SOLUTION BRIEF

TANIUM
Public Sector

Implementing a whole-of-state approach to cybersecurity

Early collaboration, clear governance and a mechanism for enterprise-wide validation are key pieces to a whole-of-state strategy.

Fragmented cybersecurity adds to IT risk

State, local and tribal entities are all grappling with how to reduce their IT risk. But many struggle with a fragmented governance structure, lack of streamlined policies and procedures and have little certainty of how to truly validate the level of cyber hygiene across a state — not to mention operating under tight budgets for talent and tools to keep up with modern cyber threats.

Enter the whole-of-state approach to managing cybersecurity.

A Whole-of-State architecture creates support for cybersecurity management by combining resources to find better ways of sharing information, responding to incidents, addressing workforce challenges, and standardizing tool solutions. This type of framework helps to bolster cyber defenses across all levels of government to provide more secured devices for constituents.

Barriers to a more secure government

When it comes to sharing resources to protect against cyber threats, government agencies and departments are all grappling with the same challenges:

LACK OF COORDINATION

Lack of coordination results in fragmented IT risk management across whole-of-state participants, leaving sensitive data and essential services at risk.

LACK OF VISIBILITY

Lack of visibility due to historic structure of decentralized cybersecurity — which gives no visibility for the whole of state — results in poor cyber hygiene, insufficient protection, and high IT security risk.

LACK OF GOVERNANCE

Lack of governance creates a void of interconnectivity for cybersecurity systems across all levels of government.

INEFFECTIVE IMPLEMENTATION AND VALIDATION

Ineffective implementation and validation means the program can't scale, and success won't be measured.

The result? A fragmented approach to cybersecurity, inefficiencies in budget spend on tools that don't integrate, loss of money and damaged reputation when ransomware attacks hit, and sensitive data and essential services are left vulnerable.

Did you know?

- Almost half of IT executives rate the relationship between local government IT and their state's IT cybersecurity practices as fair in a recent study
- Roughly 44% of ransomware attacks worldwide are now targeting municipalities
- 2,354 ransomware attacks happened against government organizations in 2020

Best practices for building a whole-of-state model

To successfully implement a whole-of-state cybersecurity model, states need to focus on the three key areas of governance, implementation, and validation - built on a platform of policy, funding and relationship building.

Step 1: Governance

- Start with established policies and frameworks such as CIS or NIST for laying the groundwork for what a robust cybersecurity program looks like
- Define what good cyber hygiene means to your state, and what your risk threshold is
- Create or look for grant programs to help fund a suite of standardized cybersecurity tools and services
- Create policy templates that can be leveraged by local organizations with a mechanism for enforcement over time

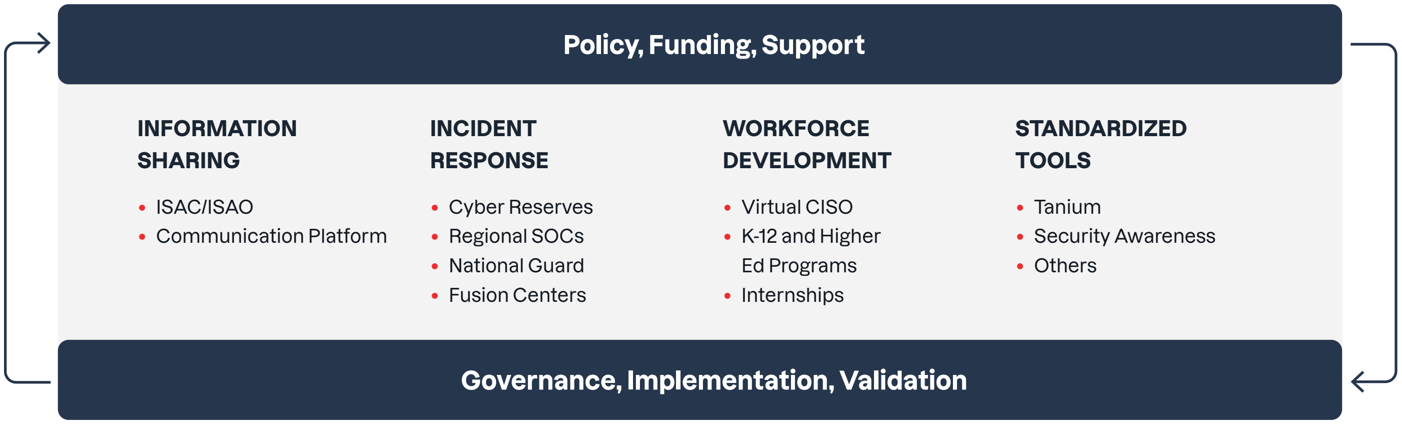
Step 2: Implementation

- Be sure you have the buy-in and set the proper expectations during the governance phase for ongoing success
- With standardized implementation practices (tool sets, etc.) it's much easier to measure risk across the whole-of-state enterprise
- Define a set of tools, how they will be selected, and how they should be used

Step 3: Validation

- Ensure that continuous care and feeding of your cybersecurity policies is built into the program (i.e. a mechanism for validation)
- Create controls that encourage policies to be followed, not changed, and are operating as designed
- Ensure automated compliance validation at enterprise scale without impacting participants

THE WHOLE-OF-STATE STRATEGY



Policy, Funding, Support

INFORMATION SHARING
- ISAC/ISAO
- Communication Platform

INCIDENT RESPONSE
- Cyber Reserves
- Regional SOCs
- National Guard
- Fusion Centers

WORKFORCE DEVELOPMENT
- Virtual CISO
- K-12 and Higher Ed Programs
- Internships

STANDARDIZED TOOLS
- Tanium
- Security Awareness
- Others

Governance, Implementation, Validation

How Tanium supports a whole-of-state approach

Tanium can provide best practices and expertise on policy, funding and building support structures; not only at the executive and technical level, but also between states and locals by identifying what support structures already exist, and how to build on them.

When it comes to tool standardization, Tanium's Converged Endpoint Management (XEM) platform validates your cyber posture with unparalleled visibility of all hardware and software assets, risk dashboards, role-based access controls and a source of truth for asset data across multiple department levels.

Read more about best practices for implementing a whole-of-state approach to cybersecurity at explore.tanium.com/wholeofstate/.

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 us at www.tanium.com/slg and follow us on LinkedIn and Twitter.