A GOVERNMENT TECHNOLOGY GUIDEBOOK

HARNESSING THE POWER OF COLLABORATION:

HOW STATE AND LOCAL GOVERNMENTS CAN WORK TOGETHER TO STRENGTHEN CYBERSECURITY

government technology | IBM®

CONTENTS

INTRODUCTION

State and local governments face a variety of security challenges, from ransomware and malware to email phishing schemes and denial-of-service attacks (DoS).

Just this year, nation-state actors targeted state election websites and attempted to download voter registration data. They also launched attacks against state and local government networks.[1] At the same time, a massive shift to remote work transformed employees' homes into the new perimeter, making endpoint security and authentication even more critical. Reports indicate cyberattacks in the public sector have increased by 50 percent in 2020, as the pandemic seemed to embolden hackers.[2] However, significant budget shortfalls due to the pandemic have made it even more difficult for governments to invest in modern security technologies.

WHILE KNOWLEDGE SHARING IS COMMON AMONG GOVERNMENT AGENCIES, IT IS CRUCIAL THEY EXPLORE MORE STRUCTURED FORMS OF COLLABORATION TO BETTER HARNESS THEIR SHARED KNOWLEDGE AND STRENGTHEN THEIR SECURITY POSTURE.

As the threat landscape becomes more sophisticated, state and local governments' incident, preparedness, response and threat detection capabilities must evolve with it. However, their ability to advance their cyber maturity differs based on the resources they have. State governments are often in a better position to take a more forward-looking, proactive approach to incident planning and response, while local and county governments typically must focus on protecting their most critical assets.

"It really depends on the size of the organization, their budgets and what they're able to invest in cybersecurity," says Richard Swain, a security architect at IBM who works with state governments to bolster enterprise security.

To better pool limited resources, state and local governments need to collaborate more around cybersecurity. While knowledge sharing is common among government agencies, according to a recent survey of more than 500 state, local and county government officials across various agencies conducted by the Center for Digital Government (CDG) in partnership with IBM, the Multi-State Information Sharing and Analysis Center (MS-ISAC), Election-ISAC and the Government Finance Officers Association (GFOA), it is crucial they explore more structured forms of collaboration to better harness their shared knowledge and strengthen their security posture. For example, models are emerging where local governments can buy services from a state or other local government to take advantage of economies of scale, which helps reduce costs and increase security.

That is just one approach that may prove effective. From implementing a whole-of-state cybersecurity model and developing multi-state partnerships to forming state and local government tiger teams for better incident management, government organizations can collaborate in innovative ways to protect their networks, systems and the valuable data they collect.

BARRIERS TO BETTER COLLABORATION & STRONGER SECURITY

Depending on the jurisdiction, local and county governments may not be required to notify other jurisdictions of a security breach, which means they may not take full advantage of state resources to better prepare for and combat future security threats.

"Whereas state agencies and higher education institutions must follow our policies and report breaches to us, local governments do not fall under those statutes," says Nancy Rainosek, chief information security officer (CISO) for the state of Texas. "So, for us to find out what is going on in the local government, it is voluntary. We may find out from them, or we may find out from MS-ISAC or read it in the paper."

This information gap exists even though Rainosek's agency, the Texas Department of Information Resources (DIR), collaborates with and provides cybersecurity resources to local and county governments through a range of programs and initiatives. However, research shows a significant portion of state governments do not undertake this level of collaboration within their jurisdictions. According to a 2019 NASCIO survey of state CIOs, 65 percent of states provide security infrastructure and services to local governments,[3] which means that more than one-third of state governments do not offer services to smaller government organizations that could benefit from these resources both operationally and from a cost-sharing perspective.

Many governments also face policy and institutional barriers that prevent them from helping or receiving help from fellow government organizations during a security incident. In the CDG survey, 70 percent of respondents said their agencies would need to get executive approval before an external agency could access their resources or networks, while 62 percent would need funding to pay for the deployment of these external resources.

There is also fear among state and local governments about giving external organizations access to systems or insight into their security infrastructure. They worry about data leakage and a potential breach due to opening their systems to third parties.

70% OF SURVEY RESPONDENTS SAID THEIR AGENCIES WOULD NEED TO GET EXECUTIVE APPROVAL BEFORE AN EXTERNAL AGENCY COULD ACCESS THEIR RESOURCES OR NETWORKS.

"This is one of the major barriers, but I think you mitigate that by having people find ways to work together so they get to know and trust each other," Swain says.

Another challenge is that it takes executive leadership and buy-in to forge effective partnerships among different government organizations. However, a willingness to take this step often competes with other business priorities. Swain says smaller city and county governments can be more willing to collaborate and pool their resources than larger city, county and state agency organizations that have the budget to be more cybersecurity independent. And the size of an organization is another factor — a region with a greater number of counties, cities, departments and agencies is a more complex environment for collaboration.

State governments also may not do a good job of sharing information about the services they offer or communicating about available federal services. The 2019 NASCIO State CIO survey found only 31 percent of states have a formal awareness and marketing campaign to promote their offerings to local governments.

"You have all these different entities that have all these different resources, like MS-ISAC and CISA [the Cybersecurity and Infrastructure Security Agency]. I think what's needed, because there are so many services, is helping people figure out where to start first," says Erik Avakian, Pennsylvania's CISO.

Several jurisdictions — including Pennsylvania, Texas, North Dakota, Maricopa County, Ariz., and Oakland County, Mich. — have taken steps to increase collaboration. Their efforts show there is no one model for how state and local governments can work together effectively to improve cybersecurity. The most important thing is that they start.

JOINING FORCES TO BOLSTER CYBERSECURITY:

HOW STATE AND LOCAL GOVERNMENTS ARE DOING IT

MARICOPA COUNTY, ARIZONA: COLLABORATING AND AUTOMATING INCIDENT PREPAREDNESS AND RESPONSE

Like most jurisdictions, the pandemic required Maricopa County leaders to reassess security.

"It really forced us to reevaluate where the risks are within our organization and then quickly come up with how we can either mitigate that risk or at least make the organization aware of what those risks are," says Lester Godsey, the county's CISO.

Thankfully, the county already had mature cybersecurity capabilities that were anchored in an agile, programmatic approach to security with strong information sharing and collaboration among agencies. For example, the county has processes in place that allow it to reprioritize aspects of its program based on input from its board of supervisors.

Godsey says there is also a structured approach to information sharing among government agencies and jurisdictions throughout the state. One recent example is the county's cybersecurity coordination around the elections.

"Months before the general election we established formal communication channels with other local, state and federal partners to prepare," Godsey says. "We shared our election war room protocols and sanitized versions of our incident response playbooks not only with the state of Arizona CISO, the FBI and DHS, but also our regional partners. We also had separate conversations with other counties."

"The threats don't know, respect or acknowledge boundaries or organizational structures," he says. "If we can share and receive information from other government agencies, there's a strong likelihood that's going to benefit us, so it behooves us to do that level of sharing."

The county also collaborated with the state of Arizona and MS-ISAC for a security, orchestration, automation and response (SOAR) pilot project with the John Hopkins Applied Physics Lab. The pilot, which included the states of Massachusetts, Louisiana and Texas, was designed to automate incident preparedness and response among state, local, tribal, and territorial governments and to enable quicker and more efficient information sharing among these entities.[4]

Each participating organization used different SOAR tools as part of the project and developed incident response playbooks based on their own business needs and the aspects of their security operations they wanted to automate, Godsey says. The county

EVERY GOVERNMENT AGENCY HAS ITS OWN PRIORITIES. BUT IF YOU ARE LOOKING AT COLLABORATION ON A WIDER SCALE OUTSIDE OF A SPECIFIC ORGANIZATION, THERE MUST BE SOMEONE TO HERD THE CATS.

also used threat intelligence from MS-ISAC, which allowed it to move away from weekly manual updates to a near real-time feed of the latest threat information.

The pilot built on the Applied Physics Lab's previous research and pilot programs, which found that using SOAR tools to automate information sharing can reduce response times during incidents from 11 hours to as little as 10 minutes.[5]

This kind of collaboration, in addition to working with local and regional partners, is key for governments to move the needle on cybersecurity.

"Every government agency has its own priorities, plan, vision and mission. But if you are looking at collaboration on a wider scale outside of a specific organization, there must be someone to herd the cats," he says.

Godsey says his team has found leadership buy-in and shared goals are vital for successful cybersecurity collaboration.

"We're coming up with tangible things that we want to accomplish and taking those tangible goals and then making milestones or specific tasks to accomplish them," he says of the county's current collaboration with the state. "It's just important that somebody within the wider community provides leadership, identifies collectively what it is you want to accomplish and then comes up with a roadmap for how you want to get it done."

TEXAS: EMBRACING A "ONE STATE, ONE SECURITY" APPROACH

Texas is gradually moving toward a "one state, one security" whole-of-state cybersecurity model. Although every state agency in Texas has its own IT organization and security chief, the Texas Department of Information Resources (DIR) sets standards and policies and provides information and services to other state agencies and local governments. This ranges from certification classes and training to security assessment services, Rainosek says. The department also partners with several Texas universities to share threat information. In addition, the state created an information sharing and analysis organization, Texas ISAO, led by a statewide cybersecurity coordinator.

A few years ago, the state formed a partnership with the Texas military department (which includes National Guard resources), its departments of public safety and emergency management, and other agencies to create a statewide incident response plan. Unfortunately, the state had to enact the plan in August 2019 when a coordinated cyberattack targeted 23 local government organizations, taking their systems offline and forcing the governor to issue an emergency disaster declaration.[6]

"We put that plan in place. All those resources, along with MS-ISAC, our incident response service provider, Texas A&M University and others all met at the state operation center. We were able to bring those governments back up to operations within seven days. It was a pretty big success for Texas and we're continuing to build on that and come up with other ways we can grow our capabilities," Rainosek says.

Pulling together state and local agencies and other public partners in this way is no easy feat, especially when each local government and state entity runs its own IT shop. However, Texas centralizes as much service and training as possible under DIR and information sharing under ISAO. Rainosek says the state also takes an enterprise managed services approach that allows local governments to access security resources.

"I really like what we're doing here in Texas with our ISAO, where we are reaching out to local governments across the state, pulling them in and providing information to them, and making sure it's useful and beneficial," she says. "The other thing is offering them services they can use, such as training and the ability to get assistance. If you are a local government in Texas and you have an incident, all you need to do — if you have a contract in place with us — is to put a ticket into our ServiceNow platform. We have SLAs

for a vendor to be on the phone or on location within a prestablished amount of time. We've really made it easy and a lot of people have come forward for help."

Texas demonstrates the value of formalizing collaboration and providing a solid framework for information sharing and incident response planning. Though a top-down approach may not work in every jurisdiction, in larger cities, states and counties it may help to create a more holistic cybersecurity strategy, centralize incident management and provide smaller municipalities with resources they may not be able to access otherwise to bolster their security defenses.

OAKLAND COUNTY, MICHIGAN: FORGING GOVERNMENT PARTNERSHIPS TO STRENGTHEN SECURITY

Oakland County, which has more than 1.2 million residents, partners with different levels of government to improve security.

Leaders there have a strong relationship with the state of Michigan Department of Technology, Management and Budget, sharing knowledge and communications weekly about the latest security threats. They are also building relationships with other counties and neighboring partners and actively engaging with MS-ISAC and EI-ISAC to access additional security resources, says T.J. Fields, the county's CISO. The CDG survey found that Oakland County is not alone in this area. MS-ISAC is one of the top three external resources governments rely on for continuing cybersecurity expertise — 76 percent of survey respondents said they used MS-ISAC for this purpose.

Fields says the county's engagement with these entities is critical because fostering more collaboration is an ongoing challenge for security teams.

"It's important to make sure the security message is spread far and wide," he says. "It's been a lot of relationship building [internally and externally]. A lot of my time that is not focused on my team and my controls has actually been spent in that outward-facing 'How do I get the voice of security out to the people who need to hear it, and how do I get those voices back into the security team?'"

Like many county governments that lack the same level of resources as state governments, Oakland County prioritizes securing its most critical assets.

OAKLAND COUNTY RECENTLY FORMED A CYBER TASK FORCE TO TAKE A COUNTYWIDE APPROACH TO SECURITY AND COLLABORATE MORE CLOSELY WITH ITS CITIES, VILLAGES, TOWNSHIPS AND NEIGHBORING COUNTIES TO BOLSTER THE REGION'S SECURITY POSTURE.

"My strategy is putting in place all of the protective controls you would expect, including anti-virus and firewall protections. But when we look at the next level of protective controls, what we tend to run up against is, 'Is it better to protect this or would it be cheaper and easier to look for anomalous activity?' Oftentimes, you find detection and rapid response is not much different from preventing it in the first place," Fields says.

With limited resources, these are the types of calculations many local and county governments must make. However, they are using collaboration to address some of their security gaps. Oakland County recently formed a cyber task force to take a countywide approach to security and collaborate more closely with its cities, villages, townships and neighboring counties to bolster the region's security posture.[7]

Fields says collaboration is key because many local governments face similar security challenges.

"Don't be afraid to ask for help. Everyone is short-staffed. Everyone is struggling to do all the things they want to do all the time. The last thing you need to do is complicate your life by trying to reinvent the wheel," he says. "We're all struggling with similar security problems, so either make use of your existing network or go find networks of people who can help each other. There's no way we can do this without reaching out."

NORTH DAKOTA: EMPLOYING A UNIFICATION STRATEGY TO PROTECT THE ENTERPRISE

Like Texas, North Dakota is also developing a statewide cybersecurity approach since smaller local

governments and other entities — including libraries, fire departments and schools — are on the state's unified network.

Kevin Ford, North Dakota's CISO, says the state focuses on a unification strategy with cybersecurity.

"In the unified environment, we act as the information technology organization for the state. This helps us consolidate our cybersecurity capabilities into one organization that can provide a lot more efficiency than if they were spread around in a lot of different agencies," Ford says.

The state is also leading an effort to develop a multi-state security operations center to automate information sharing and incident response.

North Dakota leaders work with K-12 schools and counties to strengthen their security, providing free anti-malware tools for threat prevention, detection, investigation and response.[8]

Cybersecurity exercises with the National Guard help the state strengthen its unified network, which demonstrates that state and local governments can leverage federal partners for more than just emergency response when a security incident occurs. Along with using intelligence and data from the MS-ISAC and EI-ISAC, the state leverages the Department of Homeland Security's Albert network security monitoring and management services.[9] Ford says using a SOAR platform has also helped the state automate incident management and threat mitigation.

"It drives down our mean time to respond and our mean time to mitigate cybersecurity events," he says. "It spares a lot of our on-the-ground resources. Our tier one analysts, for instance, now get to spend more time working on higher-risk incidents than maybe they normally would have."

Though North Dakota needed to take a unified approach to cybersecurity because of its network infrastructure, its strategy provides lessons for other jurisdictions that want to move toward a statewide or enterprise-wide approach to cybersecurity: Use technology to automate incident preparedness and response as much as possible, provide smaller local and county governments with resources (ideally, free) they can use to strengthen their security posture, and leverage federal partners to bolster your overall security defenses.

PENNSYLVANIA: ELIMINATING CYBERSECURITY "HAVES AND HAVE-NOTS"

The state of Pennsylvania has embraced a hybrid whole-of-state/shared services model. It works closely with county partners, local governments, school districts, townships and cities to share and socialize cybersecurity best practices. The state tries to eliminate cybersecurity "haves and have-nots" to achieve economies of scale and lower licensing costs, CISO Avakian says.

"By using this concept of cross-collaboration and getting outside our comfort zones and little silos within the state and branching out and building relationships with our county partners, school districts, townships and cities, we've started to find opportunities for how we can improve together and inform each other," he says. "Everyone's got similar challenges, but by doing this, we can learn from each other and implement shared services."

The state has quarterly meetings with the County Commissioners Association of Pennsylvania and Avakian is part of a working group with county CIOs that meets regularly.

"We talk about cybersecurity and the different opportunities available to us to collaborate so that we can collectively improve cybersecurity for the greater good across these different jurisdictional boundaries," Avakian says. "That cross-collaboration has helped build trust and forge new relationships."

It has also led to the development of a shared services model that allows counties to leverage the same cybersecurity awareness training Pennsylvania has adopted for its 85,000 users across the state's agencies. The training is now available to 75,000 users across county government. Counties can also access a service that conducts phishing exercises.

"It's utilizing collaboration to build, create and mature capabilities that either these counties may not have had before or need to expand on," Avakian says. "By doing that, we've created an environment where there are no haves and have nots. Everyone gets the same level of service."

BETTER TOGETHER:
BEST PRACTICES FOR IMPROVED CYBERSECURITY COLLABORATION

When it comes to cybersecurity, state and local governments are better together than they are apart. However, collaborating informally will not have as much impact on security as more structured approaches to collaboration. State and local governments should consider the following strategies as they work across jurisdictional boundaries to strengthen their security defenses.

Consider a whole-of-state model.

As North Dakota and Texas demonstrate, consolidating some or all security resources at the state level can advance cyber maturity across multiple levels of government.

Considering state statutes and other potential institutional barriers, states with the capacity to do so should contemplate pooling their resources to level the playing field for local and county governments and reduce costs for security solutions. With a whole-of-state model, state, local, and county governments and other public and private sector partners can work hand-in-hand to bolster enterprise security. If this is not possible, governments should consider a shared services model or expand existing resources — as Pennsylvania has — to help smaller entities better protect their systems.

Form government strike teams.

State and local governments also can consider forming tiger teams or strike teams to formulate and act on an enterprise-wide incident response and planning strategy.

“Open conversation and collaboration, doing things like capture the flag events and weekly reviews with a tiger response team in case an event happens, are just one of the ways governments can help their peers,” says Jamie Ballengee, a senior cyber security manager at IBM who works with public sector agencies.

Along with tiger teams and capture the flag events for shared incident response and security training, state and local governments can also open the door to collaboration by working together on targeted initiatives, such as election security or strengthening public safety systems, and then build from there once they have established trust.

Continue knowledge sharing and outreach.

State and local governments can share knowledge by bringing together cybersecurity experts across their jurisdictions in the form of a cyber task force, working groups or steering committees. Some states have even legislated collaborative cybersecurity working groups, Avakian says. Whether it is mandated by law

or voluntary, these types of collaborations can help build positive long-term relationships.

Along with knowledge sharing, state governments and larger local governments can connect through cybersecurity awareness outreach programs that target smaller government organizations using either their own resources or with help from a vendor. The Minnesota Secretary of State, for example, deployed a cybersecurity expert as a consultant to provide cybersecurity awareness training and incident response support for election-related cybersecurity issues to local municipalities.

Build executive buy-in.

Unfortunately, the desire to collaborate is not enough. Leadership buy-in is even more critical.

"You've got to have the backing of your leadership so they know it's important and they can support you in making things happen," Rainosek of Texas says.

Though every IT organization is structured differently, one of the most effective ways to get executive buy-in is to ensure CISOs and CIOs work together to foster a culture of cybersecurity collaboration within and outside their organizations. In the CDG survey, nearly 46 percent of survey respondents said a CIO oversees their organization's cybersecurity program, while 26 percent said this is the domain of the CISO. Therefore, these two roles must be aligned about key strategic priorities and security investments, and must communicate the value of better risk management to the rest of the organization.

Leverage federal, state and public sector partners.

To some degree, state and local governments are leveraging resources like MS-ISAC, CISA and DHS Albert services, but it may also benefit them to find out other ways they can engage with these partners.

As the NASCIO survey indicated, awareness may be a barrier as local and county governments determine how to improve their cybersecurity strategies. States can help by creating a one-stop online destination for this information, but local and county governments also must actively seek out these resources. Pennsylvania, for example, has a memorandum of understanding in place with the National Guard to provide a host of services to the state and its local government partners — aside from when a major incident occurs.

Governments also can turn to organizations like NASCIO, the National Association of Secretaries of State, the National Governors Association and entities affiliated with local universities, such as the John Hopkins Applied Physics Lab, for a range of security resources and information, including workshops, training and pilot programs.

Identify common threat management tools.

State and local governments also may benefit from a SOAR platform to automate threat monitoring and intelligence gathering and to increase visibility into their technology ecosystems. In the CDG survey, only 17 percent of survey respondents said their organizations rely on a private cyber threat intelligence platform. However, technology is an essential part of creating a comprehensive security strategy and enabling better collaboration. A SOAR platform can help government organizations automate so they can improve security while maximizing their resources.

CONCLUSION

Whether it is technology-enabled collaboration, tiger teams, working groups or knowledge sharing, state and local governments can strengthen their security defenses by harnessing their collective wisdom, experiences and resources.

Though time constraints and institutional barriers may slow down these efforts, it is crucial that state and local governments try to find a way forward. With impending budget shortfalls and the possibility of federal funding still uncertain, the best way through for state and local governments seems to be to collaborate more closely.

"An organization might be very focused on looking inward, but as much as we look inward, we need to look outward and forge relationships because someday we might need other governments' help — and vice versa," Avakian says. "With cybersecurity, we're all in this together."

This piece was developed and written by the Government Technology Content Studio, with information and input from IBM.

Endnotes

1. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
2. https://www.bluevoyant.com/state-and-local-gov-security-report
3. https://www.nascio.org/resource-center/resources/the-2019-state-cio-survey/
4. https://www.jhuapl.edu/PressRelease/200713-APL-CISA-enlist-states-cyber-defense-technology-pilot
5. Ibid.
6. https://www.texastribune.org/2019/08/19/twenty-three-Texas-cities-targeted-in-coordinated-ransomware-attack/ & Nancy Rainosek interview
7. https://www.oakgov.com/it/security/taskforce/Pages/default.aspx
8. https://www.nd.gov/itd/news/6903/ndit-provide-free-anti-malware-counties-ahead-elections
9. https://www.cisecurity.org/services/albert-network-monitoring/

Produced by:

government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

For:

IBM

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than two trillion events per month in more than 130 countries and IBM holds over 3,000 security patents.

To learn more, visit ibm.com/security.