



Protecting Our Data:

WHAT CITIES SHOULD KNOW
ABOUT CYBERSECURITY

NLC NATIONAL
LEAGUE
OF CITIES

CENTER FOR CITY SOLUTIONS



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.

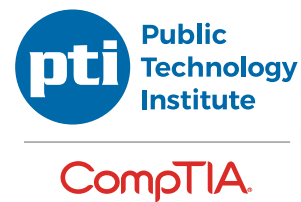
About the Authors

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.



About the Public Technology Institute

Created by and for cities and counties, the non-profit Public Technology Institute promotes innovation and collaboration for thought-leaders in government, and advances the use of technology to improve the management and delivery of services to the citizen. In 2019 PTI merged with CompTIA in order to provide an increased array of educational and information-sharing opportunities for local governments.

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

3	Foreword
5	Introduction
7	What is Cybersecurity?
8	How Prepared are Cities?
15	Policy Landscape and Resources for Local Governments
18	Local Government Examples
21	Strategies and Recommendations for Local Leaders
25	Conclusion
27	References

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.

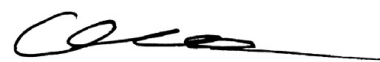
Every day in the United States, a local government is hacked. Since 2013, ransomware attacks have impacted at least 170 county, city, or state government systems. The damage can cost millions, but the loss of public trust and safety come at an even higher price.

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

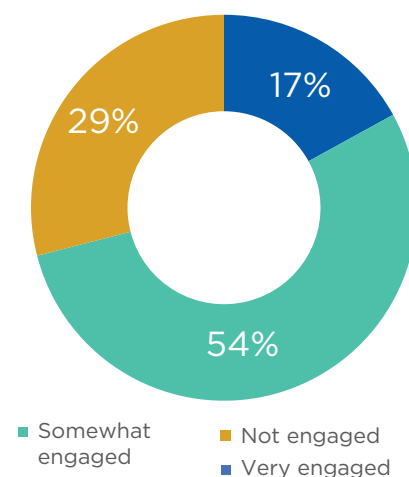
How Prepared are Cities?

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?

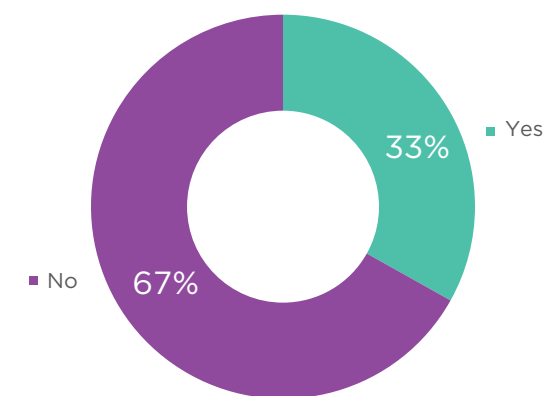
Only 17 percent of respondents say their local elected officials are very engaged in cybersecurity efforts. In fact, 29 percent admitted that they were “not engaged” at all.



IS YOUR BUDGET ADEQUATE ENOUGH TO SECURE THE NETWORK PROPERLY?

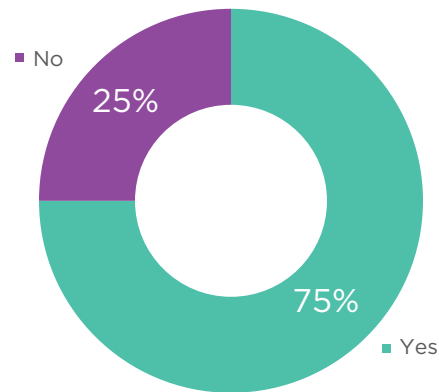
When asked if the local government’s budget was adequate, 67 percent of respondents said it was high enough to secure the network properly.

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

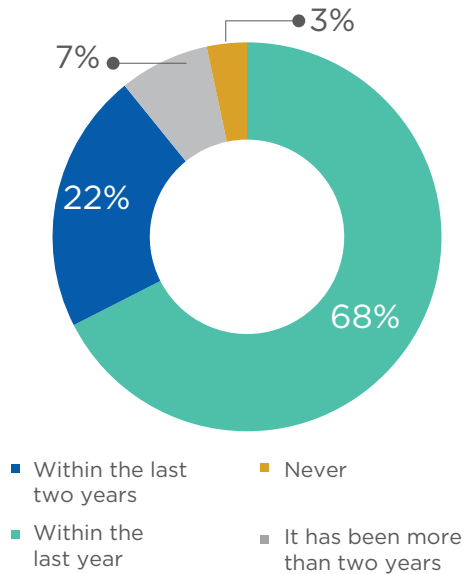


DOES YOUR LOCAL GOVERNMENT HAVE A CYBERSECURITY PLAN/STRATEGY?

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.

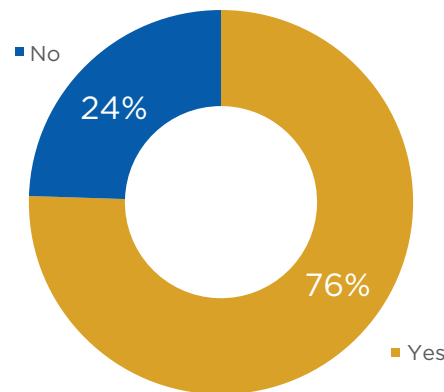


IF YOU HAVE A CYBERSECURITY PLAN, HOW OFTEN IS IT REVIEWED?

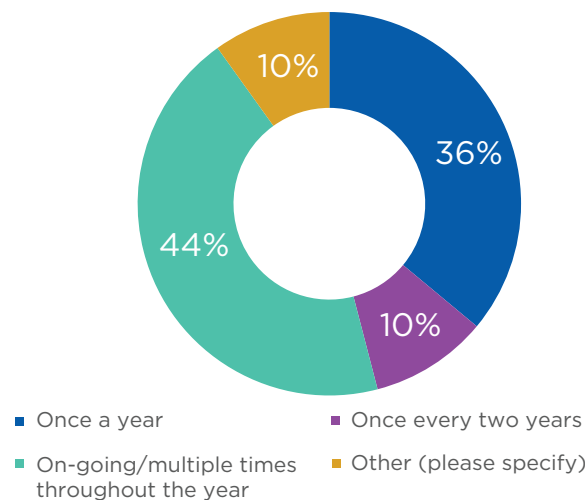


However, only 68 percent of these plans have been reviewed in the last year. This is troubling, since annual audits are considered a best practice with ever-changing technology and threats.

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.

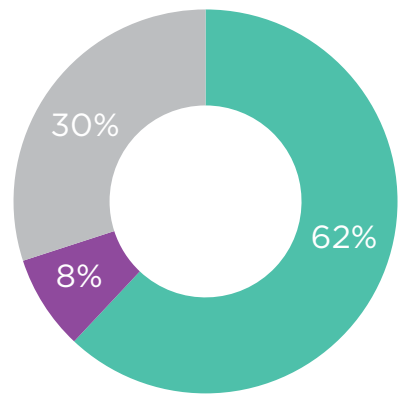
The most alarming result from the survey dispels the myth that cities, towns and villages are safe from attacks by bad actors. The survey found that 44 percent of local governments report an attack from a cyber incident hourly (26 percent) or daily (18 percent). That number rises to 66.7 percent over 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/University 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.

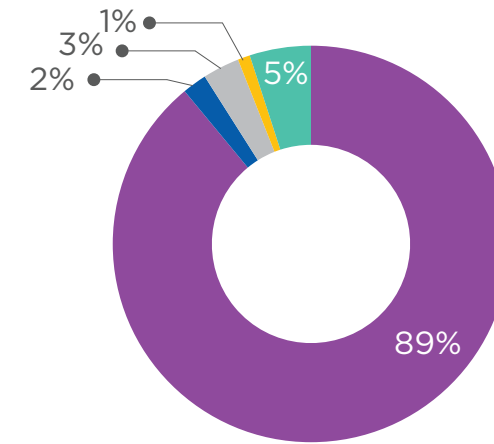
DOES YOUR LOCAL GOVERNMENT OUTSOURCE ANY OF ITS CYBERSECURITY FUNCTIONS?



- Do not outsource
- Fully outsource
- Partially outsource

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

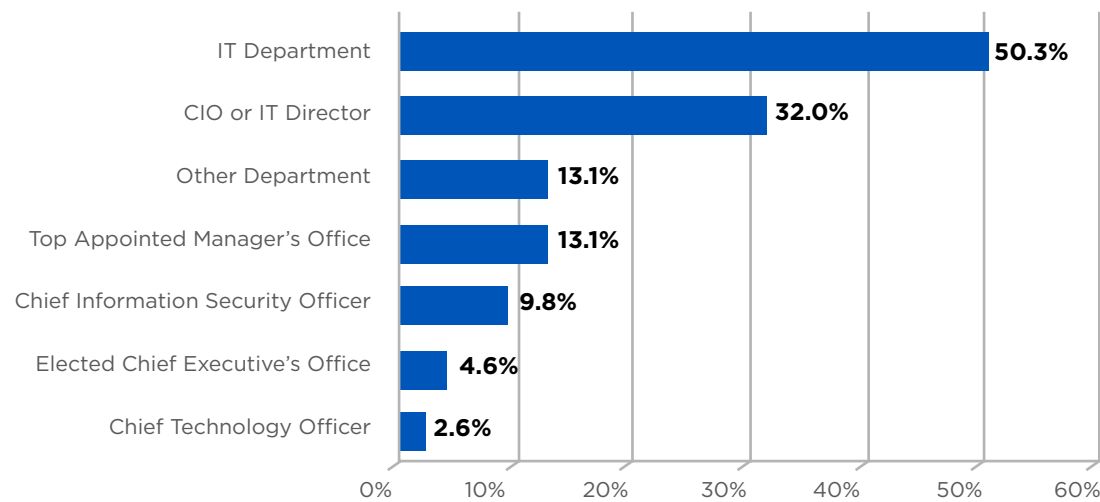
WHERE IS THE PRIMARY RESPONSIBILITY FOR CYBERSECURITY LOCATED IN YOUR LOCAL GOVERNMENT'S ORGANIZATION?



- Within IT department or related unit
- Within the elected chief executive's office
- Within the top appointed manager's office
- Stand-alone cybersecurity department or unit
- Other department, unit, or office

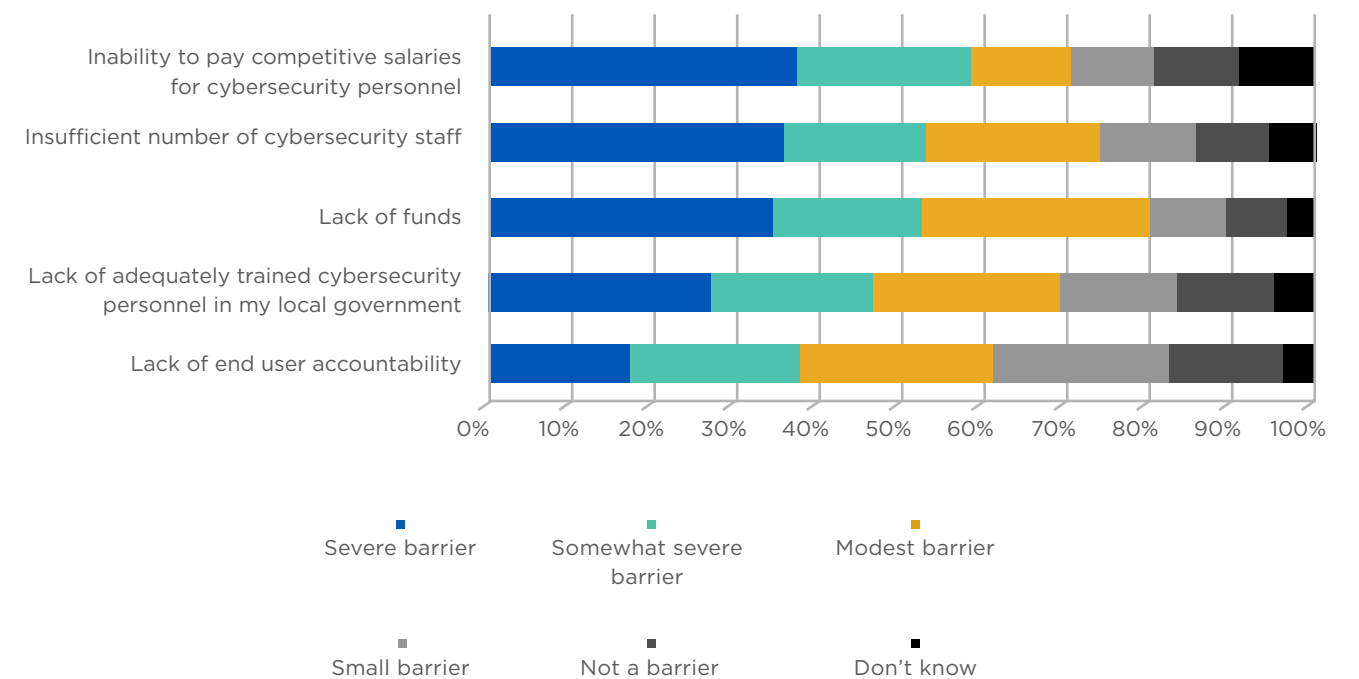
Graph courtesy of ICMA/University of Maryland, Baltimore County.

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.

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.

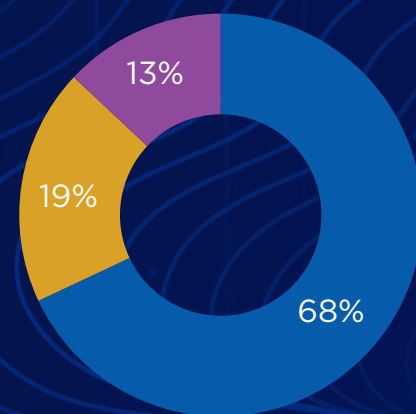
What Cities Need to Know About Cyber Insurance

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:

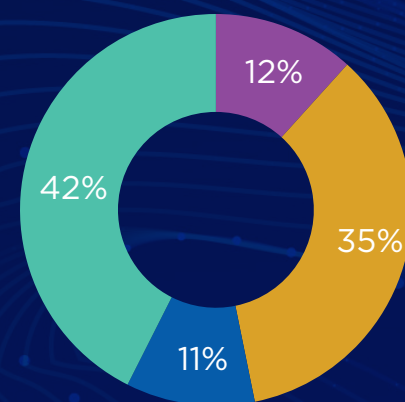
- Overtime for employees attempting to restore a system
- The cost of lost revenue (some non-recoverable)
- The cost of outside technical support services
The monthly and annual costs to provide “free” credit monitoring reports to affected citizens or businesses whose information was stolen
- The replacement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

DOES YOUR LOCAL GOVERNMENT CURRENTLY HAVE CYBER INSURANCE?



■ Yes ■ No ■ Not sure

IF YES, WHAT IS THE COVERAGE AMOUNT?



■ Less than \$1 million
■ Between \$1 million and \$5 million
■ More than \$5 million
■ I do not know

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 its 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](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

CENTER FOR CITY SOLUTIONS