Prioritizing Cybersecurity for State Government

How a 'Whole of Government' Approach Benefits All

April 2023

Compiled By:
Heather West | Senior Director
+1 202.344.4597
HEWest@Venable.com

Daniel Wolf | Director
+1 202.344.4489
DSWolf@Venable.com

Zachary Martin | Senior Policy Advisor
+1 202.344.4393
ZPMartin@Venable.com

CENTER FOR CYBERSECURITY POLICY AND LAW

Table of Contents

Executive Summary

"Are we secure?" is a common refrain from state lawmakers and executive leadership to their state Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs). While the individuals asking that question expect a simple response, the answer is typically very nuanced.

Just like you can't make a building completely fireproof, it's impossible to completely secure all of a state's information technology systems, applications, and infrastructure. State CIOs and CISOs have to educate and work with lawmakers and agency leadership to tell them about taking a risk-based approach to cybersecurity so they can marshal their resources to protect what's most critical. And in some states, the number of resources that need protecting is growing as the central state IT agency is starting to offer cybersecurity and other services to local jurisdictions and school districts. This "whole-of-government" approach is nascent, but proving more popular as these smaller jurisdictions and institutions struggle to secure their systems under constant threat with dwindling resources.

State CIOs and CISOs know they are responsible for protecting the information of their constituents while also providing readily available, easily accessible access to a range of state services online. To get an idea of the unique cybersecurity challenges the public sector faces, and to inform this paper, we spoke to current and former state CIOs and CISOs, as well as other executives and experts. They detailed the challenges they face in addition to what they need to perform their jobs, and the skills necessary to be successful.

Public sector organizations must meet a higher bar when it comes to security. This responsibility falls on the people and agencies that governments entrust with their cybersecurity. They work to ensure that when John Q. Public wants to buy a hunting license, enroll a child in school, or apply for Medicaid benefits through the state's health department, the state can keep the transaction and their information safe.

This is important because the attacks just keep coming. Between 2014 and 2022, there were 822 public sector breaches affecting 175 million individuals.[1] In recent years, the number of breaches has slowed down, but the number of individuals impacted has remained steady with the total cost of the breaches estimated at $26 billion.

Public institutions like schools are at a high risk, according to a report from the Center for Internet Security, the Multi-State Information Sharing & Analysis Center, and the Nationwide Cybersecurity Review.[2] Local governments also have significant risk, and states are cutting back IT projects to reduce overall budget shortfalls.

As malicious actors are finding other targets more difficult to penetrate, attacks are shifting to local government and other small public institutions, like school districts. Most of these institutions don't have the necessary resources to combat the evolving

[1] https://www.comparitech.com/blog/vpn-privacy/us-government-breaches/
[2] https://www.cisecurity.org/insights/blog/report-k12-orgs-concerned-about-security-budget-threats

threat landscape, so some state governments are starting to offer services to smaller jurisdictions while other communities are banding together to pool resources and realize economies of scale.

These continuous attacks and resource challenges are leading some states to rethink how to provide cybersecurity services, and that was reflected in our interviews with current and former CIOs and CISOs. In the past, a central state IT agency would provide services to other state agencies. This approach has left local governments and other public institutions on their own – with fewer resources amid increasing threats -- when it comes to cybersecurity. Some states have realized this challenge and are starting to use a "whole-of-government" approach to cybersecurity services. A whole-of-government approach enables the state IT agency to provide services to state agencies, local governments, and other public institutions, relying on increased scale and visibility to threats to protect their state at all levels. This approach is not without its own share of challenges, but can ultimately lead to greater security across the state while reducing overall costs. Recommendations for implementing this approach include:

1. Establish whether existing laws allow a whole-of-government funding model at all levels of the state for IT and cybersecurity; if not, enable this approach.

2. Ensure appropriate resources so that the state IT agency can serve a larger set of stakeholders.

3. Create a voluntary approach for providing services, rather than mandates.

4. Equip state CISOs to integrate across the state and with local governments.

5. Consider best practices for cybersecurity and ensure consistency when proposing and passing state legislation, including legislation that would impact a broader set of constituents than just state government employees and systems. (*Additional recommendations can be found in the appendix*)

State cybersecurity priorities are diverse, including implementing zero trust, vendor management, and emerging issues like artificial intelligence (AI). But eventually it all comes back to following fundamental cybersecurity tenets, such as effective risk management, protecting data, and using trusted software and services. Aside from these more technical considerations, these state executives also need to think about how to recruit and retain cybersecurity professionals, explain how they operate to other state leaders and learn what they need, create effective partnerships, and educate policymakers in order to bring them along.

About the Center for Cybersecurity and Law

The Center for Cybersecurity Policy & Law is an independent organization dedicated to enhancing cybersecurity worldwide by providing government, private industry, and civil society with practices and policies to better manage security threats. Established in 2017 as a 501(c)(6) nonprofit within Venable LLP's Cybersecurity Services group, the Center combines policy expertise with convening power at global, national, and local levels to bring industry leaders together with policymakers to form coalitions and launch initiatives that produce real-world outcomes. Applying a consensus-oriented, risk management-based approach, the Center seeks to demystify the complexities and dispel the confusion around cybersecurity by promoting pragmatic solutions and policy recommendations drawn from the perspectives and practices of those on the frontlines of securing digital infrastructure and information systems.

Methodology

To research this paper, the Center's team interviewed current and former State CIOs, CISOs, and other executives about their priorities and the challenges they face. In order to have honest and frank conversations, these interviews were conducted off the record. All interviewees were asked the same questions, which were edited to reflect their role and current position. Their answers were compiled, then we identified themes and commonalities across approaches, and the end result is this paper. While some examples are raised in this paper, they are not indicative of whether we discussed that example with someone from that state.

Introduction

State Chief Information Officers (CIOs) and state Chief Information Security Officers (CISOs) are under increasing pressure to enable a digital-first presence for their state agencies while also ensuring the highest levels of security to protect employee and constituent data. State IT leaders understand that their constituents want to interact with their state digitally, which means that state systems increasingly hold a great deal of important constituent data. Critical systems and infrastructure also operate digitally, and disruption can significantly impact people's lives. Despite the unique challenges for states, everyone expects their information to stay safe and their services to remain operational.

These unique challenges include the general inflexibility of state budgets, the manner in which a state chooses to fund technology projects, the state's tax structure, or the low tolerance for operational risk given the critical nature of government services. Also, some state constitutions may prevent a central agency from providing services to smaller jurisdictions.

Despite those challenges, state governments in recent years have become increasingly aware that cybersecurity risk is not limited to a state's enterprise technology systems, and that other important pillars of their state are left to fend for themselves. Most states have a central IT agency that manages services for state agencies, but local government, higher education institutions, K-12 public schools, and other institutions typically don't fall under that umbrella and must address the same cybersecurity challenges, with even fewer resources to solve them. This can leave critical public sector systems vulnerable to malicious actors across a state putting all state systems and constituent data at risk.

Taking a holistic approach to cybersecurity with a "whole-of-government" approach – which would include all state agencies, local government, and education institutions – could help solve some of these challenges. However, there are numerous legal, bureaucratic, financial, and programmatic barriers to such an approach. The approach outlined in this paper includes foundational steps for every state to take to secure their systems and ensure that states can offer services that are easy to use, free of disruption, and readily available to citizens. It also discusses a number of priorities from state CIOs, CISOs, and other experts.

For this paper, the Center interviewed current and former state cybersecurity officials and other executives to get a sense of the challenges they are experiencing and how they work with other state's executive leadership, other state agencies, and local government. Based on the interviews we conducted as well as our own research and public information, this paper will:

- Identify themes and priorities shared across states,
- Examine how some states have started to pool cybersecurity knowledge and share resources,
- Discuss key steps that every state should prioritize, and
- Suggest how state legislators can enable those priorities.

Our hope is that this paper will help inform the cybersecurity efforts of state policymakers and provide an evergreen roadmap for states to follow as they work to protect their constituencies.

The Vision

The director of accounts payable for streets and sanitation in Pleasantville, USA would like new accounting software in order to have better visibility into the amount of materials the village is using to fix its streets to better monitor costs. Jane S. Civilservant has done some research and has narrowed it down to three vendors, but can't move forward without going through a formal request for proposal (RFP) process, which will add time and complexity to the acquisition. Because she's not able to use the due diligence that other agencies within the state have already done, she must spend extra time and effort.

Just across the state border, John S. Infotech, the IT manager at a small school district, knows that hackers have been using ransomware and targeting education institutions. Multi-factor authentication (MFA) is one technology that can be deployed to secure their infrastructure and help prevent these kinds of attacks. The manager, however, is more used to helping set up laptops, manage the network within the buildings, and help with other general IT related tasks and not cybersecurity.

If their states used a whole-of-government approach, both of them would be able to go to a state website and see a list of vendor products and applications that have already been vetted and approved and see which best suit their needs and existing infrastructure. If the product is on the list, they can move ahead with the acquisition without an RFP and use rates that have already been negotiated by the state – saving time and money at every step of the process. Additionally, this approach gives the smaller agency access to technology and vendors that they might not normally have, as larger vendors might not bother to reply to RFPs from local governments. It also helps the agency choose a product that fits the necessary requirements and make an informed choice. Rather than kicking off a long process, they can begin discussing the rollout of the technology chosen to secure their systems quickly and at a lower cost.

The whole-of-government approach has not been widely adopted across U.S. states, but its use may be expanding. States wanting to set up this kind of shared service offerings need to be thoughtful when setting them up and communicate clearly with stakeholders and have necessary resources available to help those who need it.

This recent move towards a whole-of-government approach is driven in part by federal grant dollars that are allocated for local governments but distributed by the state. The Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency (CISA) have allocated $1 billion over four years to help states and local governments improve their cybersecurity posture with the majority of funds going to the smaller jurisdictions. One of the key components of CISA's State and Local Cybersecurity Grant Program (SLCGP) is that each state must create a cross-functional "cybersecurity planning committee."[3] Not only must that group include diverse stakeholders from state and local government, higher and K-12 education, and public health, it must also have representatives from rural, suburban, and high-population jurisdictions – a clear push toward a whole-of-government level of collaboration on cybersecurity strategic planning that was unprecedented in many states.

[3] https://www.cisa.gov/state-and-local-cybersecurity-grant-program

States are starting to set up different kinds of shared services offices to enable those dollars to flow more freely and to optimize the use of that money. It's also because attackers are going after the weakest point, which is often the smaller local governments who are less equipped to protect themselves in isolation. The state may have secure systems, but an outage or breach at the local level can still impact the larger state system, and attackers know that it can be easier to gain access to smaller targets that are integrated into the whole, which now is the local government.

A whole-of-government approach to IT can help ease the acquisition process for local governments and education institutions. States with a shared service office with an approved products list would enable these organizations to access to trusted and secure software and services at pre-negotiated rates. The products and services would have been vetted by the state previously and come from trusted providers. Instead of a months-long process with an RFP, states could potentially roll out new products and services in weeks. Programs to ease the procurement process, such as StateRAMP,[4] NASPO Valuepoint,[5] and the GSA IT Schedule 70[6] enable public bodies to benefit from the experience of other procurement and technology officials. This allows smaller jurisdictions to lean on the expertise of the program as well as the state IT agency, rather than attempting to evaluate technology themselves.

It's not just about easing the acquisition process. The IT manager at the local school who doesn't know much about MFA could also receive assistance from the state when implementing the technology. These shared services offices can answer technical questions when it comes to rolling out new systems at a lower cost than if the local agency was to go it alone.

This doesn't mean that states should rush into a whole-of-government approach to cybersecurity. First, states that are considering this approach should look at existing laws and policies to determine if it's even possible, as rules around spending may preclude this approach and legislation may be required to enable it. State leaders also must be mindful that local jurisdictions may feel that their choices are being taken away or they might have specific technologies in place already and won't want to replace it with another product. When rolling out this approach, states should take a phased approach, rather than a big bang where everything would shift over all at once.

States implementing a whole-of-government approach should consider:

- **Grandfathering existing technologies** - Just because a technology isn't on the approved products lists doesn't mean the organization has to replace it with something that is on the list. Any existing technology can be used as long as it fits the needs of the agency and meets the necessary security controls. Over time, these technologies are likely to either get vetted and added to the application portfolio or be phased out in favor of technologies that more easily scale and offer benefits across the state. However, there is not an urgent timeline for that work.

- **Establish a voluntary approach** – Local officials may not be thrilled with a mandate from the capitol stating they have to use a new service that may require wholesale changes. While a mandatory approach would bring uniformity, it could also breed resentment. These services should either be voluntary or only mandatory if a jurisdiction is bringing a new

[4] https://stateramp.org/
[5] https://naspovaluepoint.org/
[6] https://www.gsa.gov/technology/technology-purchasing-programs/mas-information-technology

service online. This may improve overall buy in from local officials and tamp down any resentment. Over time, the program will show clear value for participants.

- **Defining a process for new technology** – When new technology is being considered, there should be a vetted process for that technology to be approved and added to the list. These processes will give transparency to stakeholders, who can in turn trust those technologies that have been approved. It also helps vendors understand how to ensure that they can provide services across the state and incentivizes them to submit their technology for approval and use.

- **Easing procurement burdens** - Once a new technology is chosen by the smaller agency, the process of producing it from the vendor should be simplified with this approach. Instead of having paper go back and forth, the process should be digitized and the central IT agency and vendor should be notified and figure out an implementation plan once the local official makes the decision.

- **Finding consensus among stakeholders** – The state IT agency should have working groups of members from across the state that can help define the needs and requirements of the smaller jurisdictions. This will help build engagement and buy-in to the process, as well as ensuring that the needs of institutions and governments of all sizes are reflected in the program.

The biggest challenge with the whole-of-government approach is resources, since the state will be working across a broader set of stakeholders and infrastructure. Shifting funding towards this type of statewide system, even with grant funding available, can be daunting. The state IT agency will need to scale up its personnel and services to roll out this approach, and that will require sign off from the state legislature. However, this investment will drive significant savings and provide important tools that make the whole state more secure.

Additional legislation may also be necessary to enable the state to offer the services to the local officials. Some states may have a "home rule" in place, which means they can make their own decisions when it comes to various concerns, such as technology, and the state cannot mandate requirements. Policymakers may need to update existing laws to enable the state to offer services to other jurisdictions, but also ensure that the recommendations above are taken in order to phase this approach in and demonstrate clear value across the state over time.

Regardless of anything else, states rolling out this holistic approach to cybersecurity need to plan accordingly, communicate clearly with stakeholders, and make sure they have appropriate resources available to help out those local officials.

The Broader Role of State Technology Leaders

Being a CIO or CISO at a state IT agency is not an easy task. As states are undertaking a "digital first" approach to services, state CIOs and CISOs are working across agencies to help facilitate this change while also ensuring that systems are secure. Some leaders may look at cybersecurity as something that needs to be worked around and nothing more than an obstacle to meeting their agency's mission. This can result in de-prioritizing cybersecurity work, skipping important risk management steps, or creating "shadow IT" systems - which can lead to critical incidents at any level of the state.

The stereotype of a CIO or CISO may be an individual focused on technology over everything else. These people do exist, but these roles require additional skills outside of the technical services these agencies provide. As the Center researched this paper and spoke with CIOs and CISOs, it became clear that these roles require leadership and communication skills in addition to deep technical knowledge, and every current and former official we spoke to emphasize the importance of education and consensus building within their context. Ultimately, these individuals need to carry forward a strategic vision and set forth a culture that listens to stakeholders while also prioritizing the mission.

A good way to approach the security topic is by working as a business partner with diverse stakeholders across state government. Taking a "we're in this together" tactic and discussing how to best tackle the challenges and work together has benefited many, including some of our interviewees.

The CIO and CISO need to be cybersecurity champions to the non-technical stakeholder, helping people across the state appreciate the need for proactively addressing cybersecurity. And they need to understand how to enable the people working across their state, instead of simply locking technical infrastructure down.

Strategic Partnership

Clear communication and partnership will also go a long way to getting other state agencies and leaders to work together happily and willingly. It is clear that state CIOs and CISOs must undertake a clear and proactive approach to creating partnerships across state agencies.

Several leaders also spoke about the importance of planning and strategy in these partnership discussions. Instead of talking about how many attacks were thwarted, it is important to find consensus on the state's overall cybersecurity plan and priorities. A robust cybersecurity strategy is key in this discussion and a necessary piece of any agency's long-term plans. Linking the plan and cybersecurity to economic development has also proven successful for some states.

Discussions around how cybersecurity leaders can work with local business and government leaders to improve the cybersecurity infrastructure and offer robust services can be a boon for jurisdictions. It can also create jobs and help fill much needed positions in the cybersecurity workforce as state officials work with local schools and higher education institutions to train them for cybersecurity careers.

Risk management

Technology leaders can often be at odds with others in a state agency. There are those who see cybersecurity as an obstacle to be overcome or dealt with. To counter this, the successful CIO or CISO will talk about risk management and work with the other parts of an agency to mitigate risk. Technology leaders should come to other agencies as a partner and instill a culture of risk management. By taking this approach there is a greater chance that employees across the organization will see themselves as part of the solution and work to improve security as they do their job. Not every application or system needs to be locked down; instead, look at the risk of that system and put security controls in place that are appropriate to the risk. No one can manage risk away, but proactive and broad approaches to cybersecurity can give state and local leaders comfort that state and local governments are working proactively and responsibly to manage risk, allocate resources, and protect their systems.

Security staff have a reputation of telling developers what they can't do, instead of enabling their work. To improve security in state and local government, it's time to change the messaging. Instead of looking at cybersecurity as an impediment, it's time to look at it as an opportunity to educate on the basics of risk management. Good risk management can enable - not impede - work across the state.

Communication

Transparency and clear communication are key skills for these individuals. Documenting the potential risk of a system and explaining what needs to be done and why in a clear fashion is critical to obtaining buy-in from other state leaders. Having frequent stakeholder meetings to discuss challenges that agencies are experiencing and how to best remediate are important and will avoid unpleasant surprises or disagreements. At the same time, those meetings are an opportunity to inform stakeholders on the priorities for the state IT agency and how those will be introduced. This frequent, transparent communication also helps build consensus and partnerships.

Cybersecurity Priorities for States

There's an old saying when it comes to state governments: "if you've seen one state, you've seen one state." States approach their own operations very differently, and by design. Each state has different strengths, resources, and risks. Concerns can be diverse. However, in talking to state leaders, we found that there are commonalities among the concerns and priorities of state CIOs and CISOs. Each of these are areas where partnerships with other state agencies, local governments and institutions, and state legislatures towards a whole-of-government approach could show significant benefit to cybersecurity across the state.

Workforce: By far, the biggest concern for states is acquiring and retaining the best talent to secure and protect state systems. Worldwide, it's estimated that there are 3.4 million open cybersecurity jobs with more than 436,000 open positions in North America, according to ISC2.[7] States are competing for the best cybersecurity talent with companies, but they offer a mission-driven approach and clear impact that is often difficult to replicate in industry. The state CIOs and CISOs that we discussed workforce with are taking a number of different tactics to recruit and retain a workforce to fill these positions. These include:

- Working with State Colleges and Universities – Many higher education institutions are offering different degrees programs for cybersecurity. Some states even have Security Operations Centers that are ran through universities where students can get hands-on experience that can lead directly to jobs with the state. These partnerships also have the potential to foster a workforce pipeline serving other state stakeholders, like industry, who are often interested in helping fund these programs.

- No experience needed - Some states are also hiring individuals that may not have direct cybersecurity experience, but have general IT or other knowledge. While there is an increasing number of programs and certifications that will help

[7] https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

educate people in cybersecurity, bringing in diverse experience across IT and other fields can help solve problems in new, unique ways.

- Upskilling existing employees - State agencies are also upskilling existing employees by offering the opportunity to get certifications around cybersecurity. This continuing education helps their workforce remain up to date, which is critical because the cybersecurity field evolves very quickly.

- Job descriptions matter - Finally, states are spending time rewriting job descriptions for state cybersecurity positions. This has removed requirements such as how many words per minute can you type or requiring five-years of experience for an entry level job - neither of which are good indicators of the kinds of skills that someone will need to contribute to cybersecurity across a state.

By expanding cybersecurity work across additional parts of the state, and particularly educational institutions, states can foster their workforce and ensure that they have a healthy pipeline among their constituents to secure their state.

Data Protection and Privacy: Data protection is a fundamental step that the government needs to take to protect constituent information, and is a core responsibility of state IT leaders. Having a robust enterprise data protection strategy across the state means knowing what data you have, where it is stored, how it is classified, how it is backed up, and how it is being protected. Encryption is a critical step that needs to be taken to protect the information a government agency may store. More states are appointing chief privacy officers to make sure that agencies are doing what's necessary to protect and responsibly steward constituent data.

Trusted Software: It goes without saying that the digital work of state and local government requires software - and that protecting the state means that the software must be secure - that is trusted. Software management is a core role of any technology function, enabling agencies to ensure efficient and trusted software and services across their state. State IT agencies typically have a process where they review and vet any new software and then keep a trust software list. Having policies in place to make sure that government workers are only using trusted applications – be it on a laptop or other device, including smart IoT – is critical to protecting an organization's systems and infrastructure. At the same time, it is important to ensure that these trusted applications and devices are usable in order to prevent employees creating "shadow IT" systems and going outside secure options.

Mobile applications: For many state employees, using a mobile device is one of the primary ways they do their job, be it communicating with others via email and messaging apps or accessing applications or data from state systems or cloud platforms while on the go. There are divergent views on the security of mobile applications from state CISOs, but several raised the concern that employees might download unsafe or malicious applications that allow access to systems or exfiltration of data. Some think the app stores and operating systems of these devices are enough to protect employees. Others, however, take a dimmer view. With possible regulation of app stores coming, some state officials are concerned about the potential misuse of applications to gain access to systems or exfiltrate data. Officials warned to watch this space to make sure that, if the U.S. government deregulates mobile app stores, state IT leaders must plan accordingly and put safeguards in place to protect state systems.

Shadow IT: Without a way to find trusted software and mobile applications, organizations can sometimes devolve into shadow IT. This is where an employee or small group of employees buy or use an application or other IT system because it solves an immediate problem they are trying to solve, going around, or otherwise avoiding approved mechanisms. IT leaders don't like to tell their users that they can't do something, but shadow IT can lead to security problems if the right controls aren't in place. Instead, offer steps that individuals can take so the system in question can be reviewed and implemented in a safe way, or an alternative system can be found. This also offers an opportunity for state officials to offer alternatives that may already be on the approved software list, or other mechanisms to improve security for these purposes.

Securing Legacy Systems: State CISOs have difficulty securing older systems and applications that were not designed with cybersecurity in mind, which can make them more vulnerable. Protecting these systems is far more difficult than modern systems, requiring resources that may be better utilized elsewhere. This makes it critical to modernize these systems over time and to fund the systems that keep the state running at all levels, in order to ensure that they can be well protected from evolving threats. Many CISOs have roadmaps that detail when legacy systems are to be updated or decommissioned. While this is typically focused on hardware, officials also warned about concerns around legacy applications as well and making sure they are updated appropriately.

Modernization also requires a shift in mindset for state IT operations and policymakers. Instead of having capital expenses – such as buying new servers and other systems – modernization will likely involve new kinds of operating expenses, such as using cloud-based services and applications. CIOs and CISOs also need to educate lawmakers on this difference and why moving to an operating expense model isn't a bad thing. States should also consider developing a revolving fund to address up-front modernization expenses rather than simply rely on their state's general funds.

Zero Trust: Zero Trust is the cybersecurity buzzword of the decade, but industry and the federal government focus on the security architecture is making it popular among states too. Changing the security architecture of a state's network from the traditional model of perimeter security to the more flexible model of zero trust user and device authentication takes some time as states are rolling out additional monitoring tools and fine-grained authorization. A phased approach is generally the best idea for introducing the new technologies that enable zero trust, but can significantly improve the security of state infrastructure against sophisticated adversaries.

Multi-Factor Authentication: The use of stolen or compromised credentials remains the most common cause of a data breach today, and MFA can help combat that problem by requiring different authenticators to verify a user's identity. This also enables a Zero Trust architecture for the network. However, enabling MFA for state agencies can be challenging as some state employees don't want to use their own personal device and issuing an extra credential to every employee can be expensive.

Integrating with other organizations: State CISOs may have difficulty integrating their security systems with those of other organizations, such as local governments and private sector partners, which can make it difficult to share information and coordinate efforts to protect against cyber threats. Resources need to be made available so that organizations across the state have the technical ability to do the necessary integration. Legislatures should ensure that state CISOs are well equipped to integrate across the state and with local governments.

Public-private Collaboration: Best practices are often shared across sectors, and that is doubly true in cybersecurity. Attackers rarely use truly novel techniques, and the same thing that protects a mid-sized company will protect a mid-sized state

or local institution. Agencies and officials should encourage collaboration between state agencies and the private sector to share information and best practices that will improve cybersecurity. This information sharing is likely to both improve security and save money for the state. And other institutions can benefit too - the same threats can impact everyone across the state, regardless of where they sit.

Gaps in the State's Cybersecurity Risk Profile: The cybersecurity risk profiles across state agencies can differ widely. Add to that the risks from local governments and schools, and the profiles can increase exponentially. While this leads to a large number of risk profiles, there is commonality among them – for example, K-12 schools would have a similar risk profile across the state. State technology leaders need to create common risk profiles that reduce silos between schools, state, city, and county entities while still meeting the needs of a varied populace.

Performance Goals: Defining the risk is at the core of a CISOs job. One item they are finding that helps with this is the recently released performance goals from CISA. These help the government and businesses to determine which security measures are most needed to reduce risk. These are intended to be an approachable common set of IT and OT cybersecurity protections that are clearly defined, straightforward, and aimed at addressing some of the most common and impactful cyber risks. State and local governments should follow CISA's guidance to meet the appropriate security goals for their sector.

Consistency: Legislators should have consistent cybersecurity goals and guidance across their constituencies - from state and local systems to the best practices they pursue for their citizens. Utilize the best practices that have been proven effective in protecting people and infrastructure in the private sector marketplace. This makes sure that state IT leaders aren't working against other mandates, where other goals may be in tension with cybersecurity priorities. This is particularly important as more people bring their own devices to work, putting personal and employer data and applications in the same shared sandboxes.

Training: Some may look at annual cybersecurity, phishing, or privacy training as de rigueur, but this fundamental cybersecurity principle is critical. Threats are evolving and these trainings can keep employees abreast of the latest things to watch out for. On the privacy side, training is also critical, particularly as federal, state, and local data retention laws may vary and education is necessary.

Testing and tabletop Exercises: While a small number of state employees and officials tend to be directly responsible for cybersecurity across a state, every employee, official, and elected official needs to understand the importance of cybersecurity and how to prevent and respond to cyber threats. These are the worst-case scenarios, but states need to be prepared. What happens if your agency is a ransomware victim? What happens if your data center goes offline? Have you tested your disaster recovery plan? State and local jurisdictions need to make sure they test all of these plans to make sure they can recover their applications and data in these worst-case scenarios.

Future Proofing: There are any number of emerging issues that a state will need to think about in securing their institutions. For example, it's still early days for AI/ML but the use cases are growing exponentially, and the technology can help with workforce challenges. States are very interested in adopting the technologies, but hard data on what these systems can do can be difficult to understand. States would like to see more concrete data around the AI/ML models that vendors are offering and what results and efficiencies these systems can deliver. New technologies like quantum computing, too, can pose risks to established best practices to secure information like encryption. These issues aren't at the top of the priorities list for anyone we

talked to, but officials did share their concerns about their ability to proactively address them down the road given their existing resource constraints.

Policy Recommendations and Roadmap

A whole-of-government approach to cybersecurity can realize benefits for all the parties involved, but transitioning to this approach can be challenging. There are numerous policy and legislative steps that would likely have to be taken to enable this approach.

As a preliminary step, lawmakers need to see if a whole-of-government approach is allowed with current legislation. The way taxes are collected and distributed to local governments and school districts would have to be evaluated and then potentially changed if the locals were to start buying services from the central state IT agency. Ensuring a structure that enables and encourages this kind of shared services model and making sure that it's well socialized while maintaining options for local governments and institutions, will allow more efficient and effective cybersecurity protection for everyone.

In parallel, the state IT agency should start to put together service offerings and survey local government and school districts to garner which services they are interested in, in both the short and long term. A centralized model for purchasing across the state may not be as popular, so the CISO and CIO should get an idea of what services the locals would want to purchase from the start and prioritize those services as they stand up the program. States should look at setting up a steering committee of state employees and others from across the local governments and state institutions so that the new shared services office is best serving the needs of those entities and the entire population.

Next, the state should set up a shared services office and begin making lists of approved products. Most states have a central IT agency charged with administering services to state agencies, and starting with that list of products and applications will help make this process quick and easy. Additional resources would be necessary for this agency to work with local and education institutions, so ensuring that the state appropriately resources their agency as they broaden the scope of their work will be critical.

Once legislation is approved, resources are allocated, and services can be offered, it's time to go back to the local governments and school districts and educate them on the offerings and the potential benefits they can realize. Once local governments and other institutions have successfully rolled out some new services, those success stories should be shared so that other jurisdictions know that the services are available. From there, it's a matter of expanding services offerings to meet the needs of constituent agencies.

Additionally, states should develop an overarching cybersecurity strategy. These documents can help define the vision for the state, laying our priorities, and linking them back to tangible benefits, such as economic development. This will further enable a whole-of-government approach to protecting their state and constituents at all levels.

After that, it's a matter of running and maintaining the services on a whole-of-government model. This will require additional resources so that the local governments and other institutions can be serviced appropriately, ensuring that the systems being selected are trusted and secure, and meeting the needs of local governments across the state. The potential benefits of this type of view of IT services for state governments may benefit all as they realize efficiencies of scale, improved security, and lower costs.

Real World Implementation: How states and local government are banding together to fight cyber attackers

The "whole of government" approach to offering cybersecurity services is a popular idea, but one that has caught on in only a handful of states. Many states are still considering the approach, but they are wrangling with the policy and legislative matters that need to be considered.

That said, many states are providing some services to locals. Threat information sharing, disaster recovery, and tabletop exercises are some services offered by a 2020 report from the National Association of State CIOs.[8] The report highlights Texas, which has launched a managed service program that provides security device management, incident response services, and assessment services to local and K-12 entities. The former CISO has publicly shared a story where 23 local agencies suffered ransomware attacks at the same time. Resources in one school district were so scarce that they couldn't afford anti-virus software, which led to two ransomware incidents in three weeks. Instituting a whole of government approach has enabled state leaders to have better insight into what locals are dealing with in terms of cyber threats.

Texas also operates a Regional Security Operations Center out of Angelo State University that gives university students hands-on cybersecurity experience and provides local support to taxpayer-funded agencies that need assistance with major cybersecurity incidents.

Virginia has also rolled out services to 65 state agencies, local governments, and schools to help manage threats. The commonwealth has mechanisms in place where all stakeholders — down to small towns with minimal IT budgets — collaborate to protect their data, with the goal of helping one another in the event of a crisis like a cyberattack or data breach.

To help manage the program for stakeholders, the commonwealth put in place interagency and public-private boards and councils, not all of which are headed by a government official. This helps garner better communication and trust among the different stakeholders and bring up new ideas for the state.

While the economies of scale from combining these services across the state make sense, a group of towns in Massachusetts saw the threats and decided to come together and form their own consortium to do the same at a smaller scale. Thus, was born the North Shore IT Collaborative, seven communities – Danvers, Middleton, Topsfield, Wenham, Hamilton, Essex, and Manchester-by-the-Sea – joined together to address common information technology challenges among local governments.[9]

The Collaborative defines annual goals and works as a group towards those goals each year. Member communities retain local control of systems and have voting rights in collaborative decision making. The group identifies shared information technology needs and designs a regional approach to address them, leveraging distributed expertise and economies of scale.

[8] https://www.nascio.org/wp-content/uploads/2020/01/NASCIO_NGA_StateLocalCollaboration.pdf
[9] https://www.danversma.gov/617/North-Shore-IT-Collaborative

Town IT leaders meet monthly to discuss ongoing projects and define the direction of the collaborative. Benefits have been realized in the form of grant receipts, and bulk purchase cost savings.

The group has raised over $700,000 in grant funding and developed relationships with strategic partners in the areas of information technology and information security, which has increased the purchasing and reference power of the organization.

While these are three different initiatives, these examples make it clear that offering cybersecurity services with a broader scope can serve all levels of state agencies and individuals.

Appendix: Recommendation summary

To establish a whole-of-government approach, state governments should:

#	√	Task
1		Establish whether existing laws allow a whole-of-government funding model at all levels of the state for IT and cybersecurity; if not, enable this approach.
2		Ensure appropriate resources so that the state IT agency can serve a larger set of stakeholders.
3		Create a voluntary approach for providing services, rather than mandates.
4		Equip state CISOs to integrate across the state and with local governments.
5		Consider best practices for cybersecurity and ensure consistency when proposing and passing state legislation, including legislation that would impact a broader set of constituents than just state government employees and systems.

To establish a whole-of-government approach, the state IT agency should:

#	√	Task
1		Establish a shared services model, including transparent processes to vet, approve, and purchase services from vendors; consider starting with a list of products that have already been approved by the state to make services available quickly.
2		Consider grandfathering in existing technologies and services to give local governments and institutions time to transition their infrastructure.
3		Establish a clear, digital process for procuring technology once it has been approved and use that to facilitate implementation plans.
4		Create reusable roadmaps that detail how the new shared services approach can modernize legacy technology across all levels of the state.
5		Interview stakeholders across the state to understand the services that would be helpful for them and establish an ongoing group of advisors and a method to submit requests.
6		Create an ongoing working group process among stakeholders, including small jurisdictions, across the state to define the needs and requirements. Use this process to create consensus and buy-in.
7		Create ongoing public-private working groups to share best practices and information about threats and attacks.
8		Reduce silos between state, city, and county entities to reduce gaps in the state's cybersecurity risk profile and share best practices and threat information.
9		Establish performance goals to help guide which security measures are most needed.
10		Establish training for employees and officials across the state.
11		Practice state and local incident response.

State priorities:

These themes emerged across interviews, and are served by a whole-of-government approach:

#	Priority
1	Work to address staffing and workforce concerns through changing hiring practices, continuing training, and partnering with academic institutions.
2	Grandfather existing technologies and services to give local governments and institutions time to transition their infrastructure.
3	Create trusted software lists, including portfolio management that ensures only trusted applications are used, including on mobile devices.
4	Learn from shadow IT, and have processes in place so individuals feel comfortable requesting new software and platforms to keep systems secure.
5	Create a plan to secure or modernize legacy systems; this may take significant time and resources but is critical to cybersecurity.
6	Explore zero-trust architectures to = more efficient and effective approaches to cybersecurity.
7	Begin to future proof infrastructure and evaluate the risk and opportunity of new technologies, like artificial intelligence and next generation encryption.
8	Train state employees around cybersecurity threats, privacy, and data retention on an annual basis. Threats are ever evolving, and training can help keep states secure.
9	Run tabletop exercises simulating attacks and disaster recovery annually.