
They may also be able to borrow skillsets from a peer organization. For example, if the core team isn't proficient in Python scripting or a particular security configuration, they may be able to invite someone from another team to help with that task.

Leverage regional SOCs to provide internship opportunities. Internships allowprovide a tremendous opportunity for people to understand what a career in cybersecurity might look like. They connect interns with practitioners in the field who can mentor them and engage them in real-world, hands-on learning.

Take action

Start talking with higher education.
Learn what cyber programs are available at your community colleges, four-year universities and other learning institutions. Identify gaps so educators can better map courses to real-world needs. Establish internship and apprenticeship programs to provide an on-ramp for early-career cybersecurity professionals.

Consult with the private sector.
Engage with private sector partners and vendors to help write curriculum and introduce new skills. They can provide best practices and lessons learned from other jurisdictions. Working closely with industry leaders will ensure your workforce is trained on the specific tools they will use to combat emerging cyber threats.



4

Pillar 4:
Tool standardization

Standardization reduces redundant costs, simplifies training, streamlines administration, and makes it easier to inventory and maintain systems. When a cyber incident occurs, standardization accelerates remediation.

Entities should start by standardizing a basic toolset.

"Some states want to get the fancier toolsets, but some smaller organizations don't have essentials like security awareness training, multifactor authentication or even visibility into their environment," says Pittman-Leeper. "You have to start at the beginning and bring people up to basic proficiency first. That does more for security than increasing the skill level of mature users or teams."

Include all stakeholders. Stakeholders are more likely to adopt new solutions when they're involved in decision-making. Listen to stakeholders. Find out what tools they currently use and what they need. If a majority already uses a specific tool, it may make sense to adopt it as the standard tool for everyone.

Establish a transparent process for choosing a cybersecurity solution. Make sure tool selection conforms to procurement

Success story

To provide maximum cybersecurity coverage, **ARIZONA** has created a standardized toolset not just for every state agency, but also for any locality that wants to opt in. The state provides 18 enterprise cybersecurity tools to state agencies and a subset of five basic tools to cities, counties, tribal entities and K-12s — all at no cost to these organizations. By having everyone on a single toolset, Arizona has strengthened security, saved costs, gained visibility across multiple levels and layers of government, and can coordinate across all components of cybersecurity and operations.

"It has brought us significant efficiencies and effective economies of scale," says state CISO Ryan Murray.[10] "Instead of many disparate groups saying, 'I want this specific tool,' or 'I need this specific problem solved,' we're all coming together to solve them at a larger scale."

Standardization has greatly streamlined and simplified the state's approach to cyber readiness, he says. "We don't have to manage 27 different tools in the state agencies and another 30 different tools in all the counties. We're using the same tools across the board — all managed by the state and supported by our local government partners."

rules and laws. Develop qualitative and quantitative metrics so that every tool is evaluated against the same requirements.

Align with known frameworks. The National Institute of Standards and Technology, the International Organization for Standardization and the Center for Internet Security publish rigorous standards and frameworks for cybersecurity. These frameworks are a tremendous resource for developing your own tool roadmap.

Embrace automation and AI. Even as you start by focusing on the basics, understand that artificial intelligence (AI) and automation are essential to any modern cybersecurity tool. As attacks increase in frequency and complexity, AI-based tools are the only way to adequately identify and address threats in real time.

Take action

Define needs and inventory existing tools. From there, identify gaps and redundancies.

Get started with basic tools. Security awareness tools and training and multifactor authentication are good choices because they are non-invasive.

"People represent your greatest threat vector. By starting with security awareness and multifactor authentication, you eliminate a majority of problems right off the bat," says Pittman-Leeper. "By identifying and inventorying your environment, you know what you have to protect."

Conclusion

Plans are great. Action is better.

Whole-of-state strategies coordinate information sharing, incident response, workforce development and tool standardization to achieve a more secure, resilient government for constituents and operations. Mastering all four pillars is a journey that states and localities can begin by taking a few simple actions.

"People like to work together to solve big problems," says Pittman-Leeper. "Local governments are clamoring to work with their state. Reach out to them and get started. It's more important to start doing something than to sit around developing the world's most perfect plan."

> "People like to work together to solve big problems."
>
> *Jennifer Pittman-Leeper*

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Tanium.

Endnotes

1. https://learn.cisecurity.org/ms-isac-handout-whole-of-state-cybersecurity
2. https://www.ndit.nd.gov/news/nd-founded-multi-state-cyber-command-expands
3. https://www.naco.org/events/whole-state-20-tale-two-states-and-counties
4. https://governor.nc.gov/news/press-releases/2022/03/16/governor-cooper-signs-executive-order-establishing-state-north-carolina-joint-cybersecurity-task
5. https://www.nationalguard.mil/News/Article/2233520/nc-national-guard-deploys-cybersecurity-response-force/
6. https://www.securitymagazine.com/articles/97462-texas-launches-regional-soc-for-local-cybersecurity-support
7. https://www.nascio.org/press-releases/cybersecurity-survey-of-state-cisos-identifies-many-positive-trends/
8. https://www.nascio.org/wp-content/uploads/2022/08/IN_CIOoffice.pdf
9. https://www.in.gov/iot/seal/
10. https://www.naco.org/events/whole-state-20-tale-two-states-and-counties

Produced by: gt CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Sponsored by: TANIUM | Public Sector

Tanium, the industry's only provider of converged endpoint management (XEM), protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. State and local governments, educational institutions, federal civilian agencies and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit **https://www.tanium.com/solutions/state-and-local-government/** and follow us on **LinkedIn** and **Twitter**.

ADOBESTOCK SHUTTERSTOCK.COM