TANIUM

How to create a whole-of-state cybersecurity strategy

Whole-of-state cybersecurity requires three components — governance, implementation and validation

44%

of ransomware attacks worldwide target municipalities.

Introduction

Cyberattacks against US state and local government agencies have increased significantly in recent years. Roughly 44% of ransomware attacks worldwide now target municipalities. Ransomware struck at least 2,354 governments, healthcare facilities and schools in 2020 alone. Too often, these attacks succeed because municipal governments, K-12 schools, and other small government agencies lack staffing, tools, and expertise they need to defend themselves adequately.

Urgent need for better cyber hygiene

Why target state and local governments? Some of the attacks are probably random, the result of spray-and-pray approaches that just happen to hit state and local agencies.

In other cases, attackers might target agencies they suspect of having cyber insurance policies that will pay ransoms and any remediation costs. There's some truth to this. In fact, when ransomware victims decide to pay, state and local agencies often pay 10 times what commercial entities pay.

> **State and local agencies often pay 10 times what commercial entities pay for ransom.**

Attackers also might target municipalities and other small agencies because they know their defenses are weaker: Most states spend only 1–2% of their IT budgets on cybersecurity, while federal agencies and commercial businesses spend 5–20%. Finally, many local government services are considered essential, giving government leaders a strong incentive to pay ransom and resolve the attack quickly.

Recognizing that municipalities and other local agencies are short-staffed and underfunded, some state governments adopt a whole-of-state strategy, pooling resources and sharing information to protect government organizations from the city to the state level.

"State governments are increasingly providing services to county and municipal governments, including endpoint protection, shared service agreements for cyber defensive tools, incident response, and statewide cybersecurity awareness and training," the National Governors Association (NGA) and the National Association of State Chief Information Officers (NASCIO) wrote in their 2020 report *Stronger Together: State and Local Cybersecurity Collaboration*. Since then, the movement has gained momentum.

A whole-of-state cybersecurity strategy comprises three practices that fit together like the legs of a stool. You need all three to make it work.

- Governance and policy making
- Implementation
- Validation

Let's explore each of these in turn.

Governance and policymaking phase

Good IT leaders will look to established policies and frameworks such as the Center for Internet Security (CIS) or the National Institute of Standards and Technology (NIST) for laying groundwork for a robust cybersecurity program. These frameworks help establish standards for good cyber hygiene, determine acceptable risk thresholds, and define policies that can be enforced over time to realize those standards and address risks.

In general, it's a good idea to separate the work of policy making from the work of implementation. That way, policies can be thought through and developed based on industry-wide best practices, rather than to accommodate existing toolsets, practices, and habits of a particular IT team.

Who creates whole-of-state cybersecurity policies?

Whole-of-state cybersecurity programs are ultimately collaborations among various government entities, each of which is responsible for its own cybersecurity policies. Some of these government entities report to the governor, but many, including school districts and the state's MS-ISAC team, do not. In most states, these entities haven't worked closely together on cybersecurity initiatives before. So the first step is to bring representatives from these groups together, make introductions, and build trust.

It's important that this cross-organizational team be an independent organization focused on governance and not simply a tiger team of IT engineers who traditionally have been responsible for implementing cybersecurity controls themselves. Policymakers should be distinct from those who implement the policy decisions. This ensures that policies are rigorous, based on industry best practices and the latest threat intelligence, and that compliance, however well intended, isn't simply a matter of rubber-stamped reporting. Some states, including Florida, Arizona, and New York, have set up departments of homeland security to ensure a separate, policy-focused body can define and validate cybersecurity policies.

The CIS and NIST frameworks provide templates for writing comprehensive, detailed security policies. Creating such comprehensive policies is a laudable goal, but implementing these policies might be beyond the means of smaller organizations such as K-12 school districts in the short term.

An alternative approach is to define comprehensive policies but to also define a high-priority list of best practices for everyone to follow. This is the approach that the State of Arizona has taken. The state's cybersecurity team identified a "Top 18" list of CIS controls to implement, giving government entities of all sizes a manageable list of projects to focus on. Security practices improved, and no organization found itself overwhelmed by an exhaustive list of demands.

Risk assessment for policymaking

Risk management comes down to identifying and protecting the IT assets and processes that are most important for supporting an organization's mission. For a state's department of motor vehicles (DMV), for example, being able to securely store and manage applicants' records is of critical importance. So is ensuring that license fees paid by credit card are protected by systems that comply with PCI-DSS standards.

Even the most comprehensive whole-of-state cybersecurity program can't afford to protect every IT asset and IT process to the greatest extent possible. IT investments will have to be prioritized. So it's a good idea to measure risks across all organizations involved in the whole-of-state program so that teams can draft reasonable policies and allocate reasonable sources for protecting what's most important to each organization.

> For some helpful guidelines on measuring risk,
> **get the Tanium eBook;** *Expert advice on measuring risk.*

Special funding considerations for a whole-of-state cybersecurity program

Look for grant programs that might help municipalities, schools, tribal organizations, or the state fund a suite of standardized cybersecurity tools and services. In addition, the federal government offers states some short-term funding increases to address cybersecurity.

The whole-of-state cybersecurity team should also work to get state funding to support the whole-of-state cybersecurity initiative. A few states have already done this. With a dedicated, multimillion-dollar fund to draw on, they can purchase the IT equipment and training services that school districts and other organizations need, ensuring that purchases are made with volume discounts and that software and hardware are as consistent as possible across government entities. This additional funding provides another incentive for organizations to participate in the initiative.

Finally, it's worth pointing out that a successful whole-of-state cybersecurity program should save money for states, municipalities, K-12 schools, and other local organizations money. If improved security eliminates the need for multimillion-dollar ransom payments or eliminates outages that lead to lost revenue, those upfront investments will pay for themselves.

Implementation phase

This is the “action” phase of a whole-of-state strategy. In this phase, IT engineers and managers administer the policies developed in the policy phase. The implementation phase includes the following:

- Continuing collaboration among cross-organizational governance teams established during the governance phase.
- Selecting, purchasing, and deploying standard cybersecurity toolsets across multiple government organizations.
- Finding private consultation organizations to help with rollout and configuration of cybersecurity tools and implementation of cybersecurity policies.
- Prioritizing which cybersecurity policies to implement.
- Communicating successes to strengthen inter-organizational relationships and reinforce the value of collaboration.

This phase is also a common area for cybersecurity strategies to break down. That’s because, without sufficient coordination between the policy team and implementation team, policies might be too sweeping or too expensive to implement. Policies should be rigorous, even bold, but they should also be practical.

> **The implementation phase is a common area for cybersecurity strategies to break down.**

Continuing collaboration established in the policymaking phase

Now entities such as the state’s DMV or a municipality have the opportunity to fine-tune policies for their particular needs and convey those needs to the cross-organizational team. They can also share their experiences solving cybersecurity problems so that everyone has a chance to learn from everyone else.

Throughout this process, it’s important that every government entity understand that:

- The cross-organization team will make recommendations, but ultimately every government entity is responsible for adopting its own policies and implementing them according to its needs.
- State-level organizations might select, purchase, and provision IT tools, but they don’t control their daily use. Individual government entities are fully in control of the tools they use for monitoring, managing, and securing their own networks and other IT resources.
- Even if government entities are responsible for using cybersecurity tools, the state can help select and purchase them at bulk rates.

Recognizing the importance of vendors and private partners

When commercial companies buy IT tools, they have internal communications teams that can share information about the tools, offer training, and help with the overall adoption of the new technology.

Public sector organizations rarely have those resources. Vendors can help make up the difference with consulting and training services to ensure a successful rollout.

For example, a good vendor partner can help with outreach efforts across organizations by creating custom, integrated documentation. Because training and documentation are so important to rollouts, when state organizations evalute IT vendors, they should evaluate their training and consulting capabilities along with their software and hardware. States should ensure that training, documentation, and any other required communications are provided as part of the purchase, so that small, overworked IT teams never have to figure out new toolsets for themselves.

> **Ensure that training, documentation, and any other required communications are part of the IT tool purchase.**

The importance of communication for implementing a whole-of-state cybersecurity strategy

There is no such thing as overcommunication in this work. Teams should work transparently, and stakeholders should be regularly reminded about next steps and requirements. Regular communication about decisions, purchases, and training will help build enthusiasm for the project overall.

> **Regular communication about decisions, purchases, and training will help build enthusiasm for the project overall.**

When the **State of Arizona set up a program like this**, it made information sharing a program pillar. Government entities across Arizona now share information through the State Fusion Center. They've also set up Slack channels for inter-organizational communication. This communication makes it easy for government security teams to securely and anonymously post information about indicators of compromise (IOC) they've encountered and other useful threat intelligence..

Validation phase

To ensure that cybersecurity is not just “paper thin,” it’s important that the people responsible for validating the policy implementation don’t just check a box, self-attesting compliance. Rather, they should demonstrate compliance by generating reports that reflect the real-time status of all IT assets under management.

Comprehensive, real-time monitoring and reporting give stakeholders a clear view of the strengths and weaknesses of the strategy. And if reports end up showing that additional investments are needed, the factual, digital nature of the reports will be more compelling than self-attestations or general remarks.

In the validation phase, teams across the state will address questions such as:

- How do we know that the new security tools and practices are improving our cybersecurity defenses?
- Which parts of our cybersecurity program are working well or not?
- Which activities and investments should be prioritized next?
- Are there particular organizations that urgently need help? If so, how can other organizations help them out?

> Comprehensive, real-time monitoring and reporting give stakeholders a clear view of the strengths and weaknesses of the strategy.

Focus on goals and results

To validate the whole-of-state cybersecurity program, leaders need to identify goals and metrics they care about and ensure they are being tracked. Chances are, they’ve already identified these goals in the policymaking and implementation phases when making decisions about budget requirements, tool selection, and more.

Ideally, the goals and metrics you select should provide a meaningful measure of progress over time. By tracking these metrics, leaders and stakeholders should be able to determine whether the state’s cybersecurity posture is improving or weakening. If the metrics you track show improvement, but government entities are succumbing to more cyberattacks, it’s time to review your data and select more meaningful metrics.

Cumulatively, all the IT and security teams across the state work with a vast amount of data, everything from network addresses, device inventories, patch statuses, and AV scans, to security frameworks, lists of vulnerabilities, and threat intelligence feeds. To track and validate goals and metrics, you need to figure out what data you will collect and how you will collect it.

Establish three levels of reporting

To validate implementation of the tools and practices adopted for a whole-of-state cybersecurity policy, you need three levels of reporting:

- Technical reporting
- Executive-level reporting
- Enterprise-level reporting

Technical reporting

This is the lowest level of reporting, delivering insights about what's happening on networks and devices. Security operations center (SOC) analysts, network managers, system administrators, and other technical specialists rely on this daily reporting to understand the state of their networks and IT assets and to determine if anything needs prompt attention.

Insights from this reporting should be tactical. For example, it should be able to report on device inventories, patch status, threat status, and so on. If something needs to be fixed, it should show up at this level. Once it is fixed, that change in status should show up here, too.

Technical reporting is useful for measuring the state of every major security objective in the whole-of-state strategy. If an objective can't be measured, then new tools and instrumentation are needed.

Executive-level reporting

This next-level report shows the big picture of IT security at a particular government entity. It summarizes details from the technical reporting level and delivers insights about the overall state of security in ways that both technical and nontechnical leaders can understand.

When I worked with the State of Arizona on its whole-of-state cybersecurity strategy, we found it useful to provide green, yellow, and red visuals for this type of reporting. An executive should be able to glance at this report and see right away what areas are on track (green), have the potential for a shortfall (yellow), or need to be addressed immediately (red).

IT and executive leaders can use this report to:

- Direct the IT team to address issues that need more attention.
- Ensure that resources are allocated appropriately.
- Share their insights and experiences with peers in other government entities.
- Help the whole-of-state team generate the highest level of reporting — enterprise-level reporting.

Enterprise-level reporting

This summary rolls up all the executive-level reports generated from entities across the state and summarizes them in a useful way. It enables the governor, the legislature, and all team members across the whole-of-state initiative to understand the state's cyber-readiness.

Like executive-level reporting, enterprise-level reporting should use hard numbers without getting lost in the details. It should convey important information simply and clearly to ensure it's understandable by government executives who are responsible for a vast number of government issues, not just cybersecurity.

I recommend continuing the traffic-light scheme (i.e., green, yellow, and red graphics) to quickly convey what is going well and what needs attention.

This reporting may reveal previously overlooked risks. It serves several important functions:

COMPREHENSIVE INSIGHTS

It provides a comprehensive view of the state's cybersecurity posture (the overall resilience of its cybersecurity tools and practices). Most likely, these leaders have never had such comprehensive reporting.

PRACTICAL INSIGHTS

Leaders can see which efforts are going well and which might need extra attention. These efforts could relate to certain types of threats affecting all organizations, or problems specific organizations are experiencing.

JUSTIFICATION FOR FUNDING

The benchmarking and demonstration of progress should help whole-of-state participants justify funding from state and or federal resources.

Implement continuous reporting, not one-time audits

You might think of reporting and validation as being like an audit. But an audit represents the status of your cybersecurity posture at a point in time. That status might change in the next minute, when an infected device connects to the network, when a new security vulnerability is announced, or a new type of zero-day attack is seen in the wild.

To provide a truly accurate picture of the cybersecurity posture of any government entity, you need continuous, real-time monitoring and analysis. That kind of analysis is only possible with automation. IT security tools should be able to collect and report data continually and automatically, rather than requiring time-consuming, manual intervention by IT technicians.

With continuous monitoring and reporting, teams at every level can see the latest data without requiring a special task force to collect weekly or monthly metrics. The data might be shared weekly or monthly, but whenever it's shared, the data is up to date, providing an accurate picture of current cybersecurity strengths and weaknesses.

The importance of visibility for reducing risks

As the whole-of-state team's reporting capabilities become more established and you have more visibility into your security posture and operations, a few things will become obvious. You'll discover which products work effectively and which don't. You might also discover some products that are redundant or barely used.

Reporting provides the visibility you need to fine-tune your tool selection and purchasing strategy. By helping you pick the right tools, reporting helps make your cybersecurity investments more effective.

At the end of the day, a whole-of-state cybersecurity program is about risk reduction. Reporting lets you see the risks, take corrective action, and demonstrate the value of that work to your stakeholders.

Learn more

Cybersecurity threats continue to increase in frequency and sophistication. Fortunately, even small government entities can improve their security hygiene by participating in a whole-of-state cybersecurity strategy. By implementing these broad, inclusive strategies, states can ensure that every government entity has the best training, tools, and insights available to protect their data and infrastructure and to pursue their missions.

Take a deep dive into whole-of-state cybersecurity.

LEARN MORE