NLC NATIONAL LEAGUE OF CITIES
CENTER FOR CITY SOLUTIONS

State and Local Partnerships for Cybersecurity:

A STATE-BY-STATE ANALYSIS

NLC NATIONAL LEAGUE OF CITIES

CENTER FOR CITY SOLUTIONS

About the National League of Cities

The National League of Cities (NLC) is the voice of America's cities, towns and villages, representing more than 200 million people. NLC works to strengthen local leadership, influence federal policy and drive innovative solutions.

NLC's Center for City Solutions provides research and analysis on key topics and trends important to cities and creative solutions to improve the quality of life in communities.

About the Authors

Christiana K. McFarland is the Research Director of NLC's Center for City Solutions, **Brenna Rivett** is a program manager, **Kyle Funk** is a program specialist, **Rose Kim** is a program specialist, and **Spencer Wagner** is a program specialist in NLC's Center for City Solutions.

Acknowledgments

The authors would like to thank Laura Cofsky who edited the report, and Paris Williams who designed the report.

About the Report

This report is the sixth project outcome of a research collaborative between NLC and the state municipal leagues. We are grateful for the guidance, data verification and cybersecurity narratives they provided.

Table of Contents

Foreword

Much of our world has gone digital. In many communities, everything from paying utility bills and acquiring permits, to requesting sidewalk repairs and reporting potholes, is now done online. These changes have made many aspects of our daily lives more efficient. However, they come with a price.

Today, local governments are a major target for hackers, and they can cost cities millions. More importantly, these attacks threaten to erode the trust that residents have in critical institutions. Over the last few years, cities, towns and villages — as well as states — have launched pragmatic, creative solutions to defend themselves. But perhaps more importantly, both local and state governments are increasingly realizing that they can't shoulder the burden of cybersecurity alone. It's a team sport that requires everyone to work together, using strategies that play to everyone's strengths.

As we move into election season, it is crucial that we keep our communities secure and protect our democratic systems from bad actors. At this time, there is no roadmap, and states vary widely in the kinds of cybersecurity supports they currently offer. That's why my team and I at the National League of Cities have prioritized this issue and created resources that are both reliable and immediately applicable for the cities we serve.

To that end, we have surveyed the various ways that states are supporting cities in their cybersecurity efforts. *State and Local Partnerships for Cybersecurity: A State-By-State Analysis* is meant to help local governments better understand best practices for working with their state government, and what resources may already exist that they can tap.

We are stronger together. After reading this guide, I hope that leaders of cities, towns and villages, and the states in which they reside, will be able to forge ahead and build strong, resilient systems, both online and off, to protect their residents from cyberattacks.

Onward,

Clarence E. Anthony
CEO and Executive Director
National League of Cities

Introduction

On July 4th, 2019, the town of New Bedford, Massachusetts was hit with the largest local government cyberattack in history with a ransom demand of $5.3 million. Despite the significant ransomware attack on a town of less than 100,000 people, the overall effect was muted due "to a combination of luck — at the time of attack, most devices were still turned off for the July 4 holiday — and an IT architecture that compartmentalizes several key city departments, including police, schools and utilities."[1] As a result of the city's preparations, only four percent of computers were affected and no city services were disrupted.

This incident underscores that cyberattacks can hit any community at any time, regardless of size. While many cities are not prepared, those that have cybersecurity efforts in place benefit greatly. Cybersecurity refers to the protection, confidentiality, integrity and availability of data, systems and infrastructure in technology. Cybersecurity is a combination of secure systems (hardware and software) built into technology as well as human intervention, monitoring, training, awareness, and good network habits.

Despite the necessity, the reality is that many local governments are resource constrained and do not have dedicated funding for cybersecurity infrastructure or personnel. The good news, however, is that they don't have to face cybersecurity alone. State governments can be strong allies to local governments. They have greater access to financial and workforce resources and greater capacity to provide critical services.[2]

This guide outlines some of the most impactful ways that local governments can work with their state governments to prepare and defend again cyberattacks. Strategies discussed in this guide include:

- Mandatory breach reporting;
- State training initiatives;
- Cybersecurity Task Forces, Working Groups, and Councils;
- State and Local Shared Cybersecurity Services; and
- Non-Government Cybersecurity Partners.

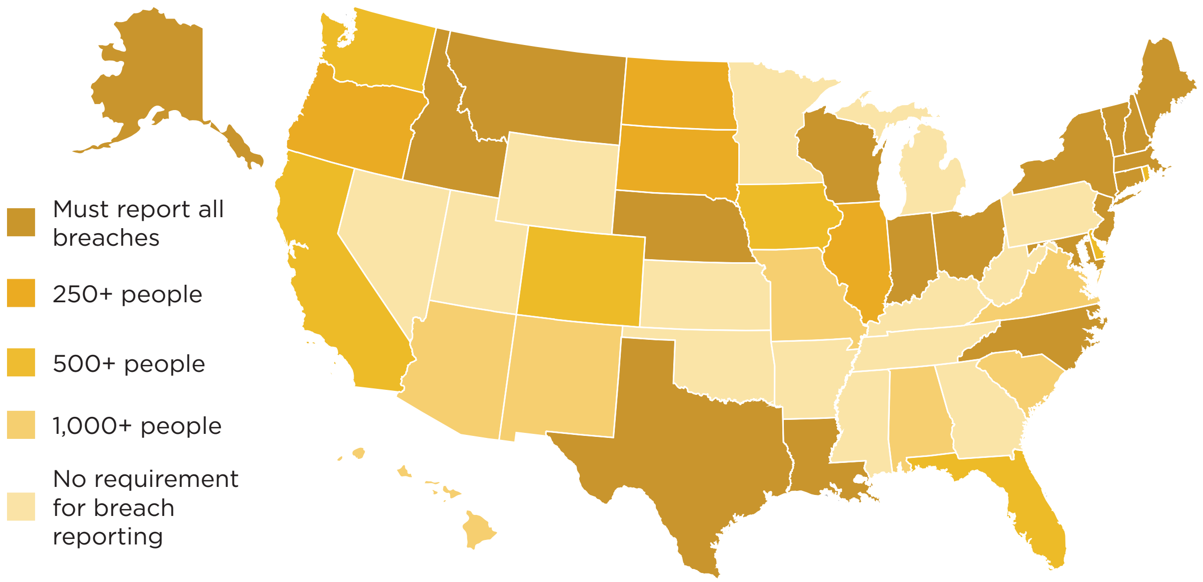
The report also includes profiles of effective city-state partnerships from across the country. As cities, towns and villages continue to be on the frontlines of cyberattacks, a collaborative approach between cities and states, together with Federal and university partners, can lead to a stronger national cybersecurity infrastructure in the face of growing threats.

Mandatory Breach Reporting

Mandatory breach reporting is required in all 50 states and the District of Columbia. These laws require private and/or public entities to alert affected individuals of any security breaches involving personal data.[3] California was the first state to enact such a law in 2002. The most recent states to enact similar laws were Alabama and South Dakota in 2018.[4] Despite consensus that mandatory breach reporting is a critical cybersecurity strategy, there are vast differences in these laws from state to state. These differences are primarily based on the type of entities affected, the type of personal information involved, the manner in which the data were stolen and the requirements for notification — such as timing and other entities that should be alerted.[5]

Mandatory Breach Reporting Thresholds for Local Governments

Is there a threshold a people affected by a breach to triggers state notification? If so, how many people?



These laws also vary in their reporting requirements. 36 states require that municipalities report breaches to the state. Typically, municipalities are required to report to the state attorney general but depending on the state it can include the state insurance regulator or other entity.

Of the 50 states and the District of Columbia, the states can be classified as either 1) having no breach reporting requirement to the state government (14 states and the District of Columbia); 2) states that require notice regardless of the number of people affected by the breach, or no threshold (18); and 3) states that have a threshold for reporting (18).

No breach reporting requirement

Fourteen states and the District of Columbia require that entities notify affected individuals (as all states do), but do not require the entity to alert the state government or officers. These include states like Georgia and Minnesota.

Reporting requirement without a threshold

Eighteen of the 36 states do not have a threshold at which they have to notify the state; thus, municipalities must report a breach to the state no matter how many people are affected. Montana, New York and Wisconsin are examples of these states.

Reporting requirement with a threshold

The other 18 states have thresholds at which point they must notify the state government. For instance, Delaware requires a public entity to alert the state if 500 or more people are affected in a breach. New Mexico on the other hand requires notice to the state if 1,000 or more people are affected. There are three common thresholds: 250, 500 or 1,000 people.

- Four states require notice if at least 250 people are affected;
- Seven states require notice if at least 500 people are affected;
- Seven states require notice if at least 1,000 people are affected.

When alerting the state, some are required to provide not just the names and contact information of the individuals affected, but also a summary of the breach and services that have been or will be offered, such as in Florida and Alabama.

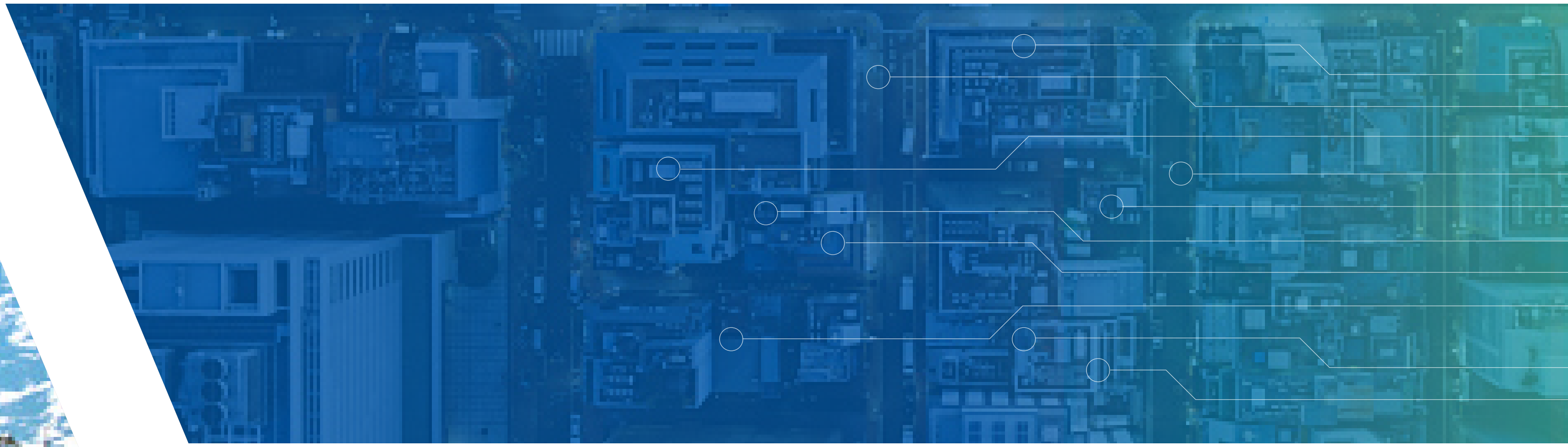
CASE STUDY:
Mandatory Breach Requirements in Alabama

One of the most recent states to adopt a mandatory breach requirement law was Alabama. According to the executive director of the Alabama League of Municipalities, Ken Smith, the recent law has not caused major headaches for cities and towns, as fortunately a major breach has not yet occurred.

"There will obviously be a problem trying to notify everybody, and we have been trying to get the word out through presentations and events," stated Smith.

He and league director of IT, Chuck Stephenson, traverse the state speaking about the law and other actions in the cybersecurity space. This represents just one proactive approach the state and the League have taken when confronting cybersecurity. In 2020, there will be regional training sessions in the state to highlight the resources available to municipalities, including The Multi-State Information Sharing & Analysis Center (MS-ISAC) and the League's cybersecurity partner, Sophicity.

Smith reiterated, "One of the biggest results that came about from some of the legislation like this was just a realization that we all needed to be a little bit more aware of it and take steps and try to prevent cyberattacks as much as we possibly can."



State Training Initiatives

As the number of cyberattacks continues to grow each year, governments assume significant, unforeseen financial losses. To address vulnerabilities and raise awareness, states have offered various types of cybersecurity training initiatives for government employees, including local governments, to protect against future incidents. Of the states that offer cybersecurity training initiatives, most governments have mandatory or voluntary trainings for state employees. Regardless of whether local government employees currently have access to these programs, it's helpful for them to be aware that they exist and to explore how to build partnerships.

Voluntary for State Employees

Currently, 22 states (Alabama, Arizona, Arkansas, California, Connecticut, Iowa, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Mississippi, New Jersey, New York, North Carolina, Oklahoma, Rhode Island, South Carolina, South Dakota, Tennessee, Utah and Wisconsin) offer voluntary cybersecurity training programs for state employees. Common resources states offer to employees include online cybersecurity training videos, toolkits and in-person classes through partnerships with postsecondary education institutions.

Trainings take many forms. The Arkansas Division of Information Systems has developed an online cybersecurity toolkit to promote cybersecurity awareness in a practical and entertaining way. The toolkit includes factsheets, guides and webinars for state government employees to utilize. Meanwhile, the Connecticut Department of Administrative Services partnered with Connecticut community colleges to offer non-IT personnel in-service courses in cybersecurity awareness. Finally, the state of Iowa's Information Security Division provides online services for state employees to utilize, such as cybersecurity education training videos, anti-malware tools, wipe utility programs, and storage and file protection programs.

Voluntary for Local Employees

Delaware is the only state that offers voluntary statewide cybersecurity training for state non-executive and local government employees. For state executive branch agencies, however, the state of Delaware requires formalized annual employee cybersecurity awareness training.

Mandatory for State Employees

Sixteen states (Colorado, Florida, Georgia, Illinois, Louisiana, Maryland, Montana, Nebraska, Nevada, New Hampshire, Ohio, Oregon, Pennsylvania, Vermont, Virginia and West Virginia) require formalized cybersecurity training programs for their state employees. In Pennsylvania, the Office of Administration's Information Technology Department developed a cybersecurity program for state agencies that includes access to antivirus software and web-based security awareness trainings on cybersecurity best practices. Similarly, Illinois' Department of Innovation and Technology has a mandatory annual online cybersecurity training course for state employees that covers phishing scams, spyware infections and identity theft, and data breaches.

Mandatory for Local Employees

In 2019, Texas passed a law that requires most state and local government employees to formalize cybersecurity trainings for their employees. Under House Bill (HB) 3834 of the 86th Texas Legislature, the Texas Department of Information Resources, in partnership with the Texas Cybersecurity Council, will be required to develop and implement a certified cybersecurity training program to state government employees that perform at least 25 percent of their duties using a computer, local government employees with access to a municipal computer system or database, elected and appointed officials, and state government contractors.[6]

Public-Private Partnership

Wyoming is the only state that established a public-private partnership to implement a state employee cybersecurity training program.

No State Training Initiative

There are nine states (Alaska, Hawaii, Idaho, Indiana, Kansas, Missouri, New Mexico, North Dakota and Washington[7]) that do not have any type of state or local government cybersecurity training program.

Although most states offer cybersecurity training programs to state-level government employees, it could be cost-effective to also grant local governments access to these cybersecurity services online and free of charge. Furthermore, as most of these resources address common cybersecurity risks that affect both state and local governments, such an initiative could encourage knowledge-sharing between different levels of government.

CASE STUDY:

Local Cybersecurity Initiatives in Michigan

Michigan has been at the forefront of developing an effective cybersecurity ecosystem model. The state is implementing innovative solutions to educate government employees on cybersecurity protection measures, improve overall awareness on cyber-related issues and prepare for future cyberattacks.

Although Michigan's voluntary cybersecurity training program is offered to state-level government employees, Michigan's state government has collaborated with local partners to develop voluntary tools to improve cybersecurity education and preparedness within the state. One type of local collaborative effort with the state includes support from five Michigan counties: Livingston, Monroe, Oakland, Washtenaw and Wayne. This partnership was successful in the development of CySAFE, a free IT security assessment tool to "help small and mid-sized governments assess, understand and prioritize their basic IT security needs."[8]

Another innovative solution was the launch of the Michigan Cyber Range in the city of Ann Arbor in November 2012. The program provides "secure cybersecurity training, research and exercise environment for IT security professionals" in educational institutions, private businesses and the public sector — including local governments.[9] The purpose of this initiative is to enhance Michigan's protection of computer systems and sensitive data through hands-on cybersecurity awareness trainings and simulation exercises.[10]

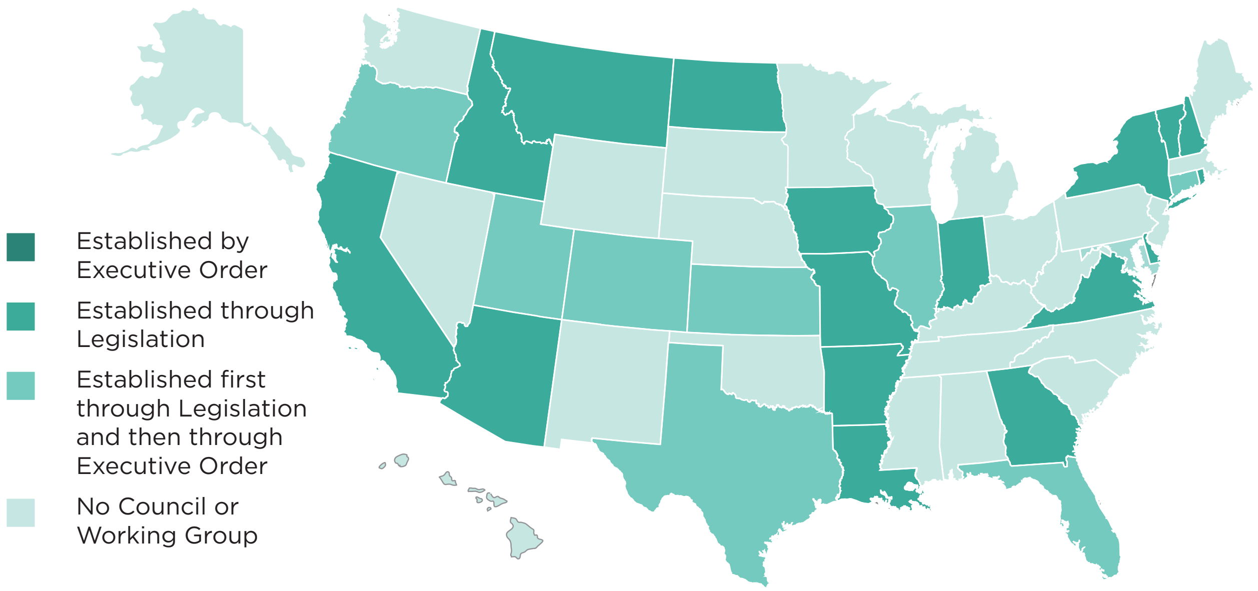
In recent years, Michigan has become one of the few state leaders in prioritizing and implementing effective state government cybersecurity measures through leadership, innovation and strong collaboration. It's essential for states to recognize the urgency of complex cybersecurity issues and develop effective cybersecurity measures to prepare for potential cyber threats in the future.

Cybersecurity Task Forces, Working Groups and Councils

Over the last few years, 25 states have established cybersecurity task forces, working groups and councils. The vast majority of these states, seventeen, created these groups through an executive order, while the other seven created the groups through legislation. One state, Maryland, utilized both an executive order and a bill to establish its cybersecurity council.[11]

From a city perspective, these groups are important because they often contribute to, or define, state policies on cybersecurity, including influencing what offerings are available to local government. In the long-term, accessing these groups could be an effective first step in times of crisis. In Massachusetts, the working group includes cities as official members, providing strong linkages across sectors and various levels of government.[12]

State-Level Cybersecurity Task Forces, Working Groups or Councils


🟩 Established by Executive Order
🟩 Established through Legislation
🟩 Established first through Legislation and then through Executive Order
🟩 No Council or Working Group

These groups serve a variety of purposes: For states that are newer to cybersecurity, they can provide an opportunity to start those conversations, while for others they create a platform for continuing discussions and policies. Unlike long-established sub-committees such as transportation and finance, cybersecurity is a relatively new arena for state and local governments, and it is not yet widely represented at state capitals. Task forces, working groups and councils are therefore important mechanisms for governments to implement policies and procedures to protect themselves and residents from cyberattacks.

The landscape of these groups varies widely from state to state. Some states establish them for a set amount of time to achieve key goals[13,14], others set them up as ongoing convenings of key personnel to address present and future issues[15,16], and several use them as temporary measures to conduct research or produce reports.[17]

When it comes to cybersecurity task forces, working groups and councils, states fall into one of three categories:

- The state has a working group, task force or council established by executive order (17 states)
- The state has a working group, task force or council established through legislation (7 states)
- The state has a working group, task force, or council established first by legislation and then an executive order (1 state)
- The state does not have an established group working on cybersecurity (25 states and the District of Columbia)

CASE STUDY:

Kansas City, MO: A Regional Approach to Tackling Cybersecurity

One example of a state-level cybersecurity council can be seen in Kansas City. The Kansas Information Technology Security Council created numerous resources for local governments and cities to utilize.[18] Additionally, working with the Center for Internet Security (CIS), MS-ISAC and the Mid-Atlantic Regional Council, Kansas City formed a Regional Cybersecurity Strategic Framework with a goal to "create a shared service model to support local governments."[19]

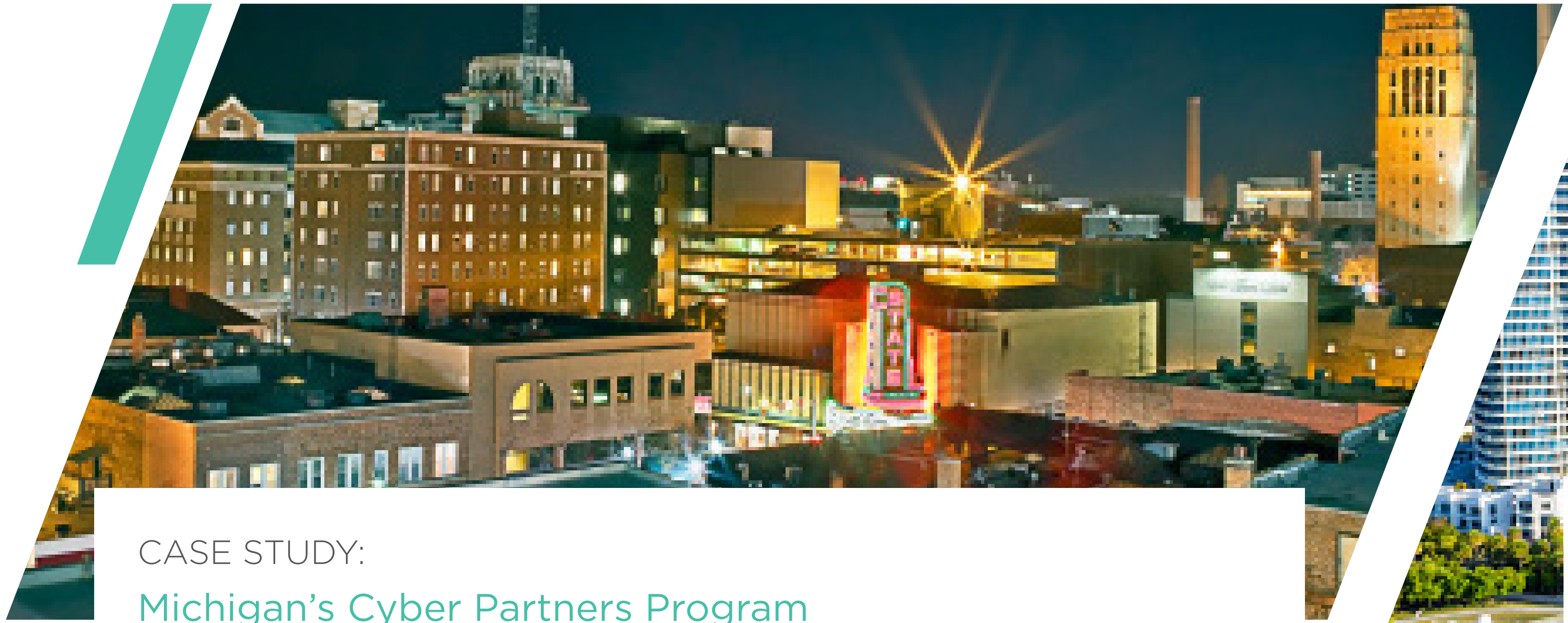
The effort started with a simple goal: to improve cyber hygiene for all communities in the region, regardless of size. Representatives from cities and counties, IT specialists and other cybersecurity experts worked together to develop the regional framework. They established benchmarks and best practices that centered around resiliency and redundancy. This regional approach is especially helpful for small cities that may not have the capacity on their own to audit their systems and upgrade accordingly. The approach also offers flexibility so that agencies that already have an effective framework are not forced to change. The CIO of Overland Park, Kansas, Tony Sage, says "one of the biggest strengths of the program is that it's based on a really collaborative approach."

State and Local Shared Cybersecurity Services

Local governments often come together with other governments to bundle purchases or to share services such as water treatment and delivery. Taking this shared approach for cybersecurity can help solve some of the critical barriers facing local governments, including budget constraints and personnel training. One approach is "inter-governmental sharing" of cybersecurity services.[20] It can include shared service agreements for cyber defense tools, IT/CIO shared staff or regional cybersecurity defense centers.

Although most states across the country do not have a dedicated state and local shared cybersecurity service, Idaho, Illinois, Michigan and Texas have created programs that others can learn from. Idaho's is currently getting ready to launch and others like Michigan and Illinois, are only in certain areas.

But cities, towns and villages cannot create this shift alone. States can help lead in this space. At a minimum, states should be building relationships with local governments and raising awareness of existing services. States can provide resources like staff or cybersecurity infrastructure to local governments. They can also play the more traditional role of providing technical assistance in the form of startup grants and loans for shared capital projects that deal with cybersecurity shared programs. States can also gather key stakeholders to enable shared cybersecurity services. Lastly, they can lower barriers by creating incentives for both the private and public realms to partner on cybersecurity programming.



CASE STUDY:

Michigan's Cyber Partners Program

Michigan's new Cyber Partners program is rebooting the state's successful Chief Information Security Officer (CISO) as a service program with a state-wide vision that includes a community approach to prevention, preparation and incident response. For two years, the state of Michigan piloted it's "CISO as a Service Program." During 2017 and 2018, thirteen communities received services from a CISO-level consultant who conducted a local cybersecurity assessment and assisted in developing a remediation plan. There were monthly teleconferences where all participants discussed assessment results, lessons learned and overall program development. The smallest community to use the program was Springfield, Michigan (pop. 13,000), which has only one full-time IT employee, and the largest was Washtenaw County (pop. 360,000).

Michigan Cyber Partners hosts monthly state-wide Skype meetings that highlight current cyber threats, discuss mitigation strategies related to the threats and provide a deeper dive on important topics. Additionally, cyber incident response is provided by the Michigan State Police Cyber Command Center and the Michigan Cyber Civilian Corps. Currently, Michigan is making plans to reintroduce the program as a public-private partnership in order to expand the program out to the rest of the state.

CASE STUDY:

Florida Innovation in the Cyber Space

The Florida League of Cities created a new grant program through the Florida Municipal Insurance Trust (FMIT) that helps local governments combat the ever-growing threat of ransomware attacks. The grant pays for cloud-managed backup services for up to two servers, along with one terabyte of backup space for each participating member. If a local government experiences a ransomware attack, its data is securely backed up in the cloud and can easily be restored, so the local government won't feel pressured to pay a ransom. The grant covers the total cost of managed backup services for the first year, and half for years two and three. After the third year, the local government takes full ownership of backing up its environment. Funding for the grant is provided through the FMIT, and the program is run by the Florida League of Cities.

"Our goal is to ensure that FMIT members understand that backing up their most sensitive and important data is a key defense against a cyberattack," said Michael van Zwieten, director of technology services for the Florida League of Cities. "The FMIT Data Recovery Grant Program gives members the tools to secure their data and make it retrievable through a managed-service partnership."

Launched in early 2020, the Data Recovery Grant Program is available to FMIT members with property and liability coverage.

> **Government in Michigan, like many states, is diverse, distributed, and interconnected. From a cybersecurity perspective, we present a broad attack surface to our adversaries. The response to this challenge can only be pulled together and address our common challenge with collective action. Michigan Cyber Partners provides the umbrella under which we'll do this.**
>
> Andy Brush
> *Cybersecurity Partnerships at the State of Michigan Department of Technology,* Management and Budget

ELECTION SECURITY AND CITIES

At the time of this writing, the 2020 primaries and presidential election are top of mind for many cybersecurity experts. For city leaders, understanding the landscape of election security is crucial so that votes are kept safe and confidential. According to election security experts, there are three main levels of election security that are important to understand:

1. NATIONAL VOTER REGISTRATION DATABASE.[21] This list contains information on all Americans registered to vote and can be accessed by the federal, state and local governments. Keeping this list accurate and secure is imperative, but also presents a challenge since there are multiple access points with varying levels of security.
2. BALLOT CREATION. If the computer that creates the ballots is directly or indirectly connected to the internet, it can be infected with malware.[22] This level of security is often the most overlooked.
3. BALLOT BOX. It is also the hardest to track, because every state and county can utilize different systems. Most states and counties are moving back toward paper voting, and away from electronic voting, which is more susceptible to hacks and security threats. But it is still a work in progress because changing the ballot type is expensive and time consuming.[23]

City leaders can work with county and state election officials to protect and safeguard the democratic process. The National League of Cities will be releasing a report later this year solely focused on local-county partnerships on this topic.

State Approaches to Cybersecurity

One of the biggest challenges in strengthening cybersecurity is that cities are often unaware of available resources at the state and national levels. Below are snapshots from four states that are representative of the diverse options available to local governments. These four state examples are meant to showcase the variety of ways that states are tackling cybersecurity and highlight new avenues that local governments can consider tapping into. The representatives from these states all had a common message for local governments: Collaboration is key. Local governments, counties, states and federal agencies all need to work together to address cyber threats, and that can look different in each state or region.

WISCONSIN

Number of Programs: 4

Type: National Guard Partnership and State Agency Programs: Defensive Cyber Operations Element, Cyber Protect Team and Wisconsin Statewide Intelligence Center

The state of Wisconsin has mobilized to build out a robust slate of services for local governments. Wisconsin, through its Department of Military Affairs, utilizes the Wisconsin National Guard to run analytics for local governments. The Defensive Cyber Operations Element (DCOE) is composed of 10 personnel who can help establish a baseline of "security, through analytics and system forensics." There is also the Cyber Protection Team (CPT) that focuses

THE MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER

Every state in the country has access to the Multi-State Information Sharing and Analysis Center (MS-ISAC) which runs under the Center on Internet Security (CIS). MS-ISAC is a free service designed to help the nation's overall cybersecurity efforts. Every state also has at least one, if not more, Fusion Center which, under the Department of Homeland Security, deals with coordinated threat protection and emergency responses. Leveraging and partnering with both of these organizations at the local and state levels could be crucial to securing municipalities around the country.

exclusively on cyber operations and threat emulation. The Wisconsin Department of Justice has created the Wisconsin Statewide Intelligence Center (WSIC), which is a fusion center for the sharing of threat-related information between state, local, territorial, federal and private sector partners. The WSIC offers a variety of products and tools for its partners, including analytic reports, malware analysis and cyber liaison officer training.

FLORIDA

Number of Programs: 1

Type: University Partnership

The state of Florida has created The Florida Center for Cybersecurity (Cyber Florida) which is built on the three pillars of education and workforce development, innovative research, and outreach and engagement.[24] Cyber Florida is hosted at the University of South Florida and works with all 12 State Universities, industry, government and defense to be a national leader in cybersecurity.[25] There is also ongoing discussion in the state legislature to consider funding Cyber Florida so it can provide matching grants to local governments to enhance technology infrastructure, employee training and technology audits. Another proposed piece of legislation aims to provide open records protection for technology-related information that might leave local governments vulnerable to cyberattacks/ransoms.

PENNSYLVANIA

Number of Programs: 1

Type: National Guard Partnership

The state of Pennsylvania has one of the strongest cybersecurity programs for county government that has yet to be extended to municipalities, known as PA Cybersafe.[26] The only resource the state of Pennsylvania offers for cities, town and villages is to help them connect with national organizations (MS-ISAC, National Council of ISACs and the Government Technology Institute Security Center of Excellence).

UTAH

Number of Programs: 4

Type: State Agency Program, Fusion Center, National Guard Partnership, and University Partnership

Utah takes a multi-faceted approach to cybersecurity. They partner with local universities to give students the opportunity to work on real-time cybersecurity projects and are in the process of finalizing a partnership with the Utah National Guard to aid in responding to cybersecurity issues. The state has also set up a Fusion Center, through the Utah Department of Public Safety, which brings together disparate levels of government and experts from a variety of fields to efficiently and effectively tackle cybersecurity threats and attacks.[27] In the past, Utah offered cybersecurity training to local officials, but the funding for those trainings has dried up and the state is currently looking for other funding sources.

Non-Government Cybersecurity Partners

University Partners

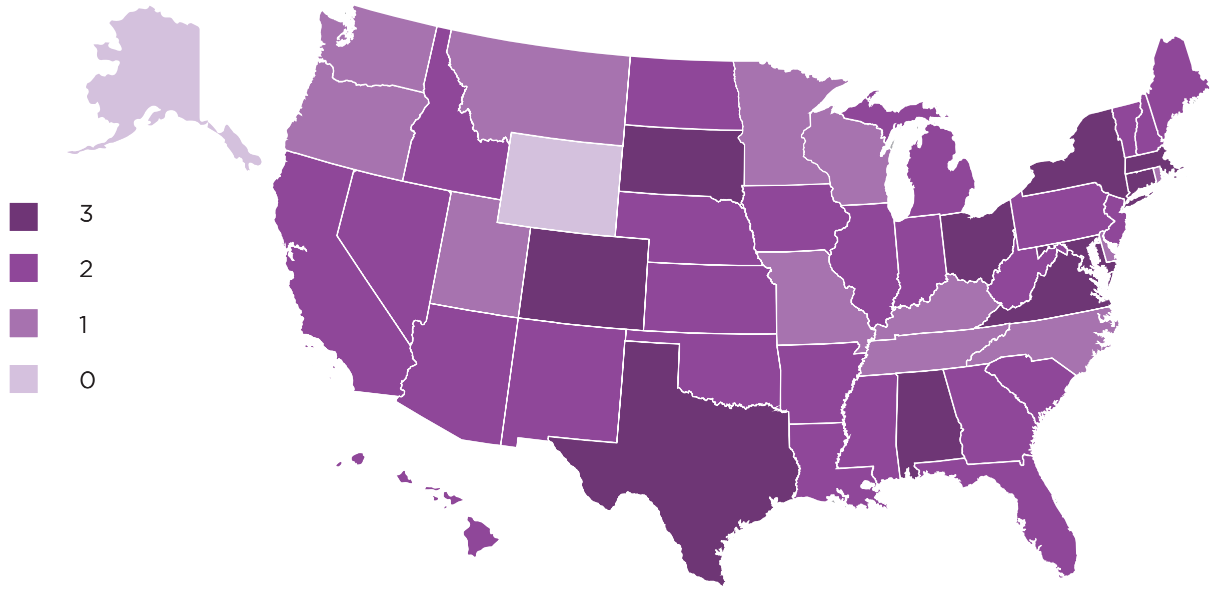
State governments have long partnered with their public or private two- and four-year universities to address critical issues in their states, from aligning talent with business needs and providing extension services, to, more recently, bolstering cybersecurity at the state and local levels. These partnerships are usually created by including a line item in the state budget that sends money to one of these post-primary education places to build a program. Strong university programs can not only help develop the cyber and IT public sector pipeline but also manage and protect data, respond to cyberattacks, offer cybersecurity training and convene critical stakeholders.

Most states (30) have created an official partnership with universities and colleges for cybersecurity-related support and services. For example, the state of Idaho partners with the SANS Institute, Girls Go CyberStart and Cyber FastTrack to identify talented youth who may be able to fill cybersecurity professional needs. Two Idaho undergraduate students won $22,000 through the Cyber FastTrack program to get a certificate in Applied Cybersecurity from the Sans Institute.[28]

The federal government, through the National Security Agency (NSA) and the Department of Homeland Security (DHS), sponsors two-year, four-year and graduate level institutions in National Centers of

Partnerships: Higher-ed, CAE Cyber Defense and CAE Cyber Operation

How many types of partnerships does each state have?



Academic Excellence (CAE) in Cyber Defense. According to CAE in Cyber Defense, "the goal of this program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise."[29] There are currently 272 total institutions throughout forty eight states with accredited universities. Only Alaska and Wyoming do not have an accredited place of higher learning. While there is no DHS funding for CAE Cyber Defense schools, some funding opportunities exist through the National Science Foundation. This system can be reworked to help local governments strengthen their cybersecurity capabilities.

The NSA also designates Centers of Academic Excellence in Cyber Operations. The program supports the President's National Initiative for Cybersecurity Education (NICE) which seeks to build a digital nation and a skilled workforce capable of supporting a cyber-secure nation. Currently, there are 16 states with a college or university holding this designation. While this program is deeply technical, it may be a source for states to tap into as technology continues to evolve.

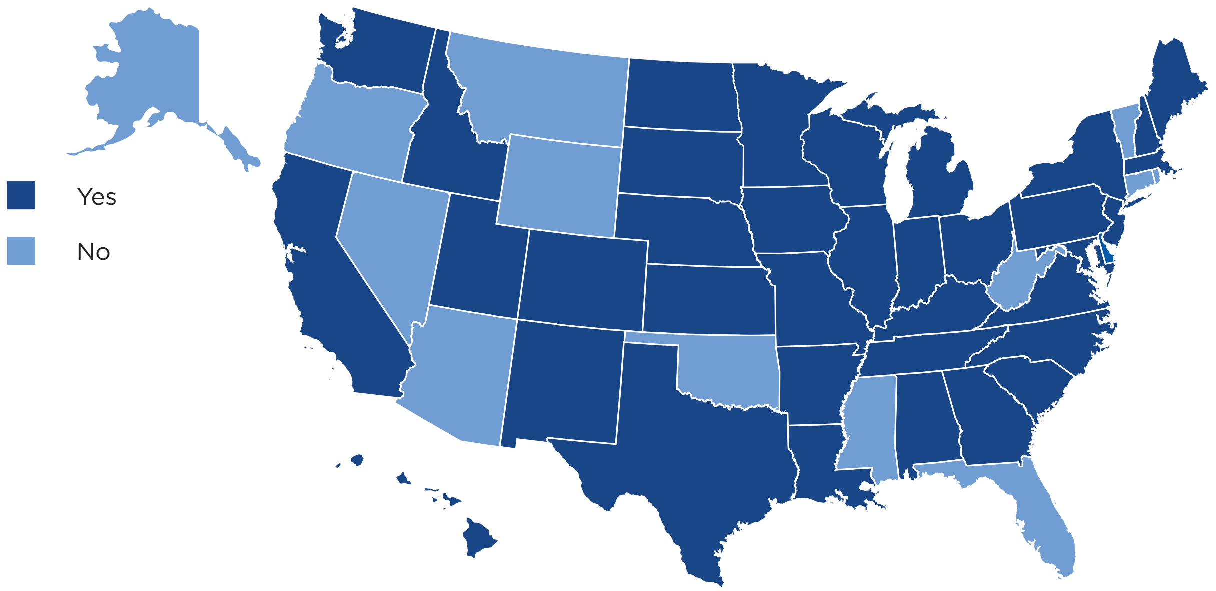
National Guard Partners

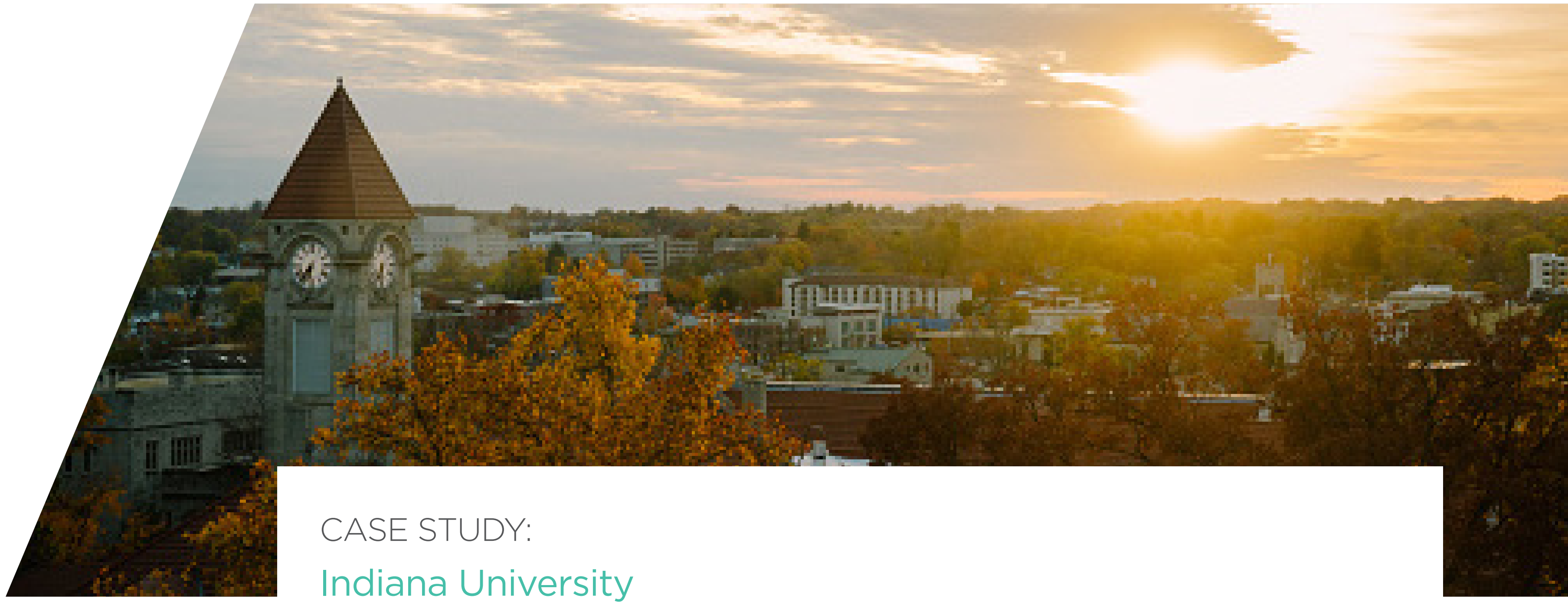
In addition to university partners, states have turned to their National Guards as a resource to defend against cyber-related attacks, safeguard information assets and protect the "digital and physical infrastructures" of localities.[30]

In total, the National Guard has "nearly 4,000 service members dedicated to cybersecurity across 59 units in 38 states and anticipates adding more through 2022."[31] Although every state has its own National Guard agency, some state cyber response units are responsible for covering multiple states. For example, the Army National Guard's 91st Cyber Brigade is based in Virginia but oversees cyber units in 30 states.[32] Within the 91st Cyber Brigade, there are only four states (Indiana, Massachusetts,

State Cybersecurity National Guard Partnerships

Does the state have a cyber response unit?





CASE STUDY:

Indiana University

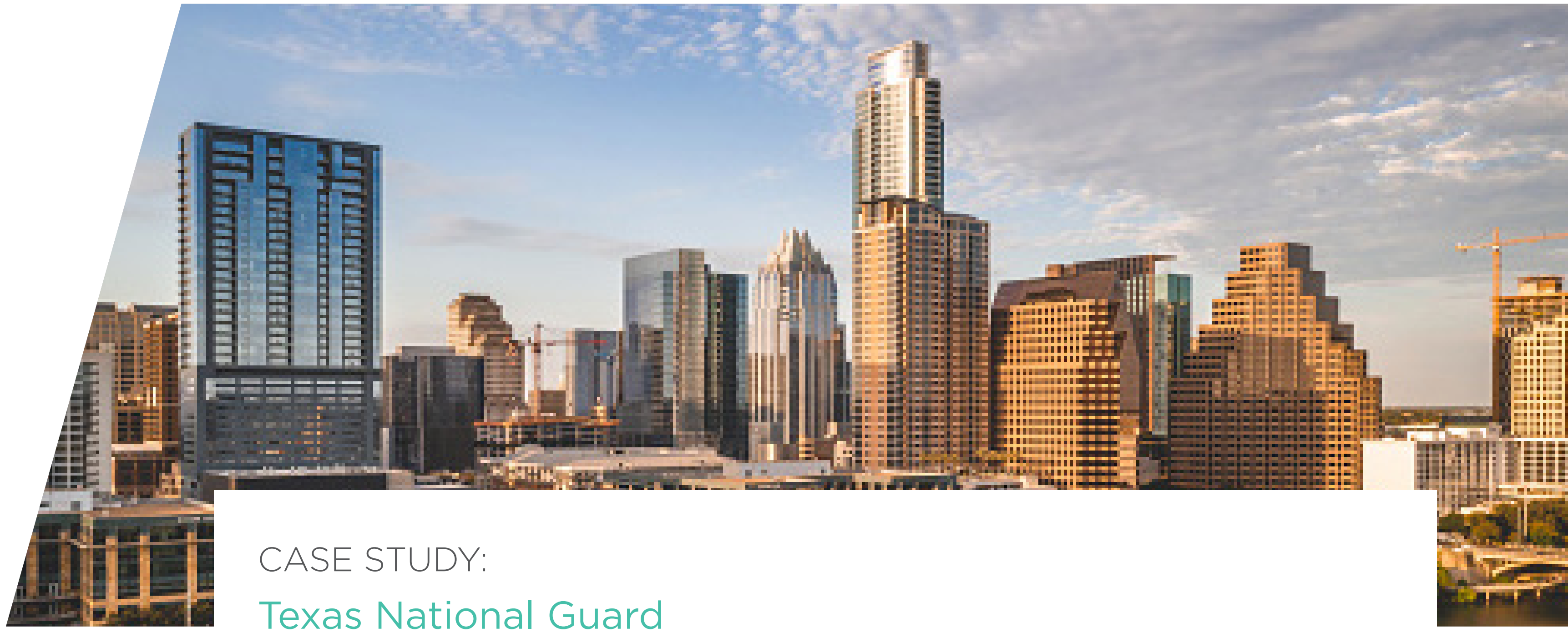
For 20 years, Indiana University (IU) has been at the forefront of universities that help manage cyber risk. has established an IU Cybersecurity Clinic to serve as a hub for Midwest cyber training needs. It will address threats faced by businesses, individuals, and state and local governments. Funding for the work comes from a grant foundation and matching funds of up to $225,000 from the Indiana Economic Development Corporation. The clinic will bring together businesses, law, informatics, computing and engineering school students to help state and local government agencies better manage cyberattacks, protect intellectual property and improve privacy. Through the clinic, IU hopes to continue Indiana's focus on supporting multidisciplinary innovation across the state. Academic director of the IU Cybersecurity Clinic Scott Shackelford is thrilled, "to train the next generation of cybersecurity professionals while helping to protect people and organizations around the globe, starting with our communities right here in Indiana."[33]

South Carolina and Virginia) that have a total of five cyber battalions in the National Guard (Virginia has two cyber battalions). In addition to responding to and neutralizing cyberattacks, members in the battalion will provide other types of support. For instance, the newest cyber battalion in Indiana will "offer cybersecurity expertise to companies, provide training readiness oversight to conduct cyberspace operations, network vulnerability assessments, security cooperation partnerships, and FEMA support along with cyberspace support of federal requirements."[34]

The National Guard has also implemented the Cyber Mission Assurance Team (CMAT), a new type of cyber response unit, in three states (Hawaii, Ohio and Washington). The purpose of this pilot program is to check federal facilities that rely on the state's critical infrastructure services. In 2014, the CMAT in Washington state conducted a utility grid assessment in the Snohomish County Public Utilities District to address vulnerabilities. Additionally, the Washington CMAT supported election security systems as they provided additional cybersecurity to ensure secure elections.

Finally, the National Guard has developed and activated eleven Cyber Protection Teams (CPTs) across 24 states (Alabama, Arkansas, California, Colorado, Georgia, Illinois, Indiana, Kentucky, Louisiana, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Jersey, New York, North Dakota, Ohio, South Dakota, Tennessee, Texas, Utah and Wisconsin).[35] CPTs provide cyber defense capabilities across all levels of government, which includes "incident response, vulnerability assessments, network and host-based analysis and threat emulation."[36]

The National Guard's mission has evolved to play a crucial role in providing effective cybersecurity support and assistance across all levels of government. This includes the development and deployment of various types of cyber units to respond and defend against cybersecurity threats in a timely manner. In the long term, continuing to develop and activate new types of cyber response units is a cost-efficient and practical option for state and local governments.



CASE STUDY:
Texas National Guard

In 2019, a ransomware virus attacked local computer systems in Jackson County, Texas. Digital services in the public sector, such as property transfers and police background checks, were disrupted. The Texas National Guard's Cyber Incident Response Team was deployed to assess the ransomware attack and work with the county's IT system to restore local network operations.

Later, in a coordinated cyberattack, 23 small Texas towns were hacked and held for ransom. Due to the experience from the ransomware attack in Jackson County earlier that year, the state responded immediately, deploying multiple agencies and resolving the attack in two weeks, without having to pay the hackers. The National Guard's role in this attack was crucial once again because it was able to perform an assessment of the attack and prevent further damage.

Concerned by the growing cyberattacks, the Texas Military Department, the "umbrella agency for the state's National Guard branches," invited state, local and county officials to demonstrate how the Texas National Guard's Cyber Incident Response Team plans to prepare for future cyberattacks on different government agencies.[37] In addition, the Texas Military Department provided information for local officials to improve their awareness on cybersecurity and advised localities on ways to protect local networks.

Hackers are increasingly targeting state, county and local governments nationwide. Small, local governments are especially vulnerable to ransomware viruses as they lack the financial resources and expertise. It's important for states to support vulnerable local governments to prepare and utilize the National Guard as an available resource to defend against cyberattacks.

Conclusion

Many cities, towns and villages remain vulnerable to cyber threats from global actors. Given their resource constraints, collaboration with their state government is proving to be a viable path forward.

Almost every state has implemented mandatory breach reporting, created state executive training initiatives and brought in non-state partners like universities and the National Guard to strengthen cybersecurity. Yet, work remains to be done in areas like election security, trainings at the city and county level, local autonomy, and state and local shared services.

To better bridge the gaps between state and local governments, consider implementing these key recommendations:

1. Build relationships with local governments: Every local government should have a point person on cybersecurity. State governments can start by identifying who that contact person is and reaching out to them. Having a strong state-city relationship is also important so that states are better positioned to support local governments. State municipal leagues are a great starting resource for building these relationships.
2. Raise awareness of existing services: A big hurdle for local governments is finding out what services exist for local municipalities at the state level. State governments can help by marketing these services or programs to localities. Annual gatherings could also help to fill the void and promote new and existing programs.
3. Update and create official policy for today's threats: In today's evolving cybersecurity world, states and cities need to make concerted efforts to partner and work together, rather than embrace a top-down approach. Creating new legislation on a new topic can be daunting, but legislators at both the state and local levels need to come together to create nimble policies that can be utilized in a variety of cybersecurity situations.
4. Include local governments in service contracts: Sound policies are only as strong as the budgets behind them. Cost can be a burden for both state and local governments and raising taxes is difficult. It is important to think about programs that build across existing networks or contain shared services for multiple government entities.
5. Work with team players such as higher education, the National Guard and the private sector: Cybersecurity and defense are team sports. State governments can lead by bringing all the pertinent partners together, including municipalities, to build programs, connect resources and defend against attacks.

By exploring these paths, state and local governments can begin to build a strong patchwork of cybersecurity. Elected leaders at every level of government know cybersecurity is an issue that is not going away. As the problem grows in complexity, it is more crucial now than ever that local and state governments work together. Doing so will result in better solutions for employees, governments and, ultimately, the residents they serve.

Additional Resources:

MS-ISAC – Center for Internet Security: One of the best free programs out there that many state and local governments are using is the Multi-State Information Sharing & Analysis Center (MS-ISAC). This coalition is open and free for all state, local, tribal and territorial governments. MS-ISAC is hosted by the non-profit Center for internet Security and supported by the Department of Homeland Security, and provides multiple resources, including a 24/7 Security Operations Center, Incident Response Services and a Vulnerability Management Program. State governments should work with State Municipal Leagues to promote and make sure all local governments know that MS-ISAC exist. More information can be found here: https://www.cisecurity.org/ms-isac/ and a list of current local government participants can be found here: https://www.cisecurity.org/partners-local-government/

Fusions Centers: There are 79 Fusion Centers across the country. Find location and contact information here: https://www.dhs.gov/fusion-center-locations-and-contact-information

What the Public Knows About Cybersecurity (Pew Research Center): https://www.pewinternet.org/2017/03/22/what-thepublic-knows-about-cybersecurity/

Americans and Cybersecurity (Pew Research Center): https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Cyber Resilience: Digitally Empowering Cities (J. Paul Nicholas, Jim Pinter, et al., Microsoft): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW6auc

Cybersecurity: Protecting Local Government Digital Resources (Microsoft and ICMA): https://icma.org/cyber-report

Cybersecurity Challenges to American Local Governments (Donald F. Norris et al., UMBC): https://ebiquity.umbc.edu/_file_directory_/papers/874.pdf

Cybersecurity: A Necessary pillar of Smart Cities: http://iranarze.ir/wp-content/uploads/2019/09/10116-English-IranArze.pdf

The Dangers of Smart City Hacking (IBM): https://public.dhe.ibm.com/common/ssi/ecm/75/en/75018475usen/final-smartcities-whitepaper_75018475USEN.pdf

National Cybersecurity Preparedness Consortium: http://nationalcpc.org/

National Cyber Security Alliance: https://staysafeonline.org/

Protecting Our Data: What Cities Should know about Cybersecurity: https://www.nlc.org/sites/default/files/2019-10/CS%20Cybersecurity%20Report%20Final_0.pdf

Endnotes

[1] Freed, B. (2019, September). Ransomware demanded $5.3M from Massachusetts city in July attack. *StateScoop*. Retrieved from https://statescoop.com/ransomware-demanded-5-3m-from-massachusetts-city-in-july-attack/

[2] National Association of State Chief Information Officers. (2019). 2019 *State CIO Survey*. Retrieved from https://www.nascio.org/wp-content/uploads/2019/11/2019StateCIOSurvey.pdf.

[3] Greenberg, P. (2018). Security Breach Notification Laws. Retrieved from www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[4] Lazzarotti, J. J., et al. (2018, April 9). State Data Breach Notification Laws: Overview of the Patchwork. *Jackson Lewis*. Retrieved from www.jacksonlewis.com/publication/state-data-breach-notification-laws-overview-patchwork

[5] BakerHostetler. *Data Breach Charts*. 2018, pp. 1–34.

[6] Freed, B. (2019, September). Texas starts mandatory cybersecurity training for government employees. *StateScoop*. Retrieved from https://statescoop.com/texas-mandatory-cybersecurity-training-government-employees/

[7] There is no public data or information available

[8] Michigan Technology, Management and Budget Department. (2015). *Michigan Cyber Initiative 2015*. Retrieved from https://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf

[9] Ibid.

[10] Mulholland, J. (2012, November). Michigan Launches ‘Cyber Range’ to Enhance Cybersecurity. *Government Technology*. Retrieved from https://www.govtech.com/Michigan-Launches-Cyber-Range-to-Enhance-Cybersecurity.html

[11] Greenberg, P. (2019, September). Statewide Cybersecurity Task Forces. Retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/statewide-cybersecurity-task-forces636129887.aspx

[12] Cyber Resilient Massachusetts Working Group. (n.d.). Retrieved from https://masscybercenter.org/cyber-resilient-massachusetts/cyber-resilient-massachusetts-working-group

[13] Boshart, R. (2015, December). Iowa Governor Calls on Tech Leaders to Craft State Cybersecurity Strategy. Retrieved from https://www.govtech.com/security/Iowa-Governor-Calls-on-Tech-Leaders-to-Craft-State-Cybersecurity-Strategy.html?utm_source=related&utm_medium=direct&utm_campaign=Iowa-Governor-Calls-on-Tech-Leaders-to-Craft-State-Cybersecurity-Strategy

[14] Cybersecurity Task Force Action Plan. (2016, December). Retrieved from https://www.cybersecurity.mo.gov/files/task_force/plans/FINAL_Cybersecurity_Task_Force_Action_Plan_12.29.16.pdf

[15] Gov. Hutchinson establishes computer science and cybersecurity task force. (2019, December 8). Retrieved from https://talkbusiness.net/2019/12/gov-hutchinson-establishes-computer-science-and-cybersecurity-task-force/

[16] Montana Information Security Advisory Council. (n.d.). Retrieved from https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC

[17] Currey, M., & Raymond, M. (2019, January 1). State of Connecticut 2018 Cybersecurity Update. Retrieved from https://portal.ct.gov/-/media/DAS/BEST/Security-Services/2018-Connecticut-Cybersecurity-Report.pdf?la=en

[18] KISO Services. (n.d.). Retrieved from https://oits.ks.gov/kiso/services

[19] Cybersecurity. (n.d.). Retrieved from https://www.marc.org/Government/Cybersecurity

[20] Kronos, J. D. (2019, January). The Role of Shared Services in Technology Investment. *Governing*. Retrieved from https://www.governing.com/topics/workforce/The-Role-of-Shared-Services-in-Technology-Investments.html

[21] Access To and Use Of Voter Registration Lists. (2019). Retrieved from https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx

[22] Shelley, K. and Williams, W. (2019, September). Election security isn’t that hard. *Politico*. Retrieved from https://www.politico.com/agenda/story/2019/09/10/election-security-000954

[23] Geller, E., et al. (2019, January). The scramble to secure America’s voting machines. *Politico*. Retrieved from https://www.politico.com/interactives/2019/election-security-americas-voting-machines/

[24] https://cyberflorida.org/

[25] About Cyber Florida. (2019). Retrieved from https://cyberflorida.org/about/

[26] Ward, M. and Brunner, M. (2020, January). Stronger Together: *State and Local Cybersecurity Collaboration*. Retrieved form https://www.nascio.org/wp-content/uploads/2020/01/NASCIO_NGA_StateLocalCollaboration.pdf

[27] Utah Department of Public Safety: Statewide Information & Analysis Center. (n.d.). Retrieved from https://siac.utah.gov/f-a-q/

[28] Hyer, M. M. (2019, November). Idaho continues partnership encouraging students to explore cybersecurity careers. Retrieved from https://gov.idaho.gov/pressrelease/idaho-continues-partnership-encouraging-students-to-explore-cybersecurity-careers/

[29] National Centers of Academic Excellence. (n.d.). Retrieved from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

[30] Ikeda, S. (2019, November). U.S. National Guard's Evolving Mission Includes Assisting Local Governments Experiencing Cyber Attacks. *CPO Magazine*. Retrieved from https://www.cpomagazine.com/cyber-security/u-s-national-guards-evolving-mission-includes-assisting-local-governments-experiencing-cyber-attacks/

[31] Ibid.

[32] Ibid.

[33] Wilkins, N. and Cook, K. (2019, July 2). First-of-its kind Cybersecurity Clinic to train 21st- century cyber professionals. *Indiana University*. Retrieved from https://news.iu.edu/stories/2019/07/iu/releases/02-cybersecurity-clinic.html

[34] Coble, S. (2019, November). Midwest to Get First Cyber Battalion. *Infosecurity Magazine*. Retrieved from https://www.infosecurity-magazine.com/news/midwest-to-get-first-cyber/

[35] Soucy, J. (2015, December 9). Guard set to activate additional cyber units. *National Guard Bureau*. Retrieved from https://www.nationalguard.mil/News/Article-View/Article/633547/guard-set-to-activate-additional-cyber-units/

[36] McClanahan, S. (2019, November 6). 169th Cyber Protection Team is capable and ready. *U.S. Army*. Retrieved from https://www.army.mil/article/229547/169th_cyber_protection_team_is_capable_and_ready

[37] Osbourne, H. (2019, October 29). State cyberteam helps agencies respond to uptick in ransomware attacks. *Statesman*. Retrieved from https://www.statesman.com/news/20191023/state-cyberteam-helps-agencies-respond-to-uptick-in-ransomware-attacks

NLC NATIONAL LEAGUE OF CITIES

CENTER FOR CITY SOLUTIONS