Cybersecurity for Local Government: A Primer

Donald F. Norris and Laura K. Mateczun

Introduction

We have written this primer about cybersecurity specifically for elected officials and top managers in American local governments. Although much of what is presented here could apply to organizations of almost all types and sizes across almost all sectors, we write for officials and top managers of local governments because there is very little cybersecurity guidance available specifically designed with them in mind. Additionally, much of the current cybersecurity guidance that is available often is written in technical language and directed at personnel trained in information technology and cybersecurity, not elected officials and top managers.

We also write for this audience because over the past several years we, along with other colleagues at our university, have conducted considerable research specifically into local government cybersecurity. We have presented findings and recommendations from this research in papers published in the professional publications as well as articles written for scholarly journals. In 2022, we published the first and only book devoted to local government cybersecurity (*Cybersecurity and Local* Government, Norris, Mateczun and Forno, 2022). While this primer is largely the product of that research, we have written it to be accessible and understandable to local government elected officials and managers throughout the more than 38,000 units of local government in this nation.

This primer covers five broad topics: what local government elected officials and top managers should know about cybersecurity; what they should do about it; questions they should ask their IT and cybersecurity staff personnel; the future of cybersecurity; and cybersecurity recommendations directed at small local governments.

A. Things to Know

In this section, we discuss several things that local officials need to know about cybersecurity. We do not (and could not in a primer) cover everything local officials need to know. But we highlight six items of considerable importance.

1. Local governments are under constant - or nearly - constant cyberattack.

Research over the past few years shows that local governments (and probably most organizations with an online presence) are under constant or nearly constant cyberattack. This is simply a fact of life and local governments cannot afford to ignore it because ignoring it substantially increases the cybersecurity risk to them.

2. Some attacks will succeed.

Even local governments with highly effective cybersecurity capabilities are likely to experience successful cyberattacks (e.g., breaches). See definition below. Those with poor cybersecurity management, planning and defense will experience more frequent and more damaging breaches. There is a saying in the cybersecurity world: "It is not whether you will be breached but when." We would add "and how many times?" Successful attacks can be devastating and very costly. Just ask Atlanta, 2018, at least $17 million to recover, and Baltimore, 2019, at least $18 million. (Chapter 1 of our book examines the breaches of these two cities' IT systems in more detail.)

> *Verizon (2023) defines a breach as: "An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party;" and an incident as: "A security event that compromises the integrity, confidentiality or availability of an information asset."*

3. Local governments may, and often do have several cybersecurity vulnerabilities.

The most common and problematic cybersecurity vulnerabilities are found everywhere inside an organization: hardware, networks, software (including operating systems), remote work, BYOD (allowing officials and staff to attach their own devices to the local government's IT system without effective controls), user authentication, and people (the weakest link). If not known or ignored, these and likely other vulnerabilities (e.g., poor access controls, third party contractors, lack of comprehensive or poorly enforced policies, etc.) can and almost certainly will result in unnecessary risk to a local government's IT system and assets. Ultimately, these vulnerabilities also increase the likelihood of breaches and other adverse cybersecurity events.

4. Most local governments report lack of adequate funding for cybersecurity.

Studies have repeatedly found that the lack of adequate funding is among the top reasons, if not the top reason given by local government IT and cybersecurity officials for their governments' inability to establish and maintain highly effective cybersecurity. This leads to the next item in our list of things local government officials must know about cybersecurity.

5. Many of not most local governments do not staff cybersecurity adequately.

As with many organizations, local governments often do not have sufficient numbers of IT and cybersecurity staff. Staffing IT and cybersecurity adequately is essential, but it is not cheap and competition for trained cybersecurity staff is high, especially competition from the private sector where pay is (often a lot) better than local governments can afford. Additionally, the national cybersecurity workforce shortage of more than 1.2 million in 2022 continues to grow annually [$(ISC)^2$, 2022, p. 6].

6. Most local governments report a lack of support for cybersecurity, often across the organization.

Ongoing support from top elected and appointed officials for proper funding and staffing of cybersecurity is essential to obtaining and implementing effective levels of cybersecurity. It helps to have a champion (better yet, champions) among elected officials and top managers to foster the development of an ongoing cybersecurity program and create a culture of cybersecurity throughout the organization. Without such support, the likelihood of being able to provide highly effective cybersecurity is diminished, and local governments can expect to experience severe and debilitating cybersecurity incidents over time.

B. Things to Do

The items discussed above naturally lead to recommendations of things that local government officials and top managers should do in order to establish and maintain high levels of cybersecurity. Here are some things that they must they do.

1. Learn the basics of cybersecurity.

Knowing the basics of cybersecurity (and this primer will help, but alone, it is not sufficient) is essential for elected officials and top managers. If they do not understand cybersecurity, how will they be able to know if it is being practiced properly and effectively? Perhaps the easiest ways to gain this knowledge are: take the internal cybersecurity awareness training offered by your local government (see Section B.7 below); enroll in a class or classes in cybersecurity at area colleges and universities; attend sessions on cybersecurity at professional conferences; attend Table Top Exercises, which gives top officials an opportunity to see the potential impact of cyberattacks on critical services (these are available at no cost to local governments from the Cybersecurity and Infrastructure Security Agency); regularly talk to your government's IT and cybersecurity leaders; and read the growing literature about the management and practice of local government cybersecurity.

2. Fund cybersecurity and IT support adequately.

Within their budgetary capabilities, local governments should fund cybersecurity adequately. We also recommend that cybersecurity have a dedicated budget rather than being part of, say, the IT budget. In 2018, the National Association of State Chief Information Officers (NASCIO) found that just under half of states had dedicated cybersecurity budgets, and states spend between zero and three percent of their IT budgets on cybersecurity. By contrast, Gartner (Nash, 2019) found that businesses in the U.S. spent between five and eight percent of their IT budgets on cybersecurity.

Without adequate funding, cybersecurity cannot be managed and practiced at the highest level possible. And remember, much of what constitutes "good cybersecurity" (such as keeping systems currently patched) often is handled by the regular IT staff. So, IT needs to be adequately funded as well.

3. Adequately staff cybersecurity with qualified personnel.

This recommendation follows from Section A.5. Because cybersecurity is underfunded, it is also understaffed in many local governments. Local governments must staff cybersecurity and IT support adequately so that best practices can be implemented and sustained at the highest level possible.

4. Think about cybersecurity as you would think about safety. It's everyone's business.

Research has found that officials in too many local governments think that cybersecurity is mainly the domain of technologists (think IT and cybersecurity staff). The reality, however, is that there are important roles for these officials to plan in cybersecurity. They need to learn as much as they can about their local governments' cybersecurity; become champions for it; be vigilant about sharing data outside of the organization; make sure cyber is baked into contracts and vendor agreements; and practice good cyber hygiene.

Cybersecurity is another form of risk management. It is essential to conduct a formal risk assessment and move toward mitigating the largest and most immediate risks facing your local government. Risk assessments help to illuminate specific cybersecurity threats, whether organizational, technological, or personnel based. These assessments also help provide a process by which threats can be prioritized by potential impact and disruption to your local government so that they can be mitigated more effectively and efficiently.

5. Practice your local government's response to a major cyberattack.

Because local governments are under constant or nearly constant cyberattack and because attacks sometimes succeed, every local government should practice its response to a large cyberattack. Such attacks can bring an organization to a halt, severely disrupt services and have significant financial impact. Having a good incident response plan and knowing who in the local government plays particular roles during a response is very important. CISA and many cyber insurers provide cyber response planning and facilitation services (CISA, n.d.a).

6. Cybersecurity should be part of emergency preparedness.

Every time there is an emergency preparedness meeting in your local government, your CISO (or other appropriate official) must have a seat at the table. This is because cybersecurity is (or should be) an integral part of emergency preparedness. It is essential to integrate your local government's incident response plan with its emergency operations plans so in the case of a significant breach the proper parties are notified and involved in the government-wide response. Similarly, the emergency operations plans should take into account the importance of ensuring that your government's network and information systems continue to operate during a disaster, whether natural, technological, or adversarial in nature.

7. Fully support cybersecurity and especially ensure full cybersecurity buy-in by top leadership (both elected and appointed).

A complaint heard repeatedly from Chief Information Security Officers (CISOs) and IT directors in local governments is that top local government officials do not provide adequate support for

cybersecurity. If top officials do not provide such support, it sends a signal to the workforce that cybersecurity is not a high priority. So, employees may rightly ask "If they don't support cybersecurity, why should we?" Thus, it is doubly important for top officials to understand and act upon the notion that cybersecurity is one of, if not the most important responsibility they have to their governments, residents and businesses.

Examples of support by top officials include elevating cybersecurity to a priority in every aspect local government management and practice, adequately funding and staffing cybersecurity, using the "bully pulpit" at every reasonable opportunity to champion cybersecurity to all parties in the organization

8. Develop and maintain a culture of cybersecurity throughout the organization.

Cybersecurity should be everyone's job, all the time. Reaching this goal, however, takes time, effort and leadership. As we note in Sections B.4 and B.7, leaders must provide adequate support for cybersecurity within their local governments. Their leadership will go a long way toward creating and maintaining a culture of cybersecurity. What constitutes a culture of cybersecurity? It is a culture within an organization in which everyone, regardless of job title, knows the importance of cybersecurity and also practices proper cyber hygiene (see definition below).

> *According to Norton (2021), cybersecurity hygiene is defined as being: "…about training yourself to think [and presumably act] proactively about your cyber security [sic] – as you do with your personal hygiene – to resist threats and online security issues." If practiced properly, cyber hygiene will become a habit.*

9. To the maximum extent possible, centralize all aspects of cybersecurity under a single, qualified Chief Information Security Officer (CISO) or other appropriate senior official.

As we note in Section D.3, many local governments operate within federated structures. One example of this is a large city in the western U.S. where the CISO's office has to work with over 50 independent departments that manage their own cybersecurity. This can make managing cybersecurity for the entire organization frustrating and difficult. Therefore, we repeat here what we said in that section. Streamline a federated structure to the maximum extent possible or, preferably, replace federated structures with a single cybersecurity office headed by the local government's CISO and appropriately staffed.

10. Require all personnel (elected and top appointed officials, department managers, staff and vendors/contractors -- everyone) to complete periodic cybersecurity training and hold all personnel accountable for their cyber hygiene.

All parties – including elected officials and those in appointed leadership -- should be required to partake in periodic cybersecurity awareness training. All parties also should be tested periodically for their online actions and re-trained and re-tested as needed. If anyone repeatedly violates their local government's cybersecurity policies and rules, consequences should follow, including job termination if warranted. Local governments can help facilitate a culture of cybersecurity by adopting sound cybersecurity policies, writing cybersecurity into all job descriptions and holding all personnel accountable for their online actions.

11. Adopt industry best-practice cybersecurity policies and processes and fully implement them.

These include such policies as: National Institute of Standards and Technology (NIST) Special Publication guidelines including the Cybersecurity Framework (NIST, 2018a), the Security and Privacy Controls for Information Systems and Organizations [800-53r5] (NIST, 2020), the Risk Management Framework [800-37r2] (NIST, 2018b), and the Incident Response Life Cycle [800-61r2] (NIST, 2012).

See Section C.7 and adopt and properly implement the recommended policies. The reasons why should be obvious but are spelled out in that section.

12. Partner with federal, state and local government entities for cybersecurity guidance and assistance, as well as CISA's regional office for your area, your local FBI field office and other entities as warranted.

Examples include but are not limited to: other local governments; local government membership and professional organizations; relevant departments and agencies of state government; state National Guard units with cybersecurity support capabilities; relevant federal agencies such as CISA's regional office for your area, and your local FBI field office; and the Multi-State Information Sharing and Analysis Center (MS-ISAC). Other ISACs – like the Water ISAC if the local government is in that critical infrastructure sector – can also be helpful to local governments. These and possibly other organizations can be helpful to local governments in many ways. Depending on the staffing and resources they have, they may provide one or more of the following: guidance and advice; policy and other important documents; training or training templates; training itself; risk assessments; alerts regarding potential cyber threats; pre-attack planning and post-attack assistance; cybersecurity scanning and more. CISA alone provides a number of free services and assessments of which local governments can take advantage. Since the adoption of various federal laws in recent years, there is also funding available from CISA to assist local governments provide improved cybersecurity. Some state governments are also beginning to provide funding to assist local governments with cybersecurity.

C. Some Questions to Ask (our local government cybersecurity staff)

Local officials should take advantage of the knowledge and experience of their IT and cybersecurity staff. These are the local governments' technical experts who can be valuable resources to help officials understand many aspects of their governments' cybersecurity. Meet with them periodically and ask questions. Here are some important questions to begin with.

1. What are our local government's biggest cyberthreats?

Ransomware attacks are the one of the biggest, if not the biggest cyberthreats facing local governments. These types of attacks involve the bad guys inserting malicious software, or malware, onto an IT system. The malware then encrypts the organization's files and systems, making them unusable unless a ransom is paid. Typically, attackers utilize social engineering,

such as phishing or spear phishing, in which users are tricked into believing comes from a known and trusted source. However, the source is anything but trustworthy. These emails contain malicious attachments or URLs that, when opened, insert the malware into the IT system. The 2022 Verizon Data Breach Investigations Report (DBIR) found a thirteen percent year-over-year increase in ransomware attacks, greater than the previous five years combined (Verizon, 2022). Verizon's 2023 DBIR found that ransomware attacks remained steady at nearly a quarter of all breaches (Verizon, 2023). Local governments are also subject to attacks attempting to glean user credentials, allowing the attackers access to the IT system and encrypt systems or steal data.

2. Is our local government capable of effective responses to cybersecurity attacks, breaches and other adverse cyber events?

In order to know if your local government is capable of responding effectively to cyberattacks and breaches, you must first know what your local government needs to protect. An accurate inventory must be taken of your local governments IT assets, including datasets, devices, hardware, software, information and networks, as well as any processes and procedures currently in effect. Your local government must also periodically conduct formal risk assessments or analyses in order to understand and prepare for vulnerabilities of all kinds. Once a risk-analysis is completed, the vulnerabilities that were identified, whether technical, operational, or procedural, must be addressed.

3. Who is in charge of cybersecurity in our local government?

Local governments require a clear cybersecurity chain of command headed by a trained and experienced CISO (or some other appropriate official) with the authority and responsibility to manage cybersecurity throughout the organization. The CISO should report directly to the top decision-maker in the government (e.g., city or county mayor, city or county manager, etc.), and should have a seat at all decision-making tables where actions are taken and/or policies are adopted that can affect the cybersecurity of the local government. As we noted in Section B.9, some local governments operate an environment of federated and dispersed IT structures in which cybersecurity is managed in individual departments, rather than a single government-wide office. We recommend streamlining this structure as much as possible or, preferably, replacing it with a single office for all of the government's cybersecurity. Doing so will help to ensure that the entirety of the local government's IT system is well understood and protected.

4. Is cybersecurity funding in our local government adequate?

As previously mentioned, studies have repeatedly found inadequate cybersecurity budgets as the top barrier to local government cybersecurity. Find out if cybersecurity is adequately funded in your government by asking your budget office, your IT director and/or your CISO. It is not necessary to know an exact dollar amount because that will vary greatly among local governments depending on the size of the overall budget. However, knowing the percent of the IT budget that cybersecurity funding constitutes will be revealing. If it is less than three percent, it is probably underfunded. As we recommended in Section B.2, the budget for cybersecurity should be dedicated. The MS-ISAC's 2021 Nationwide Cybersecurity Review found that

organizations that dedicated at least three percent of their IT budget to cybersecurity scored 21 percent higher on a cyber maturity scale than those that did not (MS-ISAC, 2021).

5. Does our local government we have the right number of cybersecurity staff, are they in the right positions, and are they properly qualified?

There is no easy way to answer this question due to the considerable variation of size and types of local governments. Some local governments completely outsource cybersecurity, while others perform this function entirely in-house and in others it is mixed. It is safe to say that local governments serving larger populations should generally have more cybersecurity staff than local governments serving smaller populations. We recommend that once a local government understands the types and range of cybersecurity functions that must be performed it can estimate the number of staff and skill sets required for those functions. Local governments can also look to similar governments with successful cybersecurity departments to emulate.

6. Has our local government adopted and fully implemented cybersecurity best practices?

Local governments must look to the following organizations for best practices and resources: the National Institute of Standards and Technology (NIST); CISA within the Department of Homeland Security; MS-ISAC; and the Office of National Cyber Director. NIST's Cybersecurity Framework is the foundational document for organizations to use to develop their own cybersecurity policies. The Framework epitomizes current cybersecurity best practices and explains a process that organizations can implement to continuously improve their cybersecurity posture. It also references specific technical best practices as laid out in NIST's Special Publications guidelines. CISA publishes a catalog of known exploited vulnerabilities, also known as common vulnerabilities and exposures (CVEs), which link to known patches and fixes, if available. CISA also performs assessments for free for local governments.

7. Has our local government adopted and fully implemented highly recommended cybersecurity policies?

The following is a list of essential cybersecurity policies that local governments should adopt and implement. There are also "desirable" but not essential policies, but for the sake of brevity, we do not list them here. For a more robust discussion of cybersecurity policies, see Chapter 7, Local government cybersecurity policies in *Cybersecurity and Local Government* by Norris, Mateczun and Forno (2022).

Essential cybersecurity policies.

- Acceptable Use Policy, which governs how people use the local government IT systems.
- Information Security Policy, which describes how data and information on a local government IT system is protected and handled, including the requirement that data at rest be encrypted at all times.
- Privacy Policy governing how the local government's websites collect, use, store and share different types of information.

- Identity and Access Management Policy establishing the process for creating and removing user accounts, categories of users, and the various roles and permissions that may be assigned to users based on their function within the organization.
- Incident Response Policy, which describes how the local government will respond in the event of an cyberattack.
- Disaster Recovery or Business Continuity Policy, which describes how the organization responds to major emergencies.

8. Does our local government require periodic cybersecurity training for all personnel?

All local government employees, including elected and top appointed officials, should receive periodic mandatory cybersecurity awareness training. This training can be tailored for specific local governments and can also be purchased from outside organizations.

9. Does our local government have accountability mechanisms in place to enforce proper cyber hygiene and does it implement them?

Not only should all elected officials, managers, staff and vendors receive cybersecurity training, but local governments should implement and utilize accountability mechanisms to enforce cyber hygiene throughout the organization. If a user accidentally or intentionally violates the Acceptable Use Policy, then they should face appropriate counseling, and if violations continue, more serious accountability measures should come into play, from loss of user privileges to termination of employment (although the latter would be difficult to impossible to enforce for elected officials).

10. Does our local government have ongoing relationships with state/federal cybersecurity and related agencies?

In addition to CISA, NIST, the FBI, and MS-ISAC, local governments should look to develop ongoing relationships with the Department of Justice's National Cyber Investigative Joint Task Force, and your state's IT and cybersecurity resources or other regional organizations or academic institutions. Some state National Guard units also provide cybersecurity assistance to local governments in the case of adverse cyber events. Local governments should also consider partnering with the IT or cybersecurity departments or units in area universities and colleges.

11. Has our local government sought state/federal cybersecurity funding?

The Infrastructure and Investment Jobs Act of 2021 established the State and Local Cybersecurity Grant Program, which appropriated $1 billion to be awarded over four years (CISA, n.d.b.). CISA and the Federal Emergency Management Agency administer this program specifically for state, local, tribal and territorial (SLTT) governments. States must apply for these funds, and once they are received, the states distribute to local governments. Eighty (80) percent of these funds must go to local governments, with a minimum of 25 percent to rural areas. Some states may also provide cybersecurity grants to local governments outside of this fund.

D. The Future of Cybersecurity

1. Ransomware

Ransomware remains one of the most prominent, devastating and costly cyberattacks, checking in fairly consistently in recent years at about one quarter of all cyberattacks. No local government should underestimate the devastating impacts of this particular cyber menace. Some sources suggest that ransomware proliferation is likely to increase, especially with the onset of Artificial Intelligence (AI) and large language models (LLMs) that can help create and disseminate powerful malware and convincing phishing and spearphishing emails. Although it is difficult to anticipate the extent to which these attacks will grow, the sheer number of local governments in the US, and the fact they provide critical infrastructure and public services, means they are attractive targets for attackers. The criminal market for ransomware is also likely to grow if organizations continue to pay the ransoms.

2. More Frequent and More Severe Attacks

Similar to the discussion of ransomware above, the onset of AI and ChatGPT indicates a new era of creating and developing attacks and disseminating them at a much faster speed. Additionally, there is a growing number of cybercriminals who are often motivated by financial incentives to attack as many organizations as possible. The barrier to entry for someone to become a cybercriminal is relatively low, as there is a plethora of inexpensive and easy to use do-it-yourself hacking kits available for sale online. It is also incredibly difficult to attribute attacks to a single person or organization, let alone apprehend them successfully, as many of them operate within hands-off nation states, or even those that outright encourage hacking groups.

4. Artificial Intelligence

Since its release, the ChatGPT artificial intelligence (AI) software has become widely known and used. From the dire predictions of the fall of mankind, to the calls for government and international regulation, AI is seemingly everywhere in the news. As previously discussed, AI and LLMs have the potential to create newer and more effective social engineering techniques and phishing attempts, as well as attack code and methods. However, AI also has the potential to aid in cybersecurity through automated monitoring and rule enforcement. AI, like technology itself, can be used for malicious and benevolent purposes. It depends on the human users and creators of AI to determine how it will be used. It is imperative that local governments using AI based software understand AI, especially how it is created, how it is used, as well as its inaccuracies and potential downsides including privacy, security and discrimination risks. For example, Connecticut recently passed regulations for governmental use of AI after the Connecticut Department of Children and Families used a predictive analysis tool to help identify children in imminent danger that was later abandoned because it "…miss[ed] urgent cases and inaccurately flag[ged] less serious ones." A study published in the journal *Child Abuse & Neglect* later found it didn't improve child outcomes (Dewey, 2023).

5. The Cloud

The “cloud” is a term that refers to information resources stored by third-party organizations separate from the local government using those resources, such as Amazon Web Services, Microsoft, Google and Oracle. (Hint: There really is no cloud!) Therefore, local governments can store their information resources not only on their own IT systems, but also with cloud providers. The 2023 CompTIA Public Technology Institute (PTI) State of City and County IT National Survey found that 69 percent of respondents had moved their on-premises infrastructure to a private cloud and that 71 percent shifted from using a local version of an application to a cloud application (Shark, 2023). However, there is great concern over the accountability of cloud providers, specifically lack of best practices and contracts that do not allow local governments to shift providers. Other concerns include: security and privacy; regulation and compliance; interoperability; cost; vendor lock-in; and lack of control.

6. IoT expansion

The Internet of Things (IoT) continues to expand rapidly, especially as some local governments move toward implementing “smart city” infrastructure capabilities. Similar to moving to the cloud, using IoT devices shifts responsibility of device security to third party developers. There are also concerns about interoperability of systems depending on the devices used, the security of these devices as many are manufactured in places such as China, and the lack of best practices in the creation of these products. Hence, purchasing from vendors that have adopted the principles of security-by-design and -default should be something that local governments seriously consider. For those unfamiliar with the concept, security by design means software developers and device manufacturers shift from vulnerable designs to designs where customer security is a core business goal, rather than a feature, and secure by default means that products are secure “out of the box” (CISA, 2023a).

7. BYOD

BYOD, or bring your own device, policies govern how and if local government employees and third party contractors can use personal devices for work, and on the local government’s IT system. The COVID-19 pandemic increased concerns over these issues, as many employees had to work from home and remotely access their government’s network and information resources. Using your own devices can drastically improve efficiency and productivity. However, these devices are extremely vulnerable to phishing attacks through direct messages and text messages. To the extent possible, local governments should provide employees secure devices that are used solely for government business, or at the very least utilize a multifactor authentication tool in order to access confidential and sensitive information.

8. Remote Work

Remote and flexible work will likely remain a component of working in local government in the future, especially as an employee recruitment and retention tool, as the world moves on from the pandemic. Insecure personal devices should not be used to conduct government business remotely, especially on insecure Wi-Fi networks. The security of the cloud and third-party vendors used by remote workers is also a concern. Local governments should require that

employees use only approved devices on secure networks. Multifactor authentication should be required to access the local government's information resources. Users should potentially even use a Virtual Private Network (VPN) when working remotely because the VPN hides the users IP information from the public and encrypts internet traffic sent and received by the user.

9. Zero Trust

The concept of zero trust in cybersecurity is essential in an increasingly complex IT environment from IoT devices to third-party and cloud contractors and multiple complex information systems. These complexities expand the attack surface of a local government. A zero trust approach to network and data security means what it says – no user and no device should be trusted to connect to the local government's network unless it is fully and continually authenticated. This means that local governments should assume that all internet traffic might be malicious and all devices might be compromised. Do not trust until verified. CISA has developed a Zero Trust Maturity Model that provides road maps for federal agencies to reference as they move to zero trust architecture, which may be of interest to local governments, as well (CISA, 2023b).

10. Defense in Depth

Defense in Depth is a strategic concept of cybersecurity management in which layers of defensive protocols are put in place to protect data and systems through redundant fail-safes that attempt to counter attacks at each level of penetration. Essentially, attacks follow different paths to attempt to reach the same thing: the data or system of interest. Each of these different paths needs to be protected, so that if at one level the attack succeeds, it can potentially be stopped at another. Similar to zero trust architecture, defense in depth is a growing concept that may ultimately be required for local governments to follow.

11. Build Cybersecurity into Everything

Planning at all levels and fields of government must deliberately include cybersecurity as an integral component. Everything from physical systems planning, to database development, or implementing new technologies and service contracting, must include cybersecurity. Before adopting or modifying any services, procedures, operations, and technologies, all aspects of their cybersecurity must be considered. Any local government implementing any new technology must consult with the IT and cybersecurity departments so that the latter can help to ensure that those technologies have built in cybersecurity.

12. Legacy Technology

The term "legacy technology" means "the old stuff," like hardware, devices, software, and systems that are outdated and obsolete. This is a current issue facing local governments, and it will continue to grow as increasing numbers of technologies and software are no longer supported by the manufacturer or creator. For example, during the pandemic, New Jersey requested volunteer programmers to help fix the state's unemployment benefits system that was running on 40-year-old mainframes using a 61-year-old programming language (Leswing,

2020). Relying on legacy technology can lead to severe security issues, as well as the potential for such a system to break down and not be fixable.

13. The Future of Cybersecurity is ever-changing

Just like technology, cybersecurity is constantly evolving. As new software and technology are developed, the bad guys will find and exploit new vulnerabilities. Security, such as encryption, will evolve to provide continued protection. Cybersecurity is also inextricably intertwined with national security and can be anticipated to grow and evolve at an increasing rate especially with the use of AI and LLMs. However, the fundamentals of cybersecurity remain the same. Protect information, in transit and at rest, from unauthorized access and alteration, so that it remains usable for those who need it.

14. State/Federal Regulation

Neither the federal government nor states engage in much, if any, regulation of local government cybersecurity today. However, this is likely to change, although perhaps slowly. Indeed, we have already seen movement in this area as states have started regulating organizational use of applications, such as TikTok. The federal government has also started to release cybersecurity recommendations, which are, or will soon likely be, mandatory for some sectors such as critical infrastructure providers (e.g., water, utility and energy). Local governments can anticipate that the federal government might also continue to provide funding to states and local governments to improve cybersecurity, especially as nation-states like Russia, China, Iran and North Korea continue to threaten local governments and critical infrastructure.

E. Small Local Governments and Cybersecurity

The United States is awash in small local governments: 12,801 with populations less than 2500 (Miller, 2018); 78 percent had 10,000 or fewer (ICMA, 2013); and 75 percent had fewer than 5,000 residents (Toukabri and Medina, 2020). Small local governments, especially the smallest, typically quite have limited budgets and equally limited staffing. This means that they are likely to have much greater difficulty providing high levels of cybersecurity than larger, more wealthy local governments. (Yes, of course there are exceptions. One of several of which is Naples, Florida, a city of less than 20,000 with multi-million dollar homes, especially on its Gulf coast.)

Here are a few suggestions to assist small local governments provide effective cybersecurity.

1. First, read and, to the extent practicable for your local government, strive to implement the recommendations in the previous sections;

2. Require mandatory cybersecurity awareness training for all elected officials, top managers, staff and vendors that will be on site or otherwise will use the local government's IT system to teach them to understand the need for cybersecurity, to

practice good cybersecurity hygiene and to understand and follow the cybersecurity rules and roles described in their governments' IT and cybersecurity policies;

3. Enable multifactor authentication;

4. Control physical access to their governments' information technological assets;

5. Perform regular data and system backups;

6. Perform regular patch management; and

7. Partner with other local governments, appropriate state and federal agencies for guidance and assistance.

Following these suggestions (and others made above) will make it more likely that small local governments will be able to provide high levels of cybersecurity. Failing to follow them will most likely produce the opposite result – a result that no local government should allow to occur.

Norris and Mateczun are authors of: ***White Paper: What Local Government Officials Should Know and Do about Cybersecurity.*** *Baltimore, MD: University of Maryland, Baltimore County. 2020 (https://publicpolicy.umbc.edu/wp-content/uploads/sites/176/2020/06/Cybersecurity-White-Paper.pdf.) This White Paper was written for and in conjunction with the Coalition of City CISOs (www.cityciso.org/research).*

Together with Richard F. Forno, Norris and Mateczun also authored: ***Cybersecurity and Local Government.*** *Hoboken, NJ, USA: John Wiley & Sons, 2022.* https://www.wiley.com/en-us/Cybersecurity+and+Local+Government-p-9781119788287

References

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.a). *Incident Response Plan (IRP) Basics.* https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.b). *State and Local Cybersecurity Grant Program*. https://www.cisa.gov/state-and-local-cybersecurity-grant-program

Cybersecurity and Infrastructure Security Agency (2023a, April 13). *Shifting the balance of cybersecurity risk: Principles and approaches for Security-by-Design and -Default*. https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

Cybersecurity and Infrastructure Security Agency (2023b, April 11). *Zero Trust Maturity Model*. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Dewey, C. (2023, June 5). AI is used widely, but lawmakers have set few rules. *Stateline*. https://stateline.org/2023/06/05/ai-is-used-widely-but-lawmakers-have-set-few-rules/

(ISC)^2. (2022). *(ISC)^2 Cybersecurity Workforce Study*. https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

International City/County Association (ICMA). 2013). *The Municipal Yearbook: 2013.* Washington, D. C. International City County Management Association.

Leswing, K. (2020, April 6). New Jersey needs volunteers who know COBOL, a 60-year-old programming language. *CNBC*. https://www.cnbc.com/2020/04/06/new-jersey-seeks-cobol-programmers-to-fix-unemployment-system.html

Miller, Ben. (2018, December 3). *Nearly Half of U.S. Cities Have Fewer Than 1,000 Residents.* https://www.govtech.com/data/nearly-half-of-us-cities-have-fewer-than-1000-residents.html

Multi-State Information Sharing & Analysis Center (MS-ISAC). (2021). *2021 Nationwide Cybersecurity Review Summary Report*. https://www.cisecurity.org/insights/white-papers/2021-nationwide-cybersecurity-review-summary-report

National Association of State Chief Information Officers (NASCIO). (2020). *Ensure dedicated cybersecurity funding for state and local governments with CIOs as key decisionmakers*. www.NASCIO.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf

National Institute of Standards and Technology (NIST). (2018a, April 16). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology (NIST). (2018b, December). *Risk Management Framework for Information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

National Institute of Standards and Technology (NIST). (2020, September). *Security and Privacy Controls for Information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Institute of Standards and Technology (NIST). (2012, August). *Computer Security Incident Handling Guide.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Nash, Kim. (2019, December 30). Tech chiefs plan to boost cybersecurity spending. *The Wall Street Journal.* https://www.wsj.com/articles/tech-chiefs-plan-to-boost-cybersecurity-spending-11577701802

Norris, Donald F., Laura K. Mateczun and Richard F. Forno. (2022). *Cybersecurity and Local Government*. Hoboken, N. J.: John Wiley and Sons. https://www.wiley.com/en-us/Cybersecurity+and+Local+Government-p-9781119788287

Norton. (2021). *Good cyber hygiene habits help stay safe online*. https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html

Shark, A. (2023, March 15). Cloud services: A cloudy forecast for state and local governments. *American City & County*. https://www.americancityandcounty.com/2023/03/15/cloud-services-a-cloudy-forecast-for-state-and-local-governments/

Toukabri, Amel and Lauren Medina. (2020, May 21). *Latest City and Town Population Estimates of the Decade Show Three-Fourths of the Nation's Incorporated Places Have Fewer Than 5,000 People.* Washington, D. C. U.S. Census. https://www.census.gov/library/stories/2020/05/america-a-nation-of-small-towns.html

Verizon. (2023). *Verizon 2023 Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/dbir/

Verizon. (2022). *Verizon 2022 Data Breach Investigations Report*. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

Verizon. (2021.) *2021 DBIR Master's Guide*. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/