STATEMENT OF

THE HONORABLE STEPHEN SCHEWEL
MAYOR, CITY OF DURHAM, NORTH CAROLINA
ON BEHALF OF
THE NATIONAL LEAGUE OF CITIES

BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

“ADDRESSING EMERGING CYBERSECURITY THREATS TO STATE AND LOCAL GOVERNMENT”

JUNE 17, 2021

Introduction

On behalf of the City of Durham and the National League of Cities, thank you for the opportunity to provide testimony to the Senate Homeland Security and Government Affairs Committee's Subcommittee on Emerging Threats and Spending Oversight on a critical threat facing our nation. We appreciate the attention that Congress is giving to ways in which federal, state, and local governments can better collaborate to protect our public networks, infrastructure, and critical services from disruption, destruction, and expense due to cyberattacks. Our nation's cities, towns and villages are deeply concerned about the increasing toll that ransomware and other criminal attacks are taking on our localities and are eager to partner with Congress to strengthen our cyber defenses and resiliency.

We appreciate the efforts by federal agencies such as the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology, as well as state leaders and National Guard detachments, for their partnership and assistance to help our cities, towns and villages prevent, survive, and recover from cyberattacks. However, we believe more can be done. Localities do not have enough resources, whether in capital or workforce, to adequately protect our networks across the nation. Our cyber adversaries are increasing the sophistication, frequency, and impact of their attacks more every year, while spending on cyber defenses has not kept up.

Most municipalities are underprepared for a cyberattack. It is not a matter of if, but when, most communities will face a serious attack. Additional resources for both state and local governments will go a long way toward empowering our communities to work together with states and federal agencies to plan, prepare, harden against, and be able to recover quickly from cyberattacks. However, to be most effective, new federal resources must encompass several key principles: they must provide dedicated new resources without cannibalizing existing grant programs and budgets; they must promote intergovernmental partnership and collaboration, and they must not impose one-size-fits-all mandates on the tens of thousands of local government units in the United States.

About the City of Durham, North Carolina

The City of Durham, known as Bull City, is a thriving city in the Research Triangle region of North Carolina, with 287,865 residents. Our city provides a variety of daily critical services to our residents, including operation of a water and stormwater system, transportation systems management and maintenance, police, fire and 9-1-1 answering services, and sanitation. We employ 2650 employees in 24 departments. Despite benefiting from our size and proximity to a highly-qualified technical workforce, Durham has experienced its share of cyberattacks and this experience has led us to dedicate an increasing share of our technology services budget to cybersecurity.

On March 5, 2020, just as the full impact of the COVID-19 pandemic was beginning to be felt in the United States, both the City and County of Durham were hit by a ransomware attack. Throughout the process of halting, evaluating, and recovering our networks from the attack, the city's lights remained on. Public safety systems, including the 9-1-1 network, remained functional throughout, although the city did lose access to key networks while we went through the process of shutting down and restoring those files and systems from backup. The city was able to return to full levels of operation within only four days and took several weeks to reimage and harden our city's more than 2700 different endpoints, including 150 servers.

The City of Durham was fortunate to weather this experience with minimal disruption, but this was not an accident. Our city had planned in the months and years prior both to prevent such an attack, and to recover when an attack inevitably did occur. After a highly disruptive attack on the Durham Public Schools network in 2009 that impacted school operations for months, the City of Durham worked to put in place policies, procedures and plans to ensure that the City would not experience a similar costly disruption. The city established a comprehensive plan and budgeted for improvements over time. The city also established working relationships with the FBI, state leaders in North Carolina, and the Multi-State Information Sharing and Analysis Center (MS-ISAC). These plans were tested in 2018 when a second attack occurred, this time impacting the city's fleet vehicle network.

The lessons we learned from this process positioned the city to move quickly and decisively when attackers struck in 2020. The city was able to work quickly to form a war room with representatives from our staff, contractors, and other government partners, including the North Carolina National Guard, to respond to and recover from the attack. This was made particularly challenging as we navigated new social distancing protocols to keep our team safe and healthy throughout. However, because we had a plan and partnerships in place, including regular backups of all city data to the cloud, we were able to maintain functions critical for life and safety, and to restore full functionality quickly and without paying a ransom.

Local Governments are Experiencing an Unprecedented Quantity and Sophistication of Cyber Threats

Building strong cyber defenses for our nation's cities, towns and villages presents serious challenges. There are tens of thousands of local government units in the United States, ranging from very large cities like New York City and Los Angeles, to mid-sized and smaller cities like Durham, to the smallest rural towns. Municipal governments, regardless of size, often manage sensitive data about our residents and are responsible for systems critical to health and safety, including water and sewer systems, traffic control systems, public safety systems, sanitation, and more. The City of Durham operates a water utility. Other local governments may operate gas or electric utilities. As seen with the attack on the water system of Oldsmar, Florida this year, if bad actors are able to gain unfettered and undetected access to these critical systems, the consequences may not just be costly, but fatal.

Municipal systems are attractive targets for criminal actors. In recent years, local governments have become major victims of ransomware attacks, with at least $144.35 million in Bitcoin paid to criminals as ransom between the years of 2013 and 2019.[1] That figure does not include ransoms paid during the past year of increased attacks as organizations dramatically expanded virtual work environments, nor does it include the operational impact of downtime and recovery from ransomware attacks. The average downtime related to a ransomware attack is 9.6 days, and the recovery cost to impacted municipalities can easily reach the tens of millions of dollars.[2]

Over the past year, as many communities observed social distancing guidance, our cities were obliged to shift very rapidly to working and conducting public meetings remotely. This presented a very large new attack surface to criminal organizations. Suddenly, municipal employees were conducting the bulk of their work from potentially unsecured home networks, and local governments had to grapple with creating new ways to hold legally required public meetings that met standards of public disclosure and access, while also protecting the proceedings from things like Zoom-bombing. Our public information technology workforce has been in overdrive setting up our staff and elected officials with new equipment, training, and security awareness.

[1] Federal Bureau of Investigation, "The National Cyber Investigative Joint Task Force Releases Ransomware Fact Sheet," February 4, 2021. Available https://www.fbi.gov/news/pressrel/press-releases/the-national-cyber-investigative-joint-task-force-releases-ransomware-fact-sheet

[2] KnowBe4, "The Economic Impact of Cyber Attacks on Municipalities," 2020. Available https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf

Ultimately, a criminal organization only must be right once when attempting to breach our systems. Our local governments must be right every time. While communities like Durham have made great strides in recent years in terms of implementing the best practices outlined by organizations like NIST and increasing the level of awareness and cyber hygiene among our elected leaders and staff, these measures are not enough on their own. Cyber criminals rely not only on social engineering tactics and careless end users, but on sophisticated attack methods to penetrate and disrupt our networks. Protection in the future will require both increased training and awareness for our teams, as well as ongoing work to keep our systems updated, backed up, and continually monitored for threats and intruders. This will not be a one-time action, but an ongoing and continuously evolving process.

Cities, Towns and Villages Have Serious Capacity Limitations

Durham is fortunate to have a fantastic city staff team to guide our cybersecurity strategy and advise our council and city manager as we budget for cybersecurity and technology expenditures. Our city also has an active partnership with local academic institutions that is helping to build our local technology workforce pipeline and create opportunities for local students. For Fiscal Year 2020-2021, the City Council approved a General Fund budget of $214.6 million, of which $9.14 million supports our Department of Technology Solutions. This represents about 4.3 percent of our city's core budget. Our Technology Solutions program must support a number of other priorities and activities in addition to cybersecurity, including our city's general technical support for employees and systems across a wide variety of activities, our open data program, as well as our city's geographic information systems (GIS) activities in partnership with the County of Durham.

Information technology generally, and cybersecurity specifically, must compete with a wide range of other city priorities in all communities. The American Society of Civil Engineers estimates that the nation's infrastructure, much of which is owned and operated directly by local governments, requires $2.59 trillion more in repair and upgrades over the next decade than is currently funded.[3] This means that cybersecurity expenditures must compete directly with activities like filling potholes, repairing water systems, modernizing 9-1-1 answering centers, and maintaining parks, all of which are much more visible to residents.

[3] American Society of Civil Engineers, "Investment Gap 2020-2029." Available https://infrastructurereportcard.org/resources/investment-gap-2020-2029/

Cities are also under substantial budgetary pressure in terms of revenues. Cities, towns and villages in at least 48 states are limited by at least one state- or voter-imposed tax and expenditure limit, which can restrict the ability of localities to raise funds.[4] These can include limits on tax rate, tax growth or overall total revenue increases from common revenue sources like property taxes. Tax and expenditure limits can hinder the ability of municipalities to expand reserves and investments when the economy is performing well and limit the capacity for a community to respond in a crisis.

Small Municipalities Have Unique Challenges

The City of Durham is fortunate, but we have still needed to make tough choices. Other communities are much less fortunate. More than 80% of municipalities in the United States are small, with populations below 50,000 and substantially fewer resources than the City of Durham. In these smaller communities, staff and budgets are seriously limited, with a single information technology staff person responsible for a wide variety of functions, including security – if the community has a full-time IT staff person at all. In a 2020 survey of local government IT executives, the Public Technology Institute found that 65.2% of respondents felt that their cybersecurity budget was inadequate. Less than half of respondents indicated that their local governments had a cyber incident response and disaster recovery plan that was tested annually.[5]

Many local governments, including nearly all small local governments, outsource IT functions and services. It is difficult for most city governments to attract a stable, qualified workforce with the necessary qualifications to maintain a cybersecurity program, and frequently does not make business sense to manage all of these functions internally. However, it is not always clear whether vendors are upholding strict cybersecurity standards of their own, and outsourcing cybersecurity is not a foolproof strategy to eliminate risk. In 2019, 22 Texas cities and counties were impacted by a serious ransomware attack that gained access to the cities' networks via a common managed service provider.[6] Individual communities, particularly smaller communities, cannot ensure the

[4] National League of Cities, "Local Budget Pressures are Real. So Why Don't Cities Just Raise Taxes?" June 1, 2020. Available https://www.nlc.org/article/2020/06/01/local-budget-pressures-are-real-so-why-dont-cities-just-raise-taxes/

[5] Public Technology Institute/CompTIA, "2020 Public Technology Institute (PTI) State of City and County IT National Survey," October 29, 2020. Available https://comptia.informz.net/COMPTIA/data/images/2020/Misc/2020-PTI-State-of-City-and-County-IT-National-Survey.pdf

[6] ProPublica, "The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once," September 12, 2019. Available https://www.propublica.org/article/the-new-target-that-enables-ransomware-hackers-to-paralyze-dozens-of-towns-and-businesses-at-once

qualifications of all possible vendors, nor can they be responsible for managing the security of hardware and software supply chains upon which they rely.

In many ways, operating a smaller town or village poses similar challenges to those faced by small businesses. They have fewer resources, but are no less vulnerable to cyber threats, and the consequences for a cyberattack are no less serious in their communities than in larger ones. They are also just as responsible for the wellbeing and data protection of their employees and residents as a larger city is. Because of their smaller scale, it does not make sense to keep many cybersecurity or information technology services and capacities in-house. However, it is also difficult for these communities to stay on top of changing best practices, procure managed cybersecurity services, software as a service, and outsource technical staffing, because they have trouble achieving economies of scale and adequately vetting vendors.

Policy Solutions for Building a Stronger Intergovernmental Partnership

Local governments are under a serious and growing threat of catastrophic cyberattack. The risks to local health, safety, and economic stability cannot be denied. The federal government cannot solve this problem with mandates: requirements to implement stronger security measures, training, and technological solutions for response are out of reach for most municipalities without additional support. Even relatively simpler best practices, such as maintaining current hardware and software, applying patches and updates on recommended cycles, implementing cyber hygiene training across the entire user base, requiring multifactor authentication and password complexity for all users, and data backups, are substantial and ongoing expenses for local governments of all sizes. For larger local governments, these activities are important, if sometimes challenging, to prioritize and budget for. For smaller towns, they may be entirely out of reach.

The federal government has an opportunity to not just financially support these activities, but to partner actively with state and local governments to improve cyber resiliency across all levels of government. The National League of Cities recommends any new federal cybersecurity legislation address several core principles:

1. Provide sustainable new funding, without cannibalizing existing funds;
2. Actively promote planning, information sharing, and business partnerships between units of government; and
3. Avoid the temptation to apply a top-down, one-size-fits-all solution to widely varying sizes and forms of local governments.

Congress Should Provide Sustainable New Funding Without Cannibalizing Existing Funds

New sources of funding are desperately needed for local government cybersecurity – but they must not come at the expense of existing public safety or homeland security resources, and they must persist over time. While a one-time infusion of resources can help a city do one-time things, such as conduct needed network or hardware upgrades, conduct risk audits, or create an initial plan for risk mitigation and response, most cybersecurity expenses are ongoing. Network monitoring, staff resources to track and apply needed patches and updates, and data backups are all key elements of reducing cyber risk and recovering effectively from an attack, and they are all significant ongoing expenses that must be maintained and budgeted from year to year. A one-time grant can help kickstart additional activities around cybersecurity and make them more affordable, but a single grant will not be a silver bullet for cybersecurity.

These grants must be reasonably flexible to account for the kinds of expenses best suited to these single-use needs. For example, after taking over administration of the .gov domain following passage of the Consolidated Appropriations Act in December of 2020, CISA elected to fulfill its congressional directive to incentivize adoption of the .gov domain by making it available free to government entities.[7] This is an important step in removing barriers to transitioning to a more secure domain for local governments but does not account for additional costs related to domain transition, such as staff time to manage the process, redesign of municipal graphic materials, and reprints of signage, business cards, and other tangible resources. These additional costs may be significant enough to discourage a municipality from changing domains, and should be considered in new grant programs.

Additionally, new resources must not come at the expense of existing grants to state and local government from the Department of Homeland Security. The existing 7.5% carveout for cybersecurity introduced this year within the Urban Area Security Initiative and State Homeland Security Program grants ultimately serves to increase the number of things state and local governments are attempting to do with a finite budget, rather than sustainably increasing the support available for cybersecurity specifically. Congress should also consider not requiring, or minimizing, cost sharing for these programs to incentivize participation by eligible units of government.

[7] Dotgov, "A new day for .gov," April 27, 2021. Available https://home.dotgov.gov/2021/4/27/a-new-day-for-gov/

New Federal Cybersecurity Programs Should Promote Collaborative Planning, Information Sharing, and Business Partnerships Between Levels and Units of Government

Any new federal cybersecurity programs should prioritize promoting intergovernmental partnership and collaboration. While local governments are ultimately individually responsible for their own security, the federal government can serve as a key central distributor of information, resources and assistance, and state governments can play similar roles within their jurisdictions. For example, the North Carolina National Guard and local governments in the state increasingly collaborate on cyberattack prevention and response, and additional resources would support the enhancement of these efforts.

The Cyberspace Solarium Commission recognized the critical role of the federal government when recommending that the Cybersecurity and Infrastructure Security Agency be granted additional funding and authority to conduct larger-scale and more advanced assistance and coordination to partners outside the federal government.[8] As attacks on energy and water systems increase, clarity around federal agencies' respective roles in preparing for and recovering from cyberattacks is also critical to ensure that local governments are operating as effectively as possible in hardening their own cyber defenses and creating or practicing incident response plans.

Procurement of solutions and services is another area ripe for additional intergovernmental collaboration. As noted previously, cybersecurity challenges are particularly severe for mid-sized and smaller municipal governments. Regional government councils, states, and municipal leagues can play a key role in achieving economies of scale in procurement, distributing information, and providing support in response to cyberattacks. Larger entities should be incentivized to consider offering assistance in procurement, such as through state purchasing portals, access to statewide contracts, or provision of certain solutions or services at cost. Federal and state entities are also well-positioned to share information about qualified vendors and products that meet minimum performance or security standards, and the federal government is positioned to establish and uphold those standards for protocols, software, and hardware supply chains. By lowering cost barriers to these tools, as well as making it easier for local governments to ensure that the purchases and contracts they make individually are adequate, federal and state

[8] Report of the U.S. Cyberspace Solarium Commission, March 2020, p. 39. Available http://www.google.com/url?q=http%3A%2F%2Ffdd.org%2Fwp-content%2Fuploads%2F2020%2F03%2FCSC-Final-Report.pdf&sa=D&sntz=1&usg=AFQjCNEjLcRR29lrpmdRUZe1aFf2Bb6EGg

governments can make it easier for local governments to meet their responsibilities within the partnership.

Congress Should Not Apply One-Size-Fits-All Solutions to Local Governments

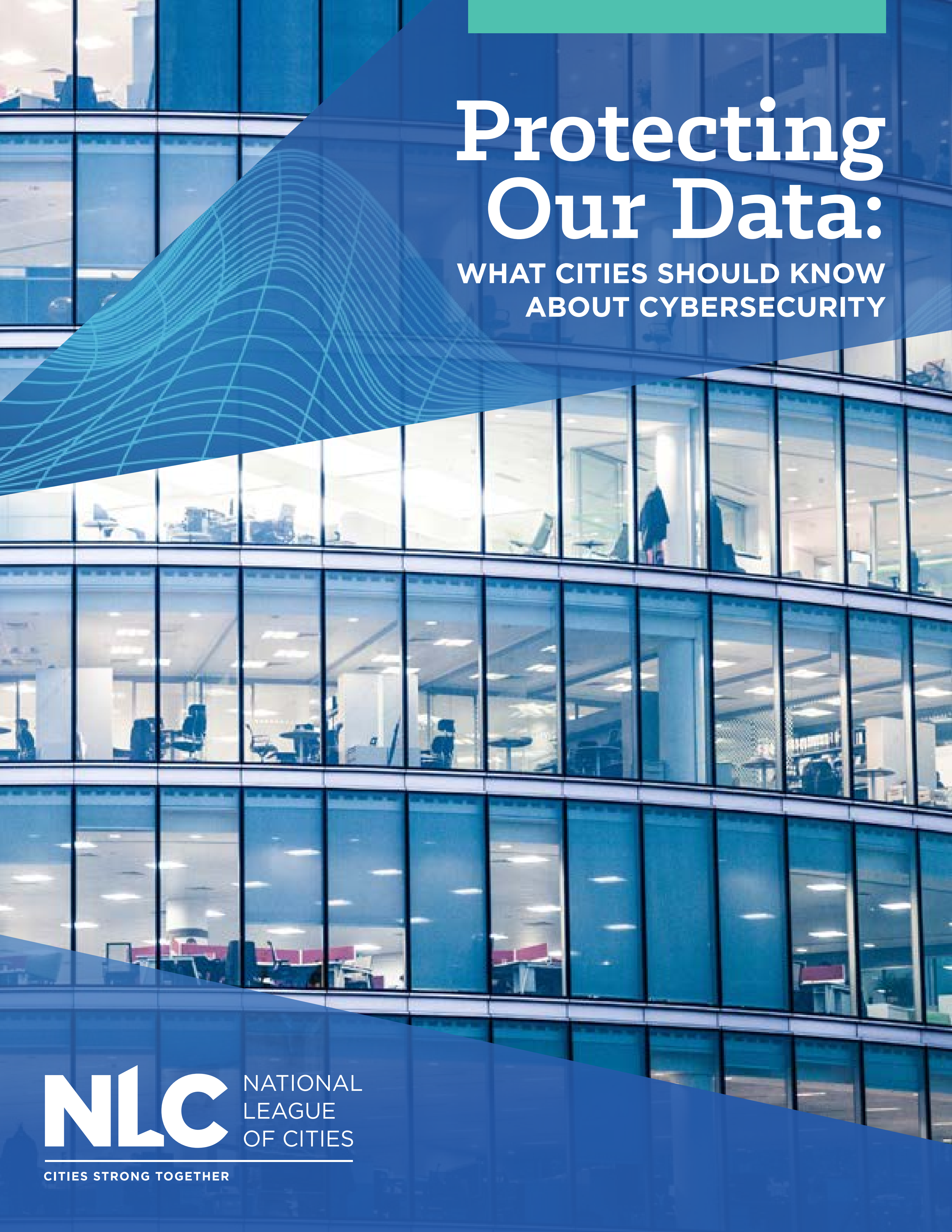
Lastly, Congress should avoid the temptation to apply a top-down, one-size-fits-all approach to local government cybersecurity. The largest cities have populations of millions, with tens of thousands of full-time employees, while the smallest towns and villages have populations measured in the tens and no full-time staff. Large municipalities are capable of effectively accessing and deploying direct federal grant dollars quickly, without additional processing through state entities, while smaller local governments may benefit from service provision or assistance through state entities. Each municipality has different assets, network architectures, and local resources available to them. Ideally, any new federal cybersecurity grant program should allow those municipalities capable of effectively managing a federal grant directly to do so, while also providing for state administration of dedicated streams of funding available to support smaller local governments.

Any state programs, whether cybersecurity incident response plans, grant systems, or business offerings, should be developed in collaboration with their local governments and with substantial local input. While federal and state agencies may bring to bear greater resources than most municipalities, they need the “eyes on the ground” provided by local officials, who have the most familiarity with their own systems, capabilities, and needs. Programs such as those outlined in the State and Local Cybersecurity Improvement Act rightly require local officials to have a seat at the table for all planning and advisory committees.

Conclusion

America’s cities, towns and villages are eager to partner with the federal and state governments to harden our collective defenses against cyber criminals. Cyberattacks, whether ransomware or other forms of intrusion, are incredibly costly for local governments and represent serious threats to the life and wellbeing of our residents. However, we cannot adequately protect our nation’s residents, economy, and infrastructure without substantial additional investment and partnership from Congress. The substantial, ongoing, and increasing expenses and actions necessary to secure our cities have outstripped the ability of many communities to keep up. The City of Durham and our fellow local leaders look forward to continuing this conversation with the members of the Senate as we develop a path forward.

APPENDIX



Protecting Our Data:

WHAT CITIES SHOULD KNOW ABOUT CYBERSECURITY

NLC NATIONAL LEAGUE OF CITIES

CITIES STRONG TOGETHER

NLC NATIONAL LEAGUE OF CITIES
CITIES STRONG TOGETHER

pti Public Technology Institute
CompTIA

About the National League of Cities
The National League of Cities (NLC) is the nation's leading advocacy organization devoted to strengthening and promoting cities as centers of opportunity, leadership and governance. Through its membership and partnerships with state municipal leagues, NLC serves as a resource and advocate for more than 19,000 cities and towns and more than 218 million Americans. 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

Kyle Funk, Program Specialist of City Solutions

Cooper Martin, Director of Sustainability & Solutions

Nicole DuPuis, former manager of the Urban Innovation program at NLC's Center for City Solutions

Alan Shark, the Executive Director and **Dale Bowen** is Managing Director, Public Technology Institute at CompTIA.

Acknowledgements
NLC is grateful for the guidance and review from the Public Technology Institute; Angelina Panettieri, Principal Associate for Technology and Communications, Federal Advocacy and John Manwell, Program Director for Information Technology at NLC; and Dan Lohrmann, Chief Security Officer & Chief Strategist at Security Mentor, Inc.

Table of Contents

Foreword

Many of us remember a time before technology permeated every aspect of life – including our local governments. Not so long ago, our communities ran on filing cabinets stuffed with documents, fax machines and paper public transit schedules. Our timecards and records were kept by hand, and resident engagement only happened in-person or over the phone.

Today, our communities have moved online. This change has made many aspects of modern life more efficient. But this digital revolution is happening quickly, often at a pace faster than we can keep up with. As a result, individuals and institutions alike have been left vulnerable to hackers and ransomware.

Every day in the United States, a local government is hacked. Since 2013, ransomware attacks have impacted at least 170 county, city, or state government systems. The damage can cost millions, but the loss of public trust and safety come at an even higher price.

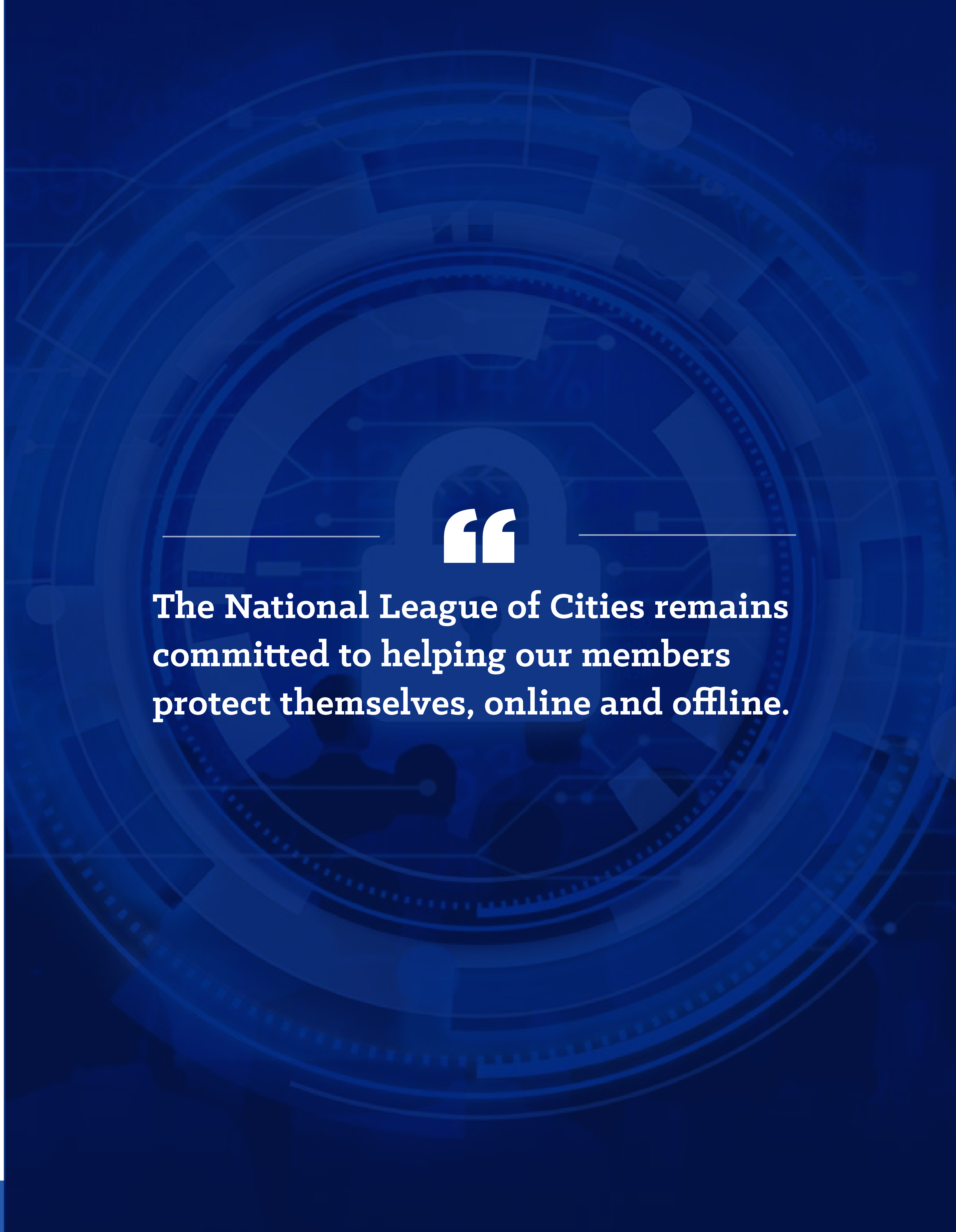
Despite being a primary target for hackers, local governments continue to integrate technology into their day-to-day operations and are increasingly collecting massive amounts of data. The pressure on cities to become "smarter" and more connected is mounting.

This rush toward digitization has resulted in a frenzy of competition and anxiety about being left behind, or not being able to provide the right services to their residents. As local leaders consider the risks and rewards of greater connection, they must also consider the crucial need for cybersecurity.

The National League of Cities remains committed to helping our members protect themselves, online and offline. That is why we are proud to release "Protecting Our Data: What Cities Should Know About Cybersecurity" in collaboration with the Public Technology Institute. This guide will help local leaders prepare and implement systems to protect their institutions online.

New technologies have the potential to create a brighter, more equitable future for the people in America's cities, towns and villages. But, cybersecurity and smart city initiatives must go hand-in-hand. If we continuously invest in the people and systems needed to keep our information secure, our communities will thrive.

Clarence E. Anthony
CEO and Executive Director, NLC



"

The National League of Cities remains committed to helping our members protect themselves, online and offline.

Introduction

The White House reported that there were 77,200 cyber incidents in 2015 occurring in federal agencies alone. The Federal Trade Commission (FTC) received more than 800,000 consumer fraud and identity theft complaints, where consumers reported losses from fraud of more than $1.2 billion. Security threats from the "outside" are increasing in frequency and sophistication, but most of the greatest threats are coming from users "within" – network users who click on malicious links, open email attachments that contain viruses, or make other mistakes that allow hackers to gain access.

Public services are going digital. At the most complex level, this requires policymakers to understand, manage and regulate the use of facial recognition software and micromobility technology like e-scooters, energy storage, smart energy meters or autonomous vehicles. But data is also increasingly at the core of more fundamental services such as trash collection, building and zoning permitting, fleet management, public facility operations, utility maintenance and even tree inventories. The pressure on cities to become "smarter" or more connected is mounting, resulting in a frenzy of competition and anxiety about being left behind. A report from the McKinsey Global Institute estimates that the economic impact of the internet of things (IoT) in smart cities could surpass $1.7 trillion worldwide in 2025.[i]

Local governments do not often think of themselves as tech organizations, but nearly everything a government does depends on its ability to create, maintain and share large quantities of data — and to ensure that data is secure. Undoubtedly, the confluence of government and technology has great potential for cities to improve service quality and efficiency. But embracing technology-driven governance is not without risk.

Today's networks are constantly being probed for weaknesses and vulnerabilities. All organizations must deal with these threats as technology continues to play a larger and larger role in business and governance. From Russia disrupting Ukraine's infrastructure and breaches of corporations such as Equifax and Marriott, to attackers targeting American cities like Atlanta, Baltimore, and Riviera Beach, FL, ransomware and email scams plague internet users daily.

Local leaders should make cybersecurity an administrative and budgetary priority. When a local government is the victim of an attack, the cost can far exceed that of proactive investment in cybersecurity. In 2016, the average cost of a data breach was estimated to be about $6.53 million.[ii] However, in many cities, the cost can be even higher, and the price of failing to secure our networks is clearly rising. The cost for Atlanta to recover from its ransomware attack was estimated around $17 million.[iii] Similarly, the recent Baltimore ransomware attack is predicted to cost over $18 million.[iv]

While there are several examples of high visibility hacks on the private sector, there are three main reasons why the concerns are very different when a local government falls victim to a breach:

- Governments collect and maintain **far more sensitive information** than most private sector companies.
- Residents **can't easily move** or choose a competitor if they are unhappy with their local government service and security.
- Trust in government is eroding, and security breaches may further **reduce faith in government.**

Cybersecurity and smart city initiatives must go hand in hand as local leaders continue to invest in 21st century infrastructure. This municipal action guide is a collaboration of the National League of Cities and the Public Technology Institute. Our aim is to strengthen cybersecurity policies and systems in local governments. The guide looks at the state of cybersecurity in local governments and includes policy recommendations for local leaders to implement in order to keep their residents, and their own data, safe. To get a clearer picture of the state of cybersecurity in local governments today, NLC and PTI conducted a small survey of PTI's IT members and NLC's Information Technology Committee (ITC). We found that while local governments are making improvements, they still lack support from elected leaders and face budget constraints that limit their abilities to improve cybersecurity further.

There are many simple and effective steps cities can take to avoid vulnerabilities and reinforce cybersecurity best practices:

- Identify one individual to be responsible for cybersecurity programs in that jurisdiction
- Make digital hygiene an institutional priority
- Educate the local workforce, elected leaders and residents about cybersecurity
- Conduct an analysis of local government vulnerabilities
- Ensure your data is properly backed up
- Implement multi-factor authentication
- Create policies or plans to manage potential attacks
- Ensure public communication is part of your attack response plan
- Adopt a dot gov (.gov) address to reduce risk of fraudulent municipal websites
- Work with educational partners to create a cybersecurity talent pool

No network can be 100 percent secure, but by following the recommendations in this guide, local government leaders can reduce the risk of a cyber-attack and be more resilient when one does occur.

What is Cybersecurity?

DEFINITIONS YOU SHOULD KNOW

CYBERSECURITY
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.

MALWARE
Short for "malicious software," this software is designed specifically to damage or disrupt a system, such as a virus.

RANSOMWARE
A type of malware that threatens to publish or block access to data until a ransom is paid

BREACH
An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party

PHISHING
The illegal practice of sending email claiming to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and social security numbers

How Prepared are Cities?

NLC and PTI conducted a survey of IT officials representing local governments from across the United States to prepare for this survey. PTI sent the survey out to their broader membership while NLC targeted members of our Information, Technology and Communications Advocacy Committee, generating 165 responses:

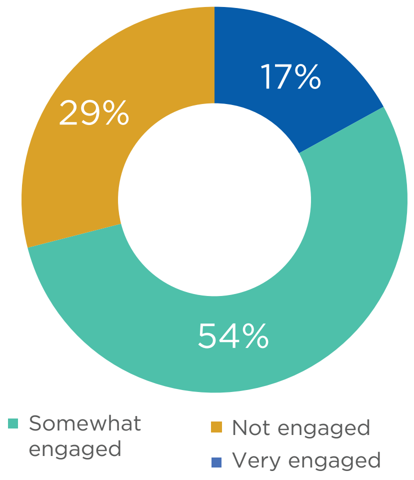
45% represent communities with a population under **50,000**

33% represent local governments in the **50,000 to 150,000** population range

22% represent local governments **above 150,000** in population.

HOW ENGAGED ARE YOUR LOCAL OFFICIALS IN CYBERSECURITY EFFORTS?

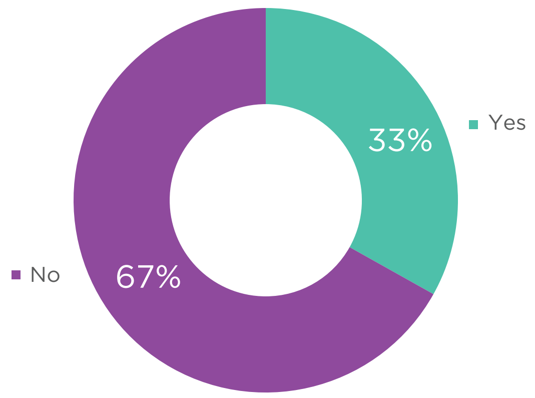
Only 17 percent of respondents say their local elected officials are very engaged in cybersecurity efforts. In fact, 29 percent admitted that they were "not engaged" at all.



IS YOU BUDGET ADEQUATE ENOUGH TO SECURE THE NETWORK PROPERLY?

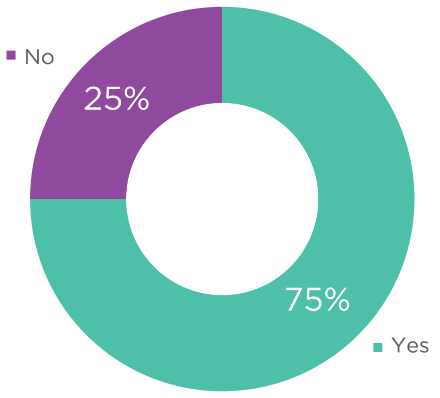
When asked if the local government's budget was adequate, 67 percent of respondents said it was high enough to secure the network properly.

Over half of those who answered the survey said that elected officials tended not to prioritize cybersecurity budgets and policy.

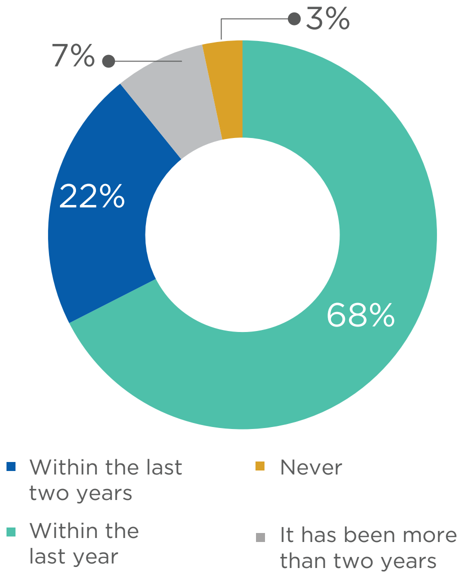


DOES YOU LOCAL GOVERNMENT HAVE A CYBERSECURITY PLAN/STRATEGY?

Over three-fourths (75%) of local governments have a cybersecurity plan/strategy in case of an attack. These plans also include the steps to recover data should the system be breached.

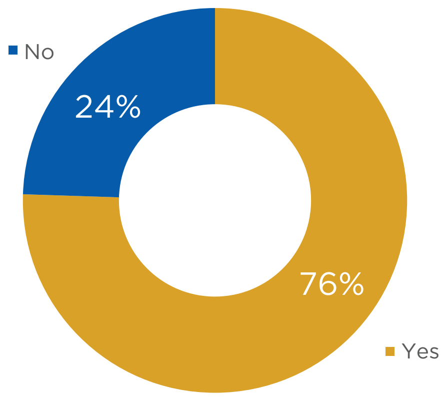


IF YOU HAVE A CYBERSECURITY PLAN, HOW OFTEN IS IT REVIEWED?

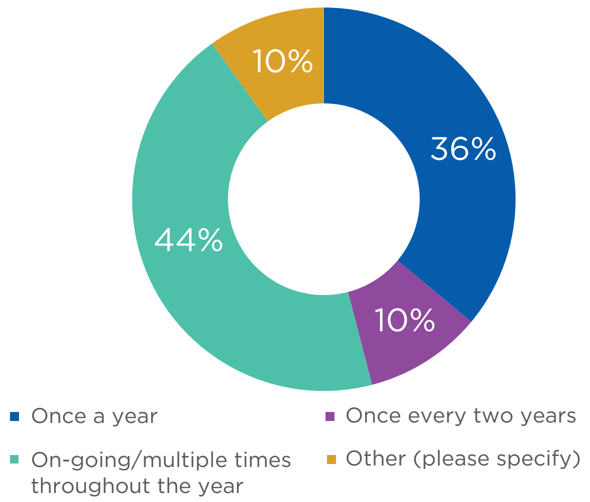


However, only 68 percent of these plans have been reviewed in the last year. This is troubling, since annual audits are considered a best practice with ever-changing technology and threats.

DOES YOUR JURISDICTION PROVIDE FOR EMPLOYEE AWARENESS TRAINING (WHAT TO DO AND WHAT NOT TO DO WHEN IT COMES TO CYBER SECURITY)?



IF YES, WHAT IS THE FREQUENCY?



PTI and NLC's survey revealed that around 76 percent of respondents conduct employee awareness trainings. While most (80%) conduct these trainings yearly, a few local governments only conduct cybersecurity training at employee onboarding.

The information collected by NLC and PTI are consistent with prior research and analyses in local government cybersecurity, indicating that little progress is being made to improve security in the face of mounting threats. In 2016, the International City/County Management Association (ICMA) and the University of Maryland, Baltimore County, conducted the first-ever survey of U.S. local governments about their cybersecurity practices and experiences. Their results revealed an alarming state of unawareness and unpreparedness for the majority of the 3,423 local governments they surveyed. These risks may cost local governments significant money and time as they seek to reverse the effects of a cybersecurity incident.

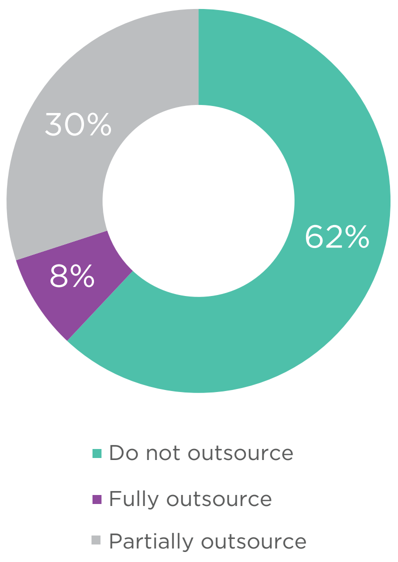
The most alarming result from the survey dispels the myth that cities, towns and villages are safe from attacks by bad actors. The survey found that 44 percent of local governments report an attack from a cyber incident hourly (26 percent) or daily (18 percent). That number rises to 66.7 percent over the duration of a year. But what is even more alarming is the large number of local governments that do not know how often they are attacked (27.6 percent), experience an incident (29.7 percent) or a breach (41.0 percent).

Worse still, while 88.8 percent of local governments know that most incidents come from external actors, nearly one-third (31.9 percent) do not know if the attacks were from an internal source or an external one. Even though local governments constantly experience incidents, a majority do not catalog or count attacks (53.6 percent).[v]

According to the ICMA/Univeristy of Maryland, Baltimore County survey, local governments are trying to improve cybersecurity resilience through policy planning. The top policies that governments adopted included rules regarding how passwords are created, requirements on the frequency that end users must change their passwords and use of employee personal electronic devices on local government systems. Even though these policies were adopted, most officials incorrectly wrote them off as ineffective to increasing cybersecurity.[vi] The experts also noted in the paper that maintaining a strong cybersecurity culture with all users was vitally important. A strong cybersecurity culture means keeping good digital hygiene on top of mind, and sharing responsibility between all end users — not just the IT department or officials.

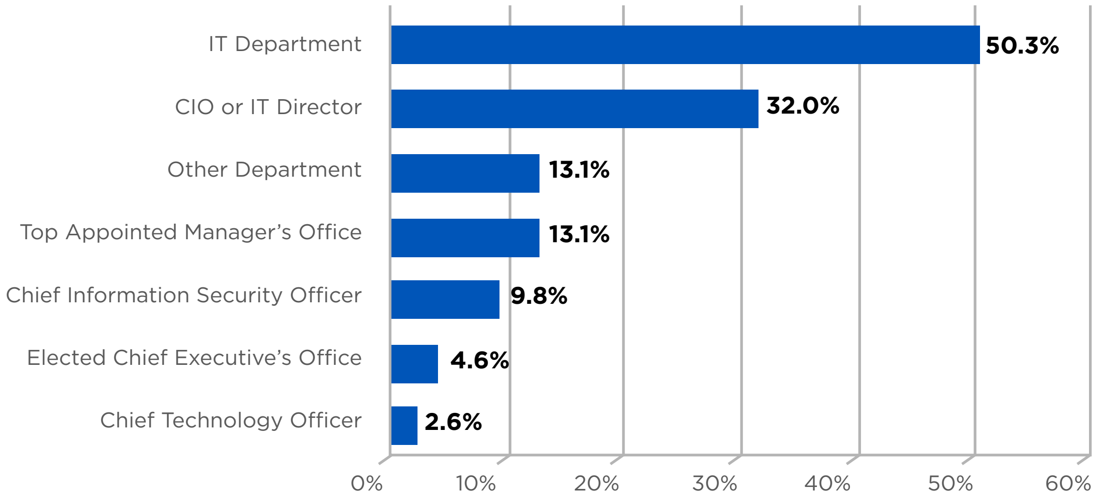
Though the ICMA/University of Maryland, Baltimore County survey revealed alarming cybersecurity results, the NLC/PTI survey shows that local governments are starting to adjust to the dangers the cyberworld presents. Three years have passed since the two surveys and cities, towns and villages seem to be progressing on cybersecurity. However, bad actors have not sat idly by. Nowadays, cybersecurity work will require constant evolution and local governments are best adapted to prepare and innovate solutions that can help the whole country remain secure.

DOES YOUR LOCAL GOVERNMENT OUTSOURCE ANY OF ITS CYBERSECURITY FUNCTIONS?



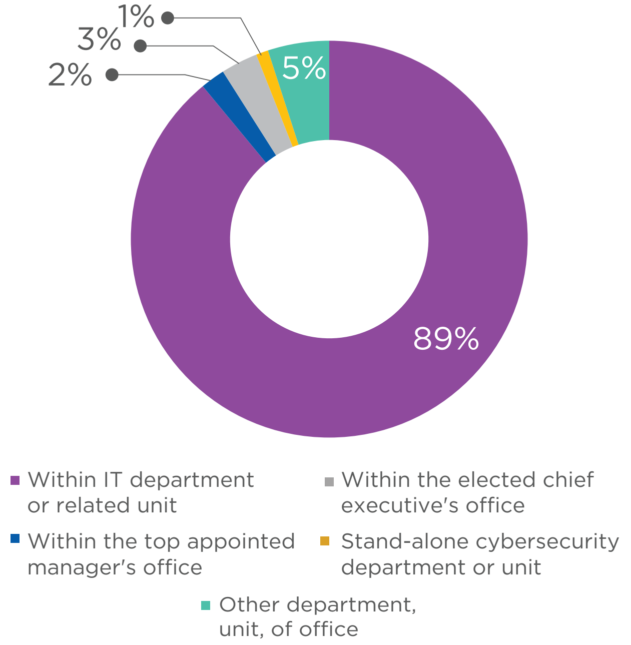
Graph courtesy of ICMA/University of Maryland, Baltimore County.

IF OUTSOURCED, TO WHAT OFFICE OR OFFICIAL IN YOUR LOCAL GOVERNMENT DOES THE CONTRACTOR(S) TO WHOM YOU OUTSOURCE CYBERSECURITY REPORT?



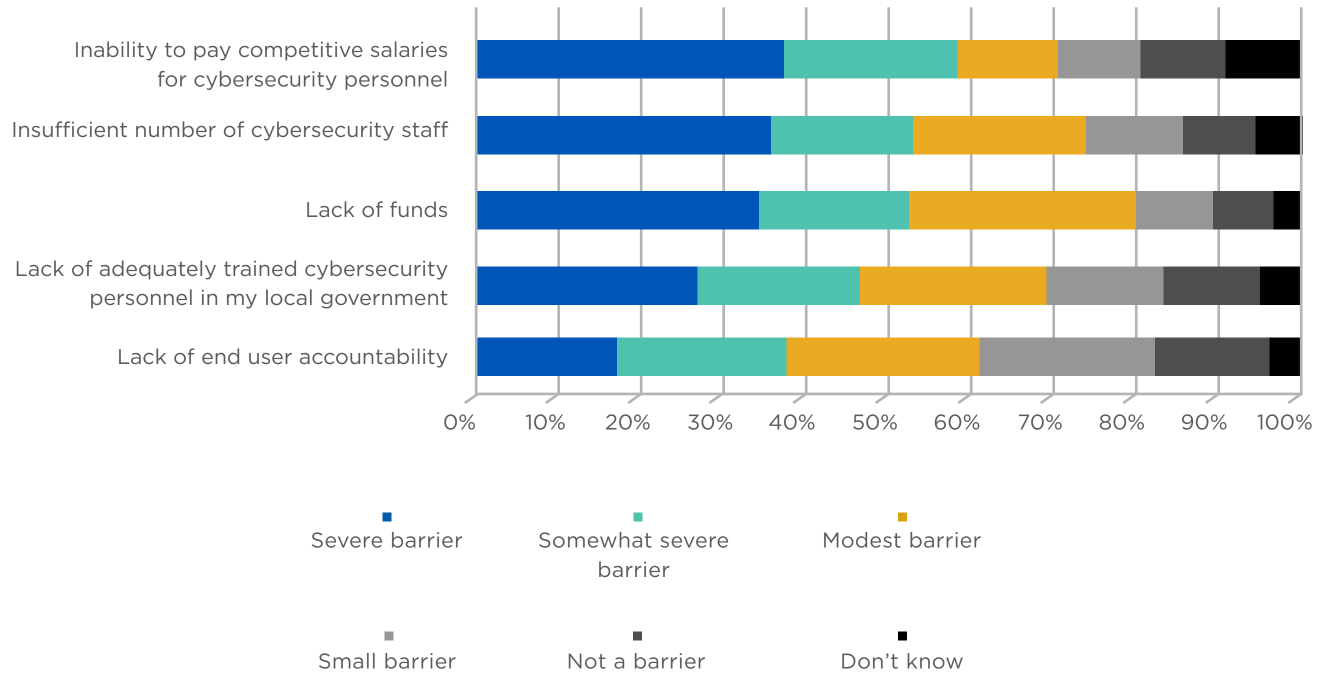
Graph courtesy of ICMA/University of Maryland, Baltimore County.

WHERE IS THE PRIMARY RESPONSIBLY FOR CYBERSECURITY LOCATED IN YOUR LOCAL GOVERNMENT'S ORGANIZATION?



Graph courtesy of ICMA/University of Maryland, Baltimore County.

TO WHAT EXTENT IS EACH OF THE FOLLOWING A BARRIER FOR YOUR LOCAL GOVERNMENT TO ACHIEVE THE HIGHEST POSSIBLE LEVEL CYBERSECURITY?



Graph courtesy of ICMA/University of Maryland, Baltimore County.

Private Sector Perspectives:

6 STRATEGIES FOR CYBER SECURE CITIES

Haiyan Song, Senior VP and GM, Security Markets, Splunk

Cities are increasingly focused on cybersecurity best practices, with several high-profile attacks in recent years causing major disruptions to city operations across our nation. Developing the practices and tools to protect our cities from ransomware, cryptomining and a wide range of emerging threats is vital to safety, data protection and the security of the critical infrastructure that cities manage. But there's hope in the chaos. The ability to dramatically improve your cybersecurity defense is within reach for the largest cities and smallest towns, provided we work together across all levels of government, academia and private sector partners.

Last fall I was honored to host a cybersecurity roundtable with the National League of Cities at Splunk's San Francisco headquarters, where I shared advice from my years of conversations with cybersecurity experts around the globe in every industry. Here are some of our observations:

1. **CITY LEADERS NEED TO UNDERSTAND THAT CYBERSECURITY ISN'T JUST AN IT DEPARTMENT CHALLENGE.** It's the responsibility of the entire organization, and the buck ultimately stops with leadership. In the private sector, there's no question that cybersecurity is now a CEO and board-level responsibility, and recent cyber incidents for local governments have made it clear that mayors, city managers and councilmembers must be informed and ready to lead on this issue. City leaders need to align with their IT and security staff and stay informed about cyber risks and their potential impact to the city.

2. **CITIES NEED TO START IMPROVING THEIR DEFENSES AND KEEP MOVING.** There is no "finish line" when it comes to cybersecurity. It's a continuous journey. No matter where your city is in its cybersecurity defense maturity, it's important to commit to always moving forward. Threats are always evolving, which means your strategy to monitor, detect and act on risks must as well. Has your city adopted a risk-based cybersecurity framework, such as the one from the National Institute for Standards and Technology (NIST)? Does your city have a cyber incident response plan? If so, how often is it tested?

3. **CYBERSECURITY IS A TEAM SPORT.** Just as cities proactively form partnerships to prepare for natural disasters, it is critical that cities forge strong partnerships for cybersecurity incident response before disaster hits. Even the most technologically mature cities will struggle with resources if they are hit with a major cybersecurity incident. Cities must play an active role in sharing and collaborating with each other, other levels of government and security industry partners.

4. **CITIES NEED TO UNDERSTAND THAT THE CYBERSECURITY TALENT GAP IS A GLOBAL PROBLEM WITH MILLIONS OF UNFILLED POSITIONS,** and everyone is scrambling to recruit and train the next generation of cyber defenders. Do your local universities, community colleges or high schools have cybersecurity programs? Identify both short- and long-term talent pipelines for cybersecurity in your region. Be a champion of these programs and your cities will benefit.

5. **BUDGETS ARE IMPORTANT.** City IT leaders have been red flagging cybersecurity and the lack of an adequate budget as their top priority for years. Does your city have a dedicated cybersecurity budget? Is that budget realistic to provide the protection you're aiming for?

6. **LASTLY, THERE'S AN IMPORTANT QUESTION ALL LOCAL GOVERNMENTS SHOULD ASK: DOES YOUR IT LEADERSHIP HAVE ACCESS TO THE MODERN TOOLS IT NEEDS TO DO ITS JOB EFFECTIVELY?** A modern cybersecurity practice fundamentally comes down to being smarter with data than those looking to do you harm or hold your data for ransom. Big data analytics, machine learning and even artificial intelligence (AI) aren't futuristic fantasies, they're the core technologies of today's cybersecurity defenses.

It's paramount that all city leaders look at security as a mission enabler and not just a checkbox. The most advanced cities I come across understand that data needs to be at the heart of any security operations center (SOC). And there's a hidden pot of gold in putting advanced data analytics at the center of your security strategy. We've seen countless enterprises that learned the modern skills of being "data driven" through their cybersecurity practices, and then transformed their organizations by transferring those skills into their core missions. There are even examples of organizations taking the data skills and machine learning tools they use for cybersecurity and applying them to pressing policy issues like combating the opioid crisis and human trafficking.

Policy Landscape and Resources for Local Governments

Cities are not alone in this effort to secure public information. Several state governments are stepping up to assist cities as they identify areas of cybersecurity vulnerability. Local leaders should be aware of what their own state might offer, and advocate for programs that have been successful from other state governments.

Examples of this work can be found in Georgia and West Virginia, which are cultivating state government ecosystems to help cities improve their cybersecurity defenses. Georgia offers consultations to all municipalities upon request. They do this by creating IT contracts that allow them to work for local governments for general purpose or incident response needs.[vii] West Virginia has also followed this route, setting up state contracts to allow local governments to take advantage of state resources.[viii]

New York and Virginia are attempting to help local governments with different approaches. New York's Department of Homeland Security and Emergency Services is helping local governments evaluate their vulnerability assessments against the Cybersecurity Framework developed by NIST. Virginia, on the other hand, is tackling cybersecurity with help from the military. The state has mobilized its National Guard to 'State Active Duty' status to perform vulnerability assessments and penetration tests on local government networks. The Commonwealth also plans to use homeland security grants to hold regional working group meetings on cybersecurity.[ix]

For any cybersecurity program to work, sharing costs and retaining talented cybersecurity employees in local governments is crucial. State officials in Michigan launched a chief information security office (CISO) service to aid nine small- and medium-sized governments. The program allows local governments to pay a fraction of the price for a trusted cybersecurity expert to assist them with their cybersecurity needs. CISO and other tech officials are engaged through this cost-sharing system which allows them to receive the expertise they normally could not afford on their own. This partnership approach resulted in improved cybersecurity for the state and was cited by FEMA as being a valuable example for other jurisdictions.[x]

Dozens of state and local government agencies are members of 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.

Cyber Disruption Response Plans

> **Every government must be prepared to respond to cyber emergencies, in the same way that fire departments train and prepare to respond to fires. The National Governors Association (NGA) has created guidance on how to respond to emergency cybersecurity incidents. The NGA publication examines 'Cyber Disruption Response Plans' across America and offers best practices and tips to help. Bottom line, every government should test their processes and procedures with business leaders at least annually with a tabletop exercise that addresses cyber and other threats.**
>
> *-Dan Lohrmann, Chief Security Officer & Chief Strategist, Security Mentor, Inc., former leader of Michigan state government cybersecurity teams.*

Local Government Examples

Durham, North Carolina

(228,330 population)

Durham, North Carolina, was hit with two major cyberattacks in the last decade. The first attack, in 2009, targeted the public-school system and multiple systems managing student grades, phones and other networks were down for three months. Once the systems were back online, over 5,000 teachers had to manually reenter grades and other information. In addition to the costs of restoring or replacing hardware, the attack reduced functionality of the school system for months and it took thousands of hours to recover information.

Thus, the city of Durham worked diligently to create new policies, procedures and plans to make sure an attack like the 2009 incident never happened again. The school district and elected leaders established a cyber security framework complete with context, leadership, evaluation, compliance, audit, review and media plan. They also established partnerships with the FBI, the state of North Carolina and MS-ISAC.

When a second attack occurred in 2018, the city was better prepared. This time, the fleet vehicle network was inflicted with a virus that tried to jump to other agencies. DeWayne Kendall, deputy director of technology Solutions for the city of Durham, was worried.

"We were on our way to being in the newspaper," he said.

When the second attack took place, staff quickly reached out to partners at MS-ISAC, who then connected them with staff in Allentown, Pennsylvania, who just had a similar attack. This time, instead of taking months to diagnose and identify the attack, they were able to do it in hours. The attack was shut down completely and the city was able to eliminate reinfections of the system within two weeks.

Worcester, Massachusetts

(Population estimate: 185,877)

The city of Worcester, Massachusetts, recognized that in order for its cybersecurity awareness program to be effective and successful, it must have support at the highest level. The city has increased its security efforts over the past year by prioritizing them in the fiscal 2019 budget, and creating a full-time data security specialist position to implement policies and procedures that will help safeguard the city's data. The city also created a cybersecurity awareness trainer position, another full-time employee whose job was to deliver cybersecurity awareness training to employees on an ongoing basis. The city started its cybersecurity awareness program in October 2018.

Since cybersecurity is too broad of an area to tackle all at once, city officials identified training as the first priority. They aimed to train employees on cybersecurity awareness and equip them with the knowledge to help identify and prevent cybercrime. Additionally, the city continues to research cybersecurity best practices and available training for local government. To date, the city's cybersecurity awareness program includes: A one-hour, mandatory introduction to cybersecurity awareness class to employees;

1. A process to encourage users to report suspicious emails;
2. Acknowledgement of "cyber champions" in each department who can help their co-workers identify "fake" emails, distribute awareness flyers and posters and participate in monthly meetings to provide input for additional cybersecurity awareness training;
3. Development and enforcement of security policies and
4. Creation of a cybersecurity incident response plan.

Cities interested in bolstering their approach to cybersecurity preparedness often start by seeking grant opportunities to help fund cybersecurity risk assessments. The city of Worcester received such funding to review current policies, processes and procedures and identify potential security risks.

Matanuska-Susitna Borough, Alaska

(Population around 100,000)

The Matanuska-Susitna Borough (Mat-Su) is a local government in Alaska with a population of about 103,000. Borough officials felt that they had a fairly secure system. The borough monitored web, email, and network traffic; weathered DDOS attacks, viruses, malware, and ransomware; and had a good backup/disaster recovery system designed to withstand the next big Alaska Earthquake.

In mid-2018, several local and state government organizations in Alaska were hit by cyber attacks. Matanuska-Susitna was hit with an advanced malware suite on July 23, 2018, that took down 150 servers and nearly 600 desktop computers. Mat-Su and the nearby city of Valdez were completely incapacitated. Both governments were infected with ransomware, but each responded differently. Valdez decided to pay the ransom, whereas Mat-Su did not. Upon investigation, Mat-Su found that the attack had infected and encrypted their backups. Primary cleanup and mitigation took three months and cost $2.5 million. To reduce the risk of a new infection, both locations completely rebuilt their networks and scrubbed all data imported to the new networks.

As for ransomware, the Mat-Su subscribes to the conventional wisdom of never paying a ransom, as doing so simply encourages the attacker to use new and bolder methods, and paying never guarantees a return of assets.

There are many models for cybersecurity, and the most common, *prevention*, is no longer enough. Since the attack, the municipality's multi-level email filters capture more than 650,000 bad emails an hour, and yet there are still dozens of targeted email attacks that get through daily. For prevention to work, a city's defense has to be correct 99 percent of the time, as no system will ever be perfect. Mat-Su now uses the *detect and contain* approach for that reason.

National League of Cities

The National League of Cities suffered a ransomware attack in February 2017. The total downtime experienced was less than 15 hours thanks to the inclusion of cybersecurity in NLC's disaster recovery plan. By having, following and sticking to the plan, NLC was able to recover the stolen files without having to pay the ransom.

One evening, a network user noticed that several files were locked on the network drive and suspected that this was a potential ransomware attack. They immediately called NLC's IT director who confirmed that the files were in a state of encryption caused by a ransomware attacker. The managed services provider (MSP) who maintains NLC's network was contacted and quickly discovered the attack was coming from an account logged on through a terminal network that allows for remote working — essentially, the attacker was posing as an NLC employee. They immediately disconnected the user and reset the password to stop the hacker from getting back into the network.

By that time, over 11,000 files had been locked by the attack. However, there was no need to pay the ransom because NLC backs up its data every night. The first thing NLC's disaster plan calls for is a recovery via a shadow copy from the off-site location to the on-site location, but this failed because of inadequate free space. A second action called for making the off-site file server the primary file server for the time being while the MSP took time to wipe clean and re-build the on-file server from scratch. Additionally, it was decided that terminal services be terminated during the recovery period and was later rebuilt.

There is nothing like an attack to test the disaster recovery plan for any government or organization, and NLC learned several important lessons about its strengths and vulnerabilities. First, the rapid response plan and nightly file backups allowed the organization to quickly respond to the initial attack. Second, hosting those backup copies off-site allowed the organization to quickly restore critical services after the attack, even while the primary file server was being rebuilt. Third, there were additional steps that the NLC could take to prevent similar attacks in the future. This included lengthening employee passwords to a minimum of 14 characters as suggested by the NIST security standard, adding an application to strengthen the terminal services by limiting the number of invalid login attempts, and implementing multi-factor authentication (MFA) on the terminal service and VPN. Finally, NLC made cybersecurity training mandatory for all staff with a focus on phishing and scams.

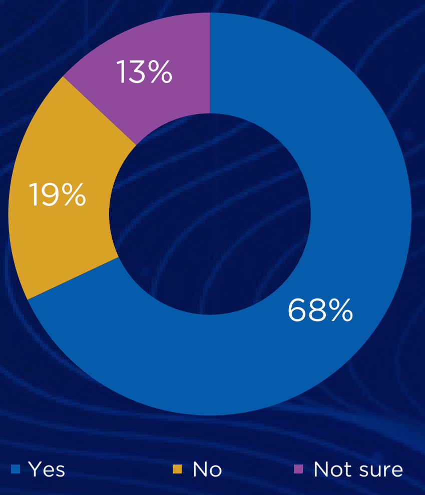
What Cities Need to Know About Cyber Insurance

As cyberattacks against local governments have become more widespread, cyber insurance has emerged as an attractive backup for some cities to expand the full set of cybersecurity protections. Insurance should not be considered an alternative to updating systems and improving digital hygiene, but no system can be 100% safe in such a dynamic and changing environment.

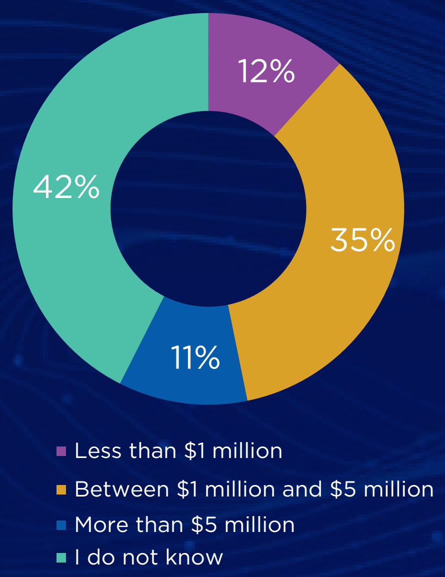
Cyber insurance premiums can cost thousands of dollars, but they can save a municipality much more, in the event that there is a cyberattack. Here are just a few things cities should include when thinking about the scope of potential coverage:

- Overtime for employees attempting to restore a system
- The cost of lost revenue (some non-recoverable)
- The cost of outside technical support servicesThe monthly and annual costs to provide "free" credit monitoring reports to affected citizens or businesses whose information was stolen
- The replacement of some equipmentLegal fees
- Forensics after an attack occursCrisis management and post-event related expenses

DOES YOUR LOCAL GOVERNMENT CURRENTLY HAVE CYBER INSURANCE?



IF YES, WHAT IS THE COVERAGE AMOUNT?



WHAT DO CYBER INSURANCE COMPANIES LOOK FOR?
Some cyber insurance forms ask dozens of key questions. Failure to answer honestly could lead to a denial of payment. Imagine a chain smoker who smokes ten packs a day and falsely claims to be a non-smoker on a medical insurance form. Were the patient to succumb to a smoking-related illness, the insurance company is not obligated to pay anything. In the cyber realm, those providing cyber insurance want to minimize their risk as well, and premiums and deductibles are predicated on how good your jurisdiction manages its digital infrastructure. Common questions are:

- Has the jurisdiction adopted a cybersecurity incident response plan and adopted basic technology practices and policies?
- Are internet and email use policies reviewed with employees, elected leaders and contractors?
- Are employee access rights reviewed?
- How often is employee training provided and what is addressed?
- How are backups of devices managed?
- What anti-spam, anti-virus filters, anti-malware are utilized?
- Is computer access terminated when an employee departs?
- Is there an on-going process of forcing employees to change passwords?
- Are service providers required to demonstrate adequate security policies and procedures?
- What are the security and privacy provisions for cloud and managed services?
- What procedures are in place to test or audit your policies, procedures and controls?

PTI's and NLC's national survey of local government information technology officials revealed that 70 percent of respondents have cyber insurance. However, when asked what the amount of their insurance coverage was, 50 percent of respondents "did not know." Whether known or not, the amount of coverage and exposure should be reviewed on a regular basis to make sure your organization is properly covered. While cyber insurance does not protect your municipality from a cyber-attack or breach, it does help to mitigate the risk that your municipality could be crippled indefinitely by an attack or faced with the prospect of having to front thousands of even millions of dollars in the wake of a cyber event. With this in mind, cyber insurance should be considered a key component of your government's cybersecurity strategy.

Finally, be sure to reach out to your state municipal league to determine whether they offer cyber insurance through their affiliated risk pools.

Strategies and Recommendations for Local Leaders

1. **Identify one individual to be responsible for cybersecurity programs in that jurisdiction**
   This individual should be the “go-to” person when a security problem arises, and also serve as an “ambassador” who promotes cybersecurity awareness within the organization. With this role, they can also serve to enforce your cybersecurity rules and ensure staff receive the necessary training. They should report directly to the local government’s top executive/administrator. Larger municipalities should hire a full time IT executive. For smaller jurisdictions with tight resources, hiring a full-time IT person to help with more complex issues may not be possible. This is when local governments should consider soliciting state/county resources or partnering with a neighboring jurisdiction to address this need.

2. **Make digital hygiene an institutional priority**
   For local elected officials, keeping residents safe and secure is no longer just about having an able police force and sound justice system. Today, security encompasses the digital world and ensuring bad global actors cannot take advantage of weaknesses in online systems. Local leaders should work to promote a shift toward cybersecurity as a governing priority, both internally and in their connected communities. This should include emphasizing the importance of cybersecurity in the city budget, instituting best practices around cybersecurity and digital hygiene, recruiting new staff with cybersecurity and technical skills, training existing staff annually, training new staff as part of onboarding, and conducting an audit to identify points of weakness within local government networks.

3. **Educate the local workforce, elected leaders, and residents about cybersecurity**
   While investing in sophisticated software is important, towns and villages should take, investing heavily in people is also critical. NLC and PTI recommend that cybersecurity awareness training happen at least once a year, if not more. All new staff, including newly elected officials, should receive cybersecurity training as part of their onboarding processes. Lastly, periodic awareness campaigns should occur throughout the year. Be sure to also think what role city hall can play in reaching out to small and medium size business and schools. These places are also under constant attack. At the annual National Night Out in 2018, the city of Bellevue, Washington, created a venue for IT staff and community relations coordinators to meet with neighborhood groups, residents of low-income housing units and other local groups to inform parents and their children about online safety. The team plans to return next year and even started a monthly newsletter.

4. **Conduct an analysis of local government vulnerabilities**
   Before making any significant investments in cybersecurity systems or reinforcements, it is valuable to assess the gaps and weaknesses in your local government’s network. For

> **“**
>
> **This is a rapidly changing landscape and there is an ongoing up-tick in attack vectors which make this a topic that cannot be ignored. Staff must know how to protect the enterprise systems and perimeter while balancing security and functionality. This requires an advanced, ever-evolving skillset and the ability to communicate and train end users rapidly. This is not just an IT problem, but an organizational one.**
>
> *-Chris J. Neves, IT Director, City of Louisville, Colorado Information Technology*

local governments, this might include identifying any vulnerabilities present in connected infrastructure throughout the city. Simple tabletop exercises for officials to practice their incident response plan can help identify these vulnerabilities, and many state governments can help coordinate these drills. As noted above, MS-ISAC is supported by the federal government to help local governments analysis and recommendations.

5. **Ensure your data is properly backed up**
   The number one defense against ransomware is tested, offline (non-connected or cloud hosted) backups. This is an extension of good digital hygiene that is worth emphasizing for its own sake. Even organizations that have policy in place need to ensure that backups are being conducted frequently, that these backups are sufficiently isolated to avoid attack, and that they are technically capable of restoring service and functionality.

6. **Implement multi-factor authentication**
   Multi-factor authentication (MFA) is a valuable tool against attacks. MFA requires a user to enter an additional security code or confirmation via their smartphone, e.g., through an app or text message. Cities should implement MFA on all business-critical systems, e.g., email. If an attacker gained the credentials of a city employee through a phishing attack, the attacker would still be blocked from gaining access because they don't have their employee's smartphone.

7. **Create policies or plans to manage potential attacks**
   Every local government should have a cybersecurity response plan. This can be developed internally or with the help of a private sector firm that specializes in security. The plan should include several key components:

- Employee awareness training, incident response and after-action planning.
- An incident response team, similar to ones created to address natural or man-made disasters.
- Protocols to notify local law enforcement as well as other appropriate officials (state officials, the US Department of Homeland Security, FBI). Almost all states require that local governments contact the state CIO, the state attorney general, and other departments.
- Prioritization of systems to restore in case of an attack. For most governments this would mean making sure safety and health services come back online first or a shifting of resources if services cannot be brought back on immediately

8. **Ensure public communication is part of your attack response plan**
   Public trust is essential to local government, and when it comes to potential attacks, public communication is a unique concern.

   Utilize all of your jurisdiction's communications channels to share information with the public – the press, social media, television. In the event of a data breach, some state laws require the local government to notify the press if a certain number of personally identifiable pieces of information are exposed.

   What should you tell the public? Your community needs to know that their local leaders are fully engaged in the situation and are working to resolve it. To maintain the public trust, it is important to be as transparent as possible, keeping in mind that your jurisdiction is involved in a situation that impacts the public safety and full details may not be available until after the situation is resolved.

9. **Consider converting to a dot gov (.gov) domain**
   Hackers are not only attempting to target cities, they may impersonate a municipal service in order to target your residents. Identity thieves can easily create websites in the dot com (.com) or dot org (.org) domains that can look and seem like a legitimate web page and direct targets there to pay bills or submit personal information. These scams can be reduced by establishing your municipal systems on a .gov domain, which is much more difficult to mimic.

10. **Work with education partners to create a cybersecurity talent pool**
    Individuals with cybersecurity skills are highly sought after in today's job market, and the public sector often struggles to compete with the higher salaries in the private sector. Local leaders should tap into local community colleges, universities and high schools to help fill cybersecurity gaps. This way students can get hands-on experience and serve their communities, which may encourage to stay in in those positions. Two examples of this already exist. For twenty years, Cisco Networking Academy has worked to help students gain technical and entrepreneurial skills. Students can take courses online in subjects such as the IoT and cybersecurity. Along the way, Cisco will help students seek out job and networking opportunities. CompTIA is also working to create certifications around cybersecurity and keep those in the IT world on a growing path throughout their careers.

Conclusion

Today, digitization of services and management of sensitive data requires cities to invest in cybersecurity to fend off risks to their network. Local governments are in the midst of a sea of change, as more and more of their basic governance functions rely on technology. Connected infrastructure is critical to service delivery and efficiency.

Many improvements to local cybersecurity will involve partnerships between cities and private consultants or vendors who can provide important services. It is essential that local leaders understand that they can outsource many of these functions, but they cannot outsource responsibility. They have a duty to embrace cybersecurity both in practice and policy as tech is integrated into our cities, towns and villages. Local governments can prepare by doing the cyber basics and then begin stepping it up from there. Local elected officials owe it to their residents to protect their most valuable data — it is their responsibility, their duty of care. The National League of Cities and the Public Technology Institute stand ready to help the nation's local governments strengthen their cybersecurity efforts.

> “
>
> **Local elected officials owe it to their residents to protect their most valuable data — it is their responsibility, their duty of care.**

References

NLC/PTI Survey: NLC and PTI conducted a survey of IT officials representing local governments from across the United States to prepare for this survey. PTI set the survey out to their members while NLC sent the survey out to it's ITC Committee. With 165 responses 45 percent represent communities with a population under 50,000, 33 percent represent local governments in the 50,000 to 150,000 population range while 22 percent represent local governments above 150,000 in population.

Label Resources

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

Americans and Cybersecurity (Pew Research Center) https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

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 And The Rise Of Smart City Vulnerability (Smart Resilient Cities) https://www.smartresilient.com/cybersecurity-and-rise-smart-city-vulnerability

Cybersecurity: Protecting Local Government Digital Resources (Microsoft and ICMA) https://icma.org/sites/default/files/18-038%2520Cybersecurity-Report-hyperlinks-small-101617.pdf

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 https://web.archive.org/web/20180218234603/http://www.ey.com:80/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf

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

MS-ISAC https://www.cisecurity.org/ms-isac/

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

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

National Institute of Standards' Cyber Security Framework https://www.nist.gov/cyberframework

End Notes

[i] Unlocking the Potential of the Internet of Things, by James Manyika and al. 2015. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[ii] Barker, "The Economic Costs of Being Hacked," BetaNews, BetaNews, Inc., February 10, 2016. http://betanews.com/2016/02/10/the-economic-cost-of-being-hacked/

[iii] Deere Stephen. Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million. *The Atlanta Journal-Constitution*. August 2018.

[iv] Duncan, Ian. Baltimore estimated cost of ransomware attack at $18.2 million as government begins to restore email accounts. *Baltimore Sun*. May 29, 2019.

[v] Cybersecurity: Protecting Local Government Digital Resources by Corey Fleming and all. ICMA and Microsoft, May 2017.

[vi] Ibd.

[vii] Cohen, Natasha. Cyber Incident Response and Resiliency in Cities: How Partnerships Can be a Force Multiplier. *New America*. February 2019.

[viii] Ibd.

[ix] Ibd.

[x] Lesson Learned: Cybersecurity: The Michigan Cyber Disruption Response Strategy

Appendix A: Cybersecurity Checklist

The following is a comprehensive checklist to determine the level of security controls within your city.
This checklist was adapted from a resource developed by James E. Pacanowski II, CGCIO, Ventnor City, NJ.

Physical Security		
Item	**Yes**	**No**
Do you have policies and procedures to address authorized and limited access to facilities, including data centers?		
Are visitors escorted in and out of controlled areas?		
Are PC screens automatically locked after an idle period?		
Do you have policies covering laptop, tablet, or mobile device security?		
Do you have a current emergency evacuation plan?		
Do you have an accurate up to date inventory of all electronic equipment?		
Are your data closets and/or server rooms equipped with intrusion alarms?		
Is your data center/server room locked at all times?		
Do you have environmental controls dedicated to your data closets and server rooms?		
Do you have fire suppression systems dedicated to your data closets and server rooms?		
Are default security settings changed on software and hardware before they are placed in operation?		
Are policies and procedures in place to control equipment plugged into the network?		
Is your physical facility monitored and reviewed via camera systems?		
Totals		

Personnel		
Item	Yes	No
Does your staff wear ID badges?		
Do you check credentials of external contractors?		
Do you have policies to address background checks of contractors?		
Do you have policies addressing background checks of employees?		
Do you have a policy for unauthorized use of “open” computers?		
Do you have a policy and procedure in place to handle the removal of employees who retire, are terminated, or leave, including passwords and access to systems?		
Do you have an acceptable use policy that governs email and internet access?		
Do you have a policy governing social media use and access by employees?		
Are employees required to sign an agreement verifying they have read and understood all policies and procedures?		
Are these policies and procedures reviewed by employees at least annually?		
Totals		

Account and Password Management		
Item	Yes	No
Do you have policies and procedures covering authentication, authorization, and access control of personnel and resources to systems?		
Are policies in place to ensure only authorized users have access to PCs?		
Are policies and procedures in place to enforce secure, appropriate, and complex passwords?		
Are information systems such as servers, routers, and switches protected with basic or better authentication mechanism?		
Has the default “Administrator” account been disabled and/or deactivated?		
Are all access attempts logged and reviewed?		
Are employees required to change their passwords on a routine schedule?		
Are employees prevented from using previous passwords?		
Are all passwords on network devices encrypted?		
Do you have legal and/or policy notifications on all log-in screens that is seen and accepted prior to access to any network device?		
Totals		

Data Security		
Item	Yes	No
Do you have policy for information retention?		
Do you have policies and procedures for management of personal private information?		
Do you have a policy for disposing of old and outdated equipment?		
Do you have policies and procedures in place for the secure destruction or sanitation of media and/or drives before they are removed, sold, or disposed of?		
Is access to data or systems accessed remotely both from a dedicated link and encrypted?		
Do you have policies and procedures in place to ensure that documents are converted into formats that cannot be easily modified before they are circulated outside the network?		
Are documents digitally signed when they are converted to formats that cannot be easily modified?		
Is access to critical applications restricted to only those who need access?		
Are UPS batteries used on all critical equipment?		
Totals		

Network Security		
Item	**Yes**	**No**
Is network traffic regularly monitored for patterns?		
Do critical systems have redundant communication connections?		
Does your network utilize redundant DNS servers in case of interruption to one server?		
Are your DNS servers reviewed on a periodic basis for anomalies and consistency?		
Is your Active Directory reviewed periodically for anomalies and consistency?		
Are all unnecessary services disabled on servers?		
Does your network utilize redundant domain controllers in case of interruption to one server?		
Are there policies and procedures governing the use of wireless connections to your network?		
Are wired and wireless networks within your organization segregated either physically or virtually through routers, switches, or firewalls?		
Do you employ firewalls on your network to control access and traffic?		
Are firewalls configured to only allow traffic from approved lists?		
Are network security logs reviewed regularly?		
Are web filters used to restrict downloading of unapproved material?		
Are filters or firewalls used to filter executable or malicious email attachments?		
Are policies and procedures in place for software patches and updates?		
Are policies and procedures in place for hardware patches and updates?		
Are your security policies reviewed on a yearly basis?		
Are current and up to date antivirus solutions loaded on all computers?		
Are antivirus and other security software updated with current patches on a regular basis?		
Do you use spyware and malware detection software?		
Are all computers current with all security and operating system patches and updates?		
Do you use employee “least privilege” access and review access privilege periodically?		
Do you have an accurate and up to date software inventory list?		
Totals		

NLC NATIONAL LEAGUE OF CITIES

CITIES STRONG TOGETHER

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.

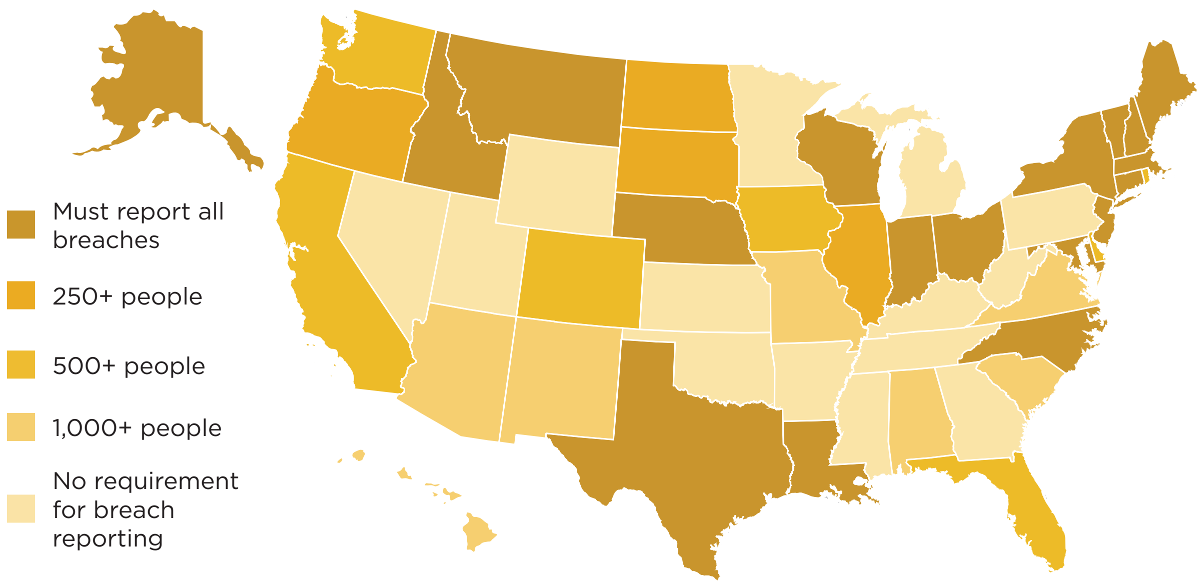
The report also includes profiles of effective city-state partnerships from across the country. As cities, towns and villages continue to be on the frontlines of cyberattacks, a collaborative approach between cities and states, together with Federal and university partners, can lead to a stronger national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

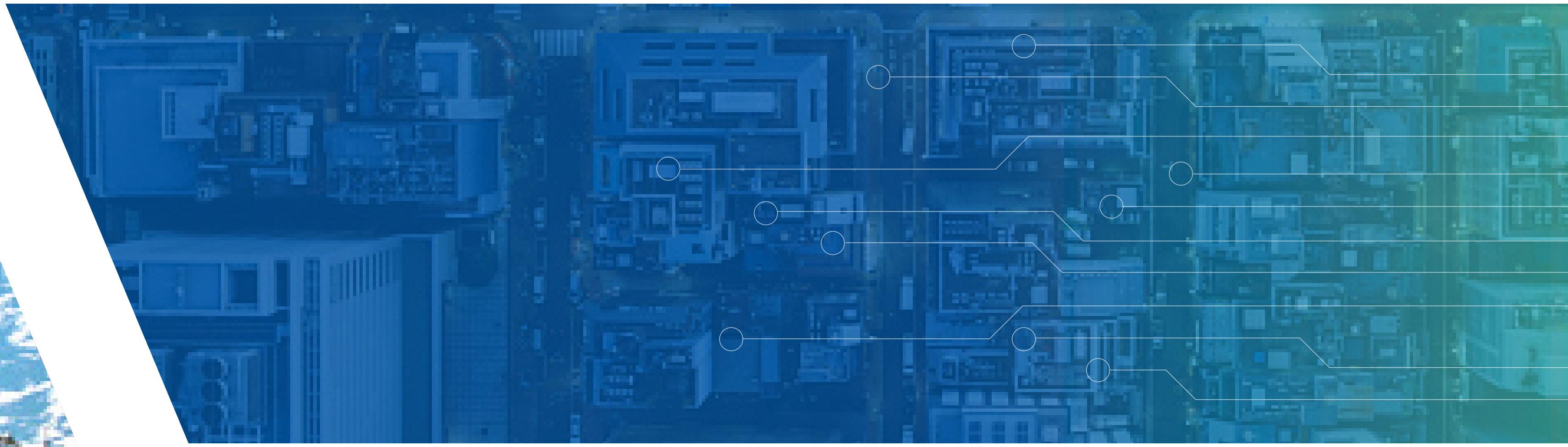
CASE STUDY:
Mandatory Breach Requirements in Alabama

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]

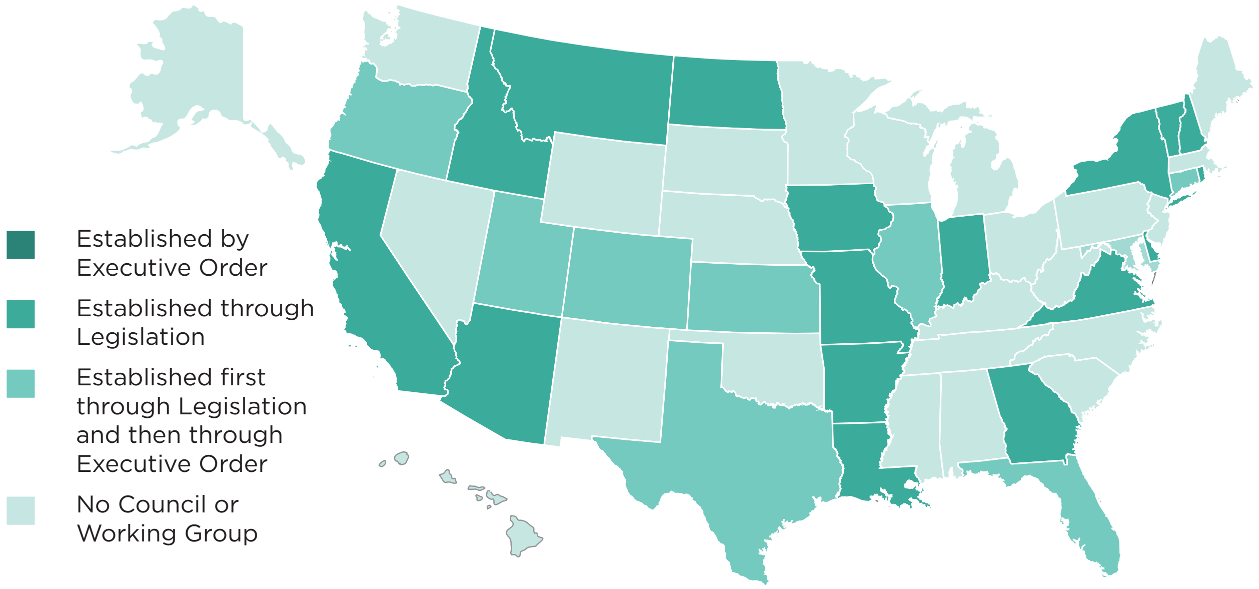
In recent years, Michigan has become one of the few state leaders in prioritizing and implementing effective state government cybersecurity measures through leadership, innovation and strong collaboration. It's essential for states to recognize the urgency of complex cybersecurity issues and develop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

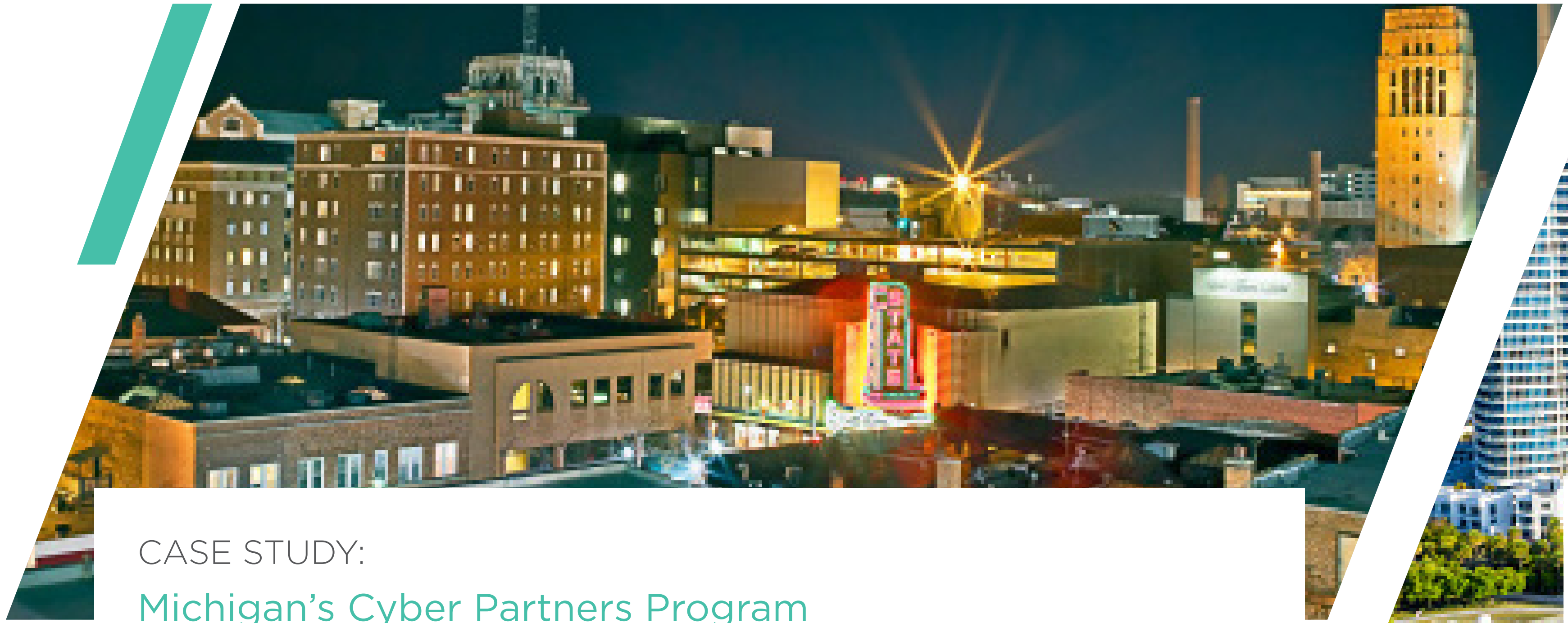
The effort started with a simple goal: to improve cyber hygiene for all communities in the region, regardless of size. Representatives from cities and counties, IT specialists and other cybersecurity experts worked together to develop the regional framework. They established benchmarks and best practices 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

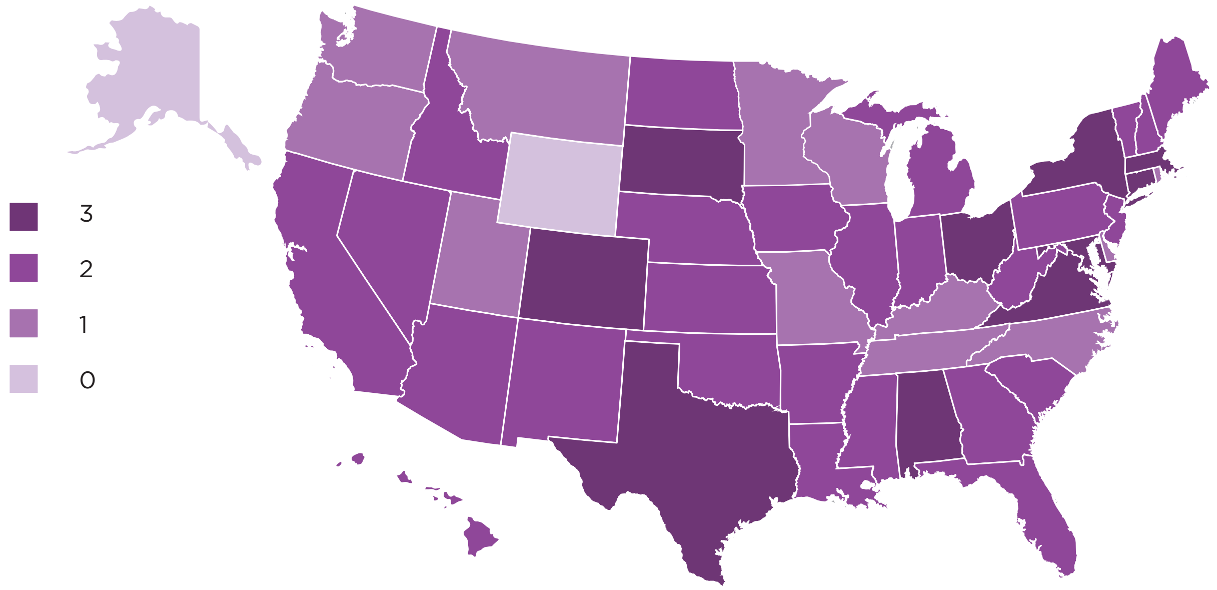
State governments have long partnered with their public or private two- and four-year universities to address critical issues in their states, from aligning talent with business needs and providing extension services, to, more recently, bolstering cybersecurity at the state and local levels. These partnerships 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.

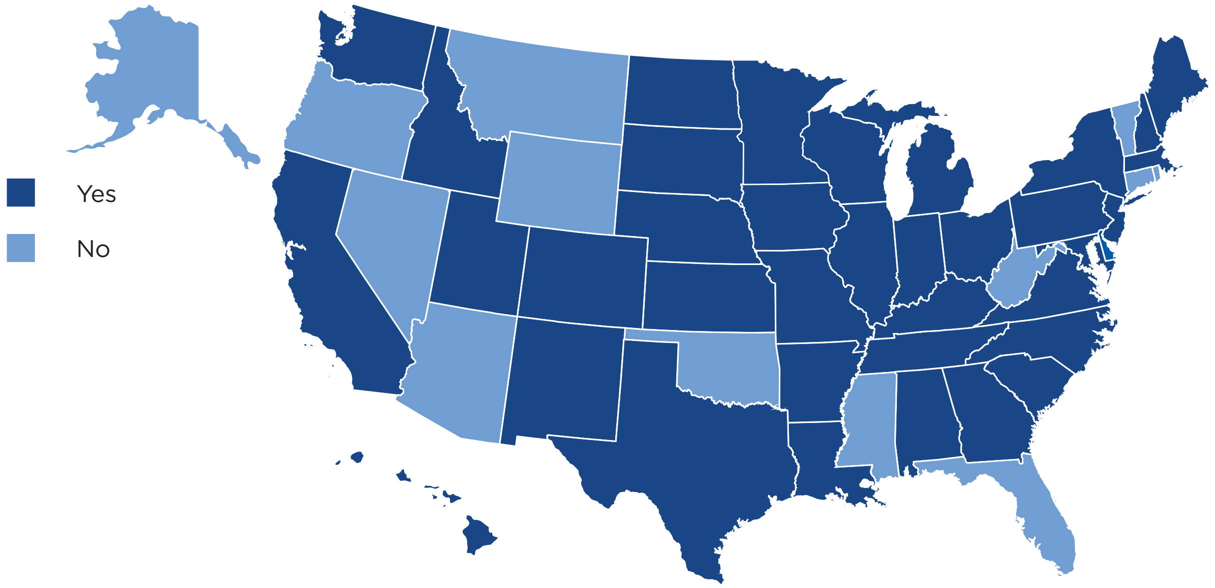
National Guard Partners

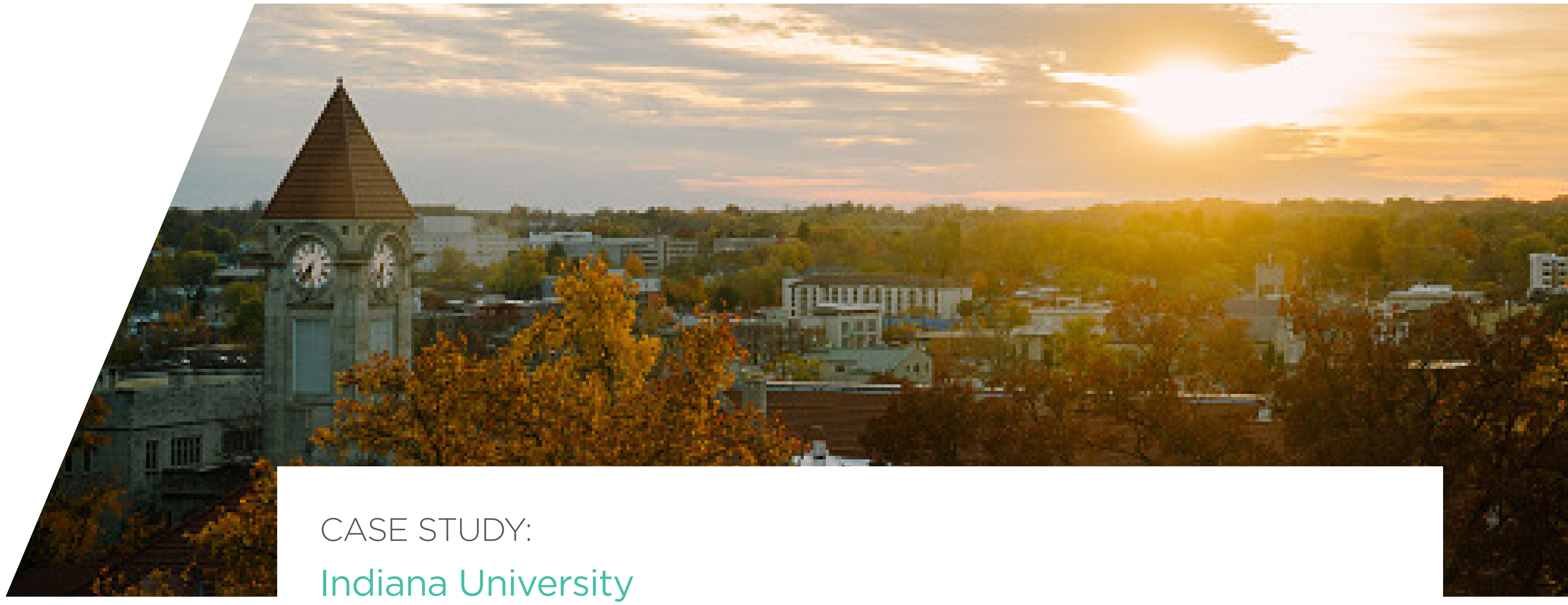
In addition to university partners, states have turned to their National Guards as a resource to defend against cyber-related attacks, safeguard information assets and protect the "digital and physical infrastructures" of localities.[30]

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

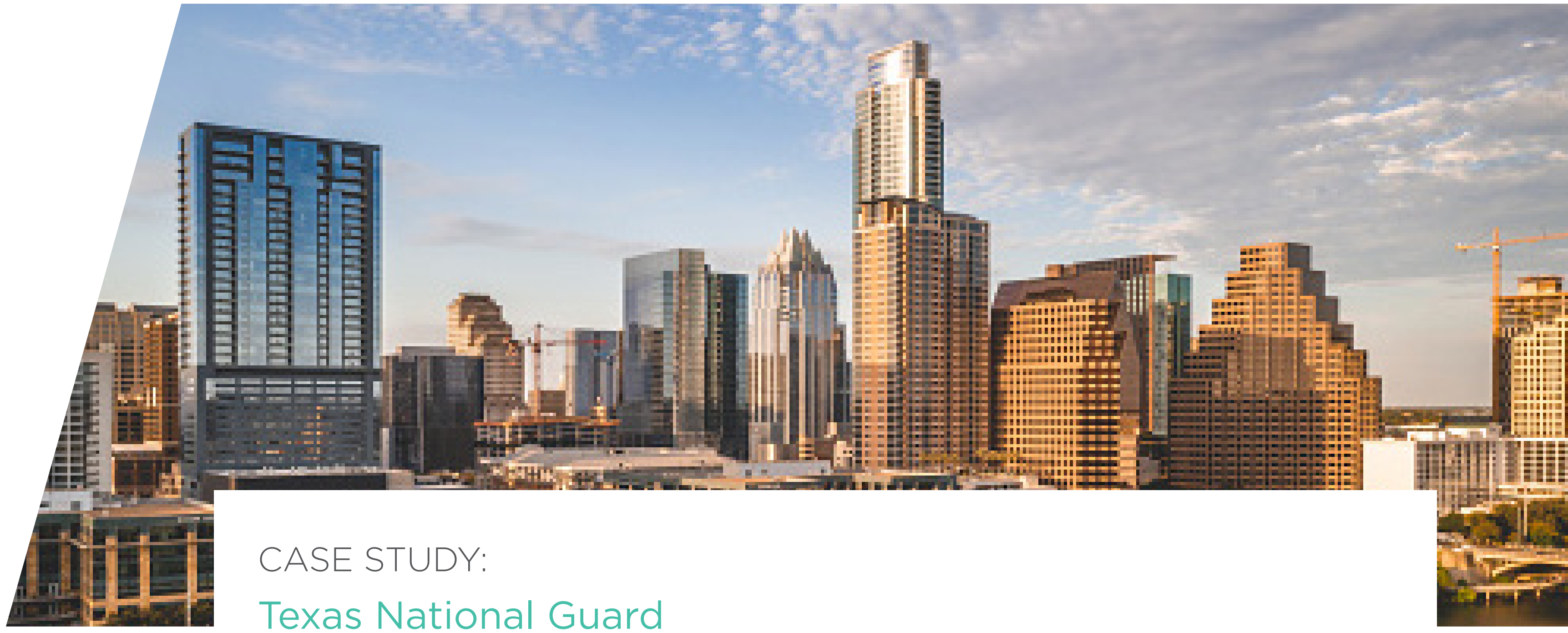
For 20 years, Indiana University (IU) has been at the forefront of universities that help manage cyber risk. has established an IU Cybersecurity Clinic to serve as a hub for Midwest cyber training needs. It will address threats faced by businesses, individuals, and state and local governments. Funding 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